

Contratto di custodia e amministrazione di cripto-attività

Nota: le presenti disposizioni riportano le condizioni contrattuali applicabili al Servizio di custodia e Amministrazione prestato da Cryptosmart S.p.A. che saranno sottoposte agli Utenti una volta ottenuta l'autorizzazione a operare ai sensi del MiCAR. Le disposizioni di seguito riportate saranno integrate all'interno delle condizioni contrattuali generali utilizzate dalla società, le quali disciplineranno altresì gli ulteriori servizi prestati ai sensi del MiCAR.

* * * *

DISPOSIZIONI PRELIMINARI

Il presente contratto (il **"Contratto"**) è concluso a distanza, in forma elettronica, tra Cryptosmart S.p.A., con sede legale in Via Bruno Simonucci n. 18, 06135 Perugia (PG), capitale sociale Euro 285.379,40, C.F., P. IVA e n. iscrizione al Registro delle Imprese di Perugia 03775010543, nella qualità di prestatore di servizi per le cripto-attività, autorizzato con numero [●], in persona del legale rappresentante *pro tempore* (di seguito, la **"Società"** o **"Cryptosmart"**), e l'utente che, identificato ai sensi della normativa applicabile, accede alla Piattaforma gestita da Cryptosmart (la **"Piattaforma"**) via *web* o *app* (l'**"Utente"**).

La Società e l'Utente sono di seguito indicati singolarmente la **"Parte"** e congiuntamente le **"Parti"**.

Formano parte integrante e sostanziale del presente Contratto i seguenti allegati:

Allegato A - Descrizione dei Wallet Omnibus, dei relativi rischi e dei presidi adottati dalla Società;

Allegato B - Descrizione dei rischi, tempi e costi delle operazioni di Staking.

La Società presta nei confronti dell'Utente, tra l'altro, il servizio di custodia e amministrazione di cripto-attività per conto degli Utenti ai sensi dell'articolo 3, par.1, n. 16, lett. a), del Regolamento (UE) 2023/1114 (**"MiCAR"**), in conformità al quadro regolamentare applicabile, incluso, ove ricorrano i presupposti, il Regolamento (UE) 2022/2554 (**"DORA"**).

L'Utente prende atto e riconosce che intende avvalersi del Servizio di Custodia e Amministrazione offerto dalla Società, alle condizioni tutte del presente Contratto.

L'Utente prende atto e riconosce che il Sito, configurato al dominio <https://www.cryptosmart.it>, gli eventuali domini di secondo livello, accessibili dalle singole pagine del Sito, e i contenuti ivi pubblicati, nonché le eventuali API (*Application Programming Interface*) di accesso a determinati contenuti del Sito o i *widget* con i dati del Sito, sono di proprietà esclusiva della Società.

La Società ha adottato una *policy* interna in materia di custodia e amministrazione di cripto-attività per conto degli Utenti, approvata dal Consiglio di Amministrazione,

la cui sintesi è pubblicata in forma accessibile sulla Piattaforma, e che qui si intende pienamente richiamata.

1. Definizioni

Salvo ove diversamente previsto, i termini riportati con lettera iniziale maiuscola avranno il significato attribuito loro nelle definizioni che seguono:

“Account” indica il profilo dell’Utente sulla Piattaforma della Società, mediante il quale l’Utente accede ai Servizi.

“Cripto-attività” indica le rappresentazioni digitali di valore o di diritto trasferibili e memorizzabili elettronicamente mediante DLT o tecnologia analoga ai sensi del MiCAR.

“Fondi” indica le somme di denaro in valuta avente corso legale ricevute e depositate dalla Società per conto dell’Utente in connessione ai Servizi.

“Hot Wallet” e **“Cold Wallet”** indicano i portafogli digitali, rispettivamente connessi e non connessi alla rete Internet, utilizzati dalla Società per la custodia delle Cripto-attività degli Utenti.

“Piattaforma” indica l’infrastruttura informatica (*web* e *mobile*) tramite cui la Società presta i Servizi.

“PoS” o **“Proof of Stake”** indicano il meccanismo di consenso che valida le transazioni bloccando (o mettendo in Staking) alcune Cripto-attività.

“Registro delle Posizioni” indica il registro nominativo e in tempo reale, tenuto dalla Società, che indica il saldo e i diritti dell’Utente sulle Cripto-attività custodite.

“Servizi” indica il servizio di custodia e amministrazione di Cripto-attività per conto

dell’Utente, nonché i servizi accessori e strumentali indicati nel presente Contratto.

“Servizio di Custodia e Amministrazione” indica il servizio di custodia e amministrazione di cripto-attività per conto degli Utenti ai sensi dell’articolo 3, par.1, n. 16, lett. a), del Regolamento (UE) 2023/1114.

“Staking” indica l’attività di blocco delle transazioni delle Cripto-attività che consente all’Utente di validare blocchi nuovi e guadagnare ricompense.

“Utente” indica l’Utente, titolare dell’Account, che accetta il Contratto tramite la Piattaforma.

“Wallet Omnibus” indica portafoglio digitale sul quale sono le Cripto-attività di più utenti, con registrazione nominativa delle posizioni nel Registro delle Posizioni.

2. Conclusione del Contratto

2.1 Il Contratto è reso disponibile sulla Piattaforma in formato digitale e si considera concluso quando l’Utente, dopo la creazione dell’Account e il completamento delle verifiche di identificazione conformemente alla normativa di volta in volta applicabile, seleziona l’apposita opzione di accettazione.

2.2 L’accettazione elettronica dell’Utente costituisce sottoscrizione ai sensi della normativa applicabile. I *log* applicativi, le marcature temporali, gli identificativi dell’Account e le evidenze informatiche generate dai sistemi della Società costituiscono piena prova della conclusione, del contenuto e della data del Contratto e delle istruzioni impartite.

2.3 Una copia del Contratto in vigore è sempre disponibile e scaricabile dall’Utente

all'interno della Piattaforma. Eventuali aggiornamenti sono comunicati secondo l'art. 17.2.

NATURA DEL SERVIZIO

3. Oggetto del Contratto

3.1 L'oggetto del presente Contratto consiste nella prestazione, da parte della Società in favore dell'Utente, del Servizio di Custodia e Amministrazione.

3.2 Tale servizio comprende, tra l'altro: la salvaguardia dei mezzi di accesso alle Cripto-attività (ivi incluse le chiavi crittografiche private), l'esecuzione delle istruzioni impartite dall'Utente in merito al trasferimento delle Cripto-attività custodite, l'aggiornamento in tempo reale del Registro delle Posizioni, nonché l'adempimento degli obblighi informativi previsti dalla normativa applicabile.

3.3 Le Cripto-attività dell'Utente sono custodite in Wallet Omnibus, con registrazione nominativa, accurata e costantemente aggiornata delle relative posizioni nel Registro delle Posizioni, grazie alla presenza di Cold Wallet multi-firma e Hot Wallet. Ulteriori informazioni sul funzionamento del Wallet Omnibus e sui relativi rischi, unitamente ai relativi presidi, sono riportate all'interno dell'Allegato A.

3.4 La Società agisce sempre sulla base delle istruzioni impartite dall'Utente non diviene mai proprietaria delle Cripto-attività dell'Utente né utilizza queste per conto proprio.

POLITICA DI CUSTODIA E MISURE DI SICUREZZA

4. Rischi connessi all'utilizzo dei Wallet Omnibus

4.1 L'Utente prende atto e riconosce che, per la prestazione del Servizio di Custodia e Amministrazione, le Cripto-attività da lui detenute saranno custodite in un Wallet Omnibus, che conterrà Cripto-attività di più clienti della Società. In tal senso, le Cripto-attività dell'Utente saranno segregate e registrate in modo nominativo nel Registro delle Posizioni, ma rimarranno fisicamente all'interno del Wallet Omnibus con altre cripto-attività degli Utenti della Società.

4.2 L'Utente prende atto e riconosce che l'utilizzo di Wallet Omnibus potrebbe essere esposto a rischi di sicurezza informatica sebbene la Società adotti misure e presidi di protezione delle chiavi private e delle Cripto-attività conformi ai più alti *standard* di sicurezza.

4.3 L'Utente prende atto e riconosce che l'utilizzo di Wallet Omnibus non comporta l'immediata disponibilità e che gli eventuali trasferimenti sono interamente gestiti dalla Società su richiesta dello stesso.

4.4 Ulteriori informazioni sui rischi a cui l'Utente è esposto in ragione dell'utilizzo di Wallet Omnibus sono riportate all'interno dell'Allegato A.

4.5 L'Utente riconosce e prende atto che nel caso di insolvenza della Società, le Cripto-attività detenute potrebbero essere soggette ai processi legali relativi alla liquidazione o procedura concorsuale, fermo restando quanto previsto dall'art. 4 in materia di segregazione.

5. Segregazione delle Cripto-attività e dei Fondi

5.1 Le Cripto-attività e i Fondi degli Utenti sono segregati rispetto al patrimonio della Società e non rientrano nella massa attiva in

caso di insolvenza della Società. La segregazione è operativa, tramite l'utilizzo di *wallet* e conti dedicati agli Utenti distinti da quelli della Società; e legale, tramite registrazioni nominative e contabilità separata attestante i diritti degli Utenti.

5.2 In caso di insolvenza della Società, 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 dei Fondi degli Utenti, fatti salvi gli adempimenti di legge.

6. Staking e servizi accessori

6.1 Ove disponibile su specifiche Cripto-attività, secondo quanto indicato di volta in volta sulla Piattaforma, l'Utente può impartire istruzioni per la partecipazione allo Staking. Le ricompense sono accreditate al netto delle commissioni indicate sulla Piattaforma. Restano ferme le specifiche cautele e limitazioni tecniche e regolamentari applicabili.

6.2 La Società non presta servizi di Staking presso *liquidity pool* o meccanismi di finanza decentralizzata non riconducibili al modello di validazione PoS; eventuali estensioni saranno oggetto di informativa preventiva.

7. Gestione dei Fondi

7.1 Tutti i Fondi utilizzati dagli Utenti ai fini della prestazione di uno o più Servizi, sono depositati entro la fine del giorno lavorativo successivo presso istituti di credito o banche centrali e in ogni caso su conti distinti da quelli della Società. I conti dedicati ai Fondi degli Utenti sono rubricati in modo tale da evidenziare la loro natura segregata.

7.2 La Società effettua riconciliazioni giornaliere tra: i saldi dei Fondi complessivi

degli Utenti risultanti dalla contabilità interna e le giacenze presenti sui conti bancari dedicati agli stessi.

7.3 L'Utente può disporre in ogni momento il prelievo dei Fondi depositati, con esecuzione da parte della Società entro il giorno lavorativo successivo alla ricezione dell'ordine, salvi i tempi tecnici del circuito bancario e le verifiche di sicurezza e antiriciclaggio.

8. Custodia delle chiavi e resilienza operativa

8.1 Le chiavi private relative ai Cold Wallet sono custodite tramite soluzioni che prevedono la partecipazione di più soggetti autorizzati e l'utilizzo di supporti fisici protetti secondo procedure di sicurezza adeguate. Gli Hot Wallet prevedono soluzioni tecnologiche che garantiscono la generazione e la gestione sicura delle chiavi, la cifratura dei *backup* e l'adozione di sistemi di autenticazione multipla. Ove venga richiesto da specifiche esigenze tecniche, possono essere impiegate soluzioni di custodia di terze parti qualificate, senza che queste abbiano accesso diretto alle chiavi private.

8.2 Sono adottate misure di sicurezza a livello applicativo e infrastrutturale, inclusa la cifratura dei dati sia a riposo sia in transito, sistemi di monitoraggio per la prevenzione e rilevazione di frodi e anomalie, nonché piani di continuità operativa e di ripristino in caso di emergenza. Vengono inoltre effettuati *test* periodici di sicurezza e sono implementate procedure di gestione degli incidenti in conformità alla normativa vigente.

8.3 La gestione delle identità e degli accessi avviene secondo il principio del minimo privilegio, con autenticazione a più fattori e

controllo dei privilegi amministrativi. L'infrastruttura è segmentata per limitare i rischi e sono adottati sistemi di protezione e monitoraggio degli accessi e delle attività. Tutti i dati sensibili sono cifrati con *standard* di sicurezza riconosciuti; le chiavi crittografiche e i segreti applicativi sono custoditi in sistemi sicuri con accesso controllato e rotazione periodica. Il ciclo di vita del *software* segue pratiche di sviluppo sicuro e sono attivi processi di gestione delle vulnerabilità e delle modifiche. I *backup* sono regolari, cifrati e conservati in modo sicuro. La gestione dei fornitori prevede verifiche di sicurezza e monitoraggio delle prestazioni. L'accesso ai sistemi critici è riservato a personale autorizzato e tracciato, con segregazione delle funzioni e controlli che impediscono a un singolo operatore di autorizzare operazioni sensibili. In caso di incidente, sono previste procedure di risposta, contenimento e ripristino, con eventuali comunicazioni alle autorità competenti.

8.4 I movimenti relativi alle attività digitali e ai fondi degli Utenti sono registrati in tempo reale e vengono riconciliati almeno con cadenza giornaliera rispetto alle giacenze effettive. È assicurata la conservazione delle evidenze e la disponibilità di *report* per le autorità competenti.

8.5 La Società applica soglie massime per gli Hot Wallet e trasferimenti automatici periodici verso i Cold Wallet al superamento delle soglie, con registrazione e controllo delle operazioni.

9. Mezzi di comunicazione, istruzioni dell'Utente e autenticazione

9.1 Le comunicazioni avvengono tramite la Piattaforma e/o all'indirizzo e-mail dell'Utente registrato sull'Account. Le istruzioni operative

(depositi, trasferimenti, prelievi) sono trasmesse mediante i canali ufficiali della Piattaforma.

9.2 L'Utente si autentica con un sistema a più fattori che include: credenziali personali (*username*/e-mail e *password*), codice di conferma via e-mail e OTP generata tramite sistema di autenticazione sicura. La Società può applicare ulteriori verifiche (es. video-identificazione) in funzione del rischio e ai fini antiriciclaggio.

9.3 La Società esegue le istruzioni solo dopo l'esito positivo dei presidi antiriciclaggio e di sicurezza e può rifiutare o sospendere operazioni in caso di anomalie, sospette frodi o impedimenti di legge.

10. Divieto di utilizzo per conto proprio e segregazione dei mezzi di accesso

10.1 La Società si astiene dall'utilizzare le Cripto-attività degli Utenti per conto proprio. È vietato qualsivoglia riutilizzo, impiego in garanzia, prestito o operazione sulle Cripto-attività degli Utenti, salvo esecuzione di istruzioni dell'Utente o attività strettamente necessarie e da questi richieste.

10.2 I mezzi di accesso alle Cripto-attività degli Utenti sono chiaramente identificati e gestiti con procedure che ne impediscono la commistione con quelli della Società.

11. Esclusione di servizi di pagamento

11.1 La Società non presta servizi di pagamento ai sensi della Direttiva (UE) 2015/2366 (PSD2), né direttamente né tramite terzi. I Servizi oggetto del presente Contratto non includono in alcun caso l'esecuzione di operazioni di pagamento.

11.2 La Società non consente il trasferimento da e verso terzi di *token* di moneta elettronica, come definiti dal MiCAR.

11.3 Qualunque tentativo di trasferimento da e verso terzi di *token* di moneta elettronica sarà impedito dalla Società. La Società si riserva il diritto di sospendere gli Account che dispongono istruzioni in violazione del suddetto divieto.

12. Rendicontazione

12.1 La Società rende disponibile all'Utente, in ogni momento tramite la Piattaforma, un rendiconto aggiornato comprendente: tipologia di cripto-attività, saldo, valore e trasferimenti nel periodo. Invia inoltre un rendiconto almeno trimestrale o su richiesta dell'Utente.

12.2 La Società informa tempestivamente l'Utente in merito a eventi straordinari che possano incidere in modo significativo sui diritti dell'Utente (es. incidenti di sicurezza gravi, sospensione o *delisting* di specifiche cripto-attività, modifiche regolamentari rilevanti).

13. Commissioni, costi e oneri

13.1 Le commissioni, i costi e gli oneri applicabili al Servizio sono resi disponibili sulla Piattaforma.

13.2 Ai Servizi disciplinati dal presente Contratto, la Società non applica commissioni e costi.

13.3 In assenza di diversa indicazione, tutte le commissioni sono al netto di oneri e imposte applicabili, che restano a carico dell'Utente.

14. Responsabilità, eventi non imputabili e forza maggiore

14.1 La Società è responsabile verso l'Utente per la perdita di Cripto-attività o dei relativi

mezzi di accesso detenuti in custodia quando conseguenti a fatto imputabile alla Società (inadempimento, dolo o colpa propria o del personale/terzi di cui si avvale). In tali casi, il risarcimento è commisurato al valore di mercato della cripto-attività al momento dell'evento dannoso e, salvo diversa previsione inderogabile di legge, sono esclusi danni indiretti o consequenziali.

14.2 La Società non risponde per eventi non imputabili o di forza maggiore, ivi inclusi, a titolo esemplificativo: malfunzionamenti su reti *blockchain*, vulnerabilità o *bug* di *smart contract* non controllati dalla Società, calamità naturali, conflitti, provvedimenti autoritativi imprevedibili. La Società adotta comunque ogni ragionevole misura per mitigare gli effetti dell'evento.

15. Reclami e risoluzione delle controversie

L'Utente può presentare reclami secondo il modulo standard reso disponibile sulla Piattaforma o via *e-mail*. La Società comunica entro 5 giorni lavorativi l'esito della ricevibilità e i tempi di gestione. Restano salvi i mezzi di tutela previsti dalla legge.

16. Durata, recesso e sospensione

16.1 Il Contratto ha durata a tempo indeterminato. Ciascuna Parte può recedere con preavviso di 30 giorni, fermo il completamento delle operazioni in corso e la restituzione delle disponibilità dell'Utente.

16.2 La Società può sospendere o interrompere i Servizi, anche senza preavviso, in caso di: violazioni contrattuali, frodi o tentativi di frode, impedimenti normativi/regolamentari, impossibilità di completare le verifiche antiriciclaggio, rischi

per la sicurezza o integrità dei sistemi, ordini o provvedimenti delle autorità.

17. Trattamento dei dati personali

17.1 La Società tratta i dati personali dell'Utente secondo l'informativa privacy disponibile sulla Piattaforma e in conformità alla normativa applicabile.

18. Legge applicabile e foro competente

18.1 Il presente Contratto è regolato dalla legge italiana.

18.2 Per qualsiasi controversia relativa a validità, interpretazione o esecuzione del Contratto è competente in via esclusiva il Foro di Perugia, fatto salvo il foro inderogabile del consumatore ove applicabile.

19. Disposizioni finali

19.1 La nullità o inefficacia di una clausola non inficia la validità del resto del Contratto, che resta efficace tra le Parti; le Parti sostituiranno

la clausola con altra valida e quanto più possibile equivalente.

19.2 La Società può modificare il Contratto per esigenze regolamentari, di sicurezza o organizzative, dandone comunicazione all'Utente con il preavviso richiesto dalla normativa applicabile. L'Utente può recedere senza oneri prima dell'efficacia delle modifiche.

19.3 La Società può cedere il Contratto e/o i diritti/obblighi a soggetti appartenenti al medesimo gruppo o a terzi in caso di operazioni straordinarie, informandone l'Utente. L'Utente non può cedere il Contratto senza consenso scritto della Società.

19.4 Il presente Contratto è accettato dall'Utente in via elettronica tramite la Piattaforma. Non sono previste firme autografe; l'accettazione online vale a tutti gli effetti di legge quale sottoscrizione. La data di conclusione è quella risultante dai sistemi informatici della Società.

ALLEGATO A

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

continuativamente 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 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.

ALLEGATO B

Descrizione dei rischi, tempi e costi delle operazioni di Staking

1. Descrizione del servizio di Staking

Lo Staking è un'attività mediante la quale l'Utente destina una determinata quantità di Cripto-attività, basate su meccanismi di consenso Proof of Stake, al fine di partecipare al processo di validazione delle transazioni sulla *blockchain* di riferimento. In cambio di tale partecipazione, l'Utente può ricevere ricompense sotto forma di Cripto-attività aggiuntive.

La Società offre il servizio di Staking esclusivamente con riferimento alle Cripto-attività e alle *blockchain* specificamente indicate sulla Piattaforma. L'elenco delle Cripto-attività ammesse allo Staking può essere aggiornato periodicamente dalla Società, con comunicazione preventiva agli Utenti.

La Società non presta servizi di Staking presso *liquidity pool* o meccanismi di finanza decentralizzata (DeFi) non riconducibili al modello di validazione PoS.

Cripto-attività ammesse allo Staking e commissioni applicabili

Alla data del presente Contratto, le Cripto-attività per le quali è disponibile il servizio di Staking e le relative commissioni applicate dalla Società sulle ricompense sono le seguenti:

- Ethereum (ETH): commissione sulle ricompense pari al 20%;
- Cardano (ADA): commissione sulle ricompense pari al 20%;
- Polkadot (DOT): commissione sulle ricompense pari al 20%;

2. BHP: commissione sulle ricompense pari allo 0%. Tempi delle operazioni di Staking

Attivazione dello Staking

L'attivazione dello Staking avviene entro un periodo variabile in funzione della specifica *blockchain*, generalmente compreso tra 1 e 30 giorni dalla conferma dell'istruzione da parte dell'Utente. I tempi effettivi dipendono dalle caratteristiche tecniche del protocollo di riferimento e dalle eventuali code di attivazione presenti sulla rete.

Periodo di lock-up

Alcune Cripto-attività in Staking sono soggette a un periodo di *lock-up* durante il quale non possono essere trasferite o prelevate. La durata del *lock-up* varia a seconda del protocollo *blockchain* ed è indicata sulla Piattaforma prima dell'adesione dell'Utente. Durante il periodo di *lock-up*, le Cripto-attività rimangono bloccate e non sono disponibili per altre operazioni.

Unstaking e periodo di unbonding

La richiesta di cessazione dello Staking (*unstaking*) comporta un periodo di *unbonding*, ossia un intervallo di tempo durante il quale le Cripto-attività cessano di generare ricompense ma non sono ancora disponibili per il trasferimento o il prelievo. Il periodo di *unbonding* varia

generalmente da 1 a 28 giorni a seconda del protocollo *blockchain* utilizzato. I tempi specifici sono indicati sulla Piattaforma.

Accredito delle ricompense

Le ricompense derivanti dallo Staking sono accreditate all'Utente secondo le tempistiche proprie di ciascun protocollo *blockchain*. L'accredito può avvenire su base giornaliera, settimanale o secondo altre periodicità specifiche del protocollo. Le modalità e le tempistiche di accredito sono indicate sulla Piattaforma.

3. Costi delle operazioni di Staking

Commissioni della Società

La Società applica una commissione sulle ricompense generate dallo Staking, il cui importo percentuale è indicato sulla Piattaforma e può variare in funzione della specifica Cripto-attività. Le ricompense sono accreditate all'Utente al netto di tale commissione.

Commissioni di rete (gas fee)

Le operazioni di Staking, *unstaking* e trasferimento delle ricompense possono essere soggette a commissioni di rete (*gas fee*) applicate dalla blockchain di riferimento. Tali commissioni sono variabili in funzione della congestione della rete al momento dell'operazione e sono a carico dell'Utente.

Assenza di costi nascosti

Non sono previsti costi aggiuntivi rispetto a quelli indicati nel presente Allegato e sulla Piattaforma. Eventuali modifiche alle condizioni economiche saranno comunicate preventivamente all'Utente.

Le commissioni specifiche applicabili a ciascuna Cripto-attività ammessa allo Staking, le eventuali soglie minime di partecipazione e le stime delle ricompense attese sono pubblicate e aggiornate periodicamente sulla Piattaforma nella sezione dedicata allo Staking.

4. Rischi delle operazioni di Staking

L'Utente prende atto e riconosce che le operazioni di Staking comportano rischi specifici, aggiuntivi rispetto a quelli connessi alla detenzione di Cripto-attività. Prima di aderire al servizio di Staking, l'Utente è tenuto a leggere attentamente e comprendere i seguenti rischi:

Rischio di slashing

In alcuni protocolli PoS, le Cripto-attività in Staking possono essere soggette a penalizzazioni (*slashing*) in caso di comportamenti scorretti o malfunzionamenti del nodo validatore. Lo *slashing* può comportare la perdita parziale o totale delle Cripto-attività in Staking. La Società adotta misure tecniche e operative per minimizzare il rischio di *slashing* ancorché tale rischio non può essere completamente eliminato.

Rischio di illiquidità

Durante i periodi di *lock-up* e *unbonding*, le Cripto-attività in Staking non sono disponibili per il trasferimento, la vendita o altre operazioni. L'Utente potrebbe non essere in grado di disporre delle proprie Cripto-attività in momenti di necessità o di opportunità di mercato.

Rischio di volatilità del valore

Il valore delle Cripto-attività in Staking può subire variazioni significative durante il periodo di Staking. Le ricompense ottenute potrebbero non compensare eventuali perdite di valore delle Cripto-attività sottostanti. L'Utente potrebbe subire perdite anche in presenza di ricompense positive.

Rischio di variazione delle ricompense

Le ricompense dello Staking non sono garantite e possono variare nel tempo in funzione di molteplici fattori, tra cui: le condizioni del protocollo *blockchain*, il numero di partecipanti allo Staking, le decisioni di *governance* della rete e le eventuali modifiche tecniche del protocollo. Le stime di rendimento indicate sulla Piattaforma hanno valore puramente indicativo e non costituiscono promessa di rendimento.

Rischio tecnologico e di protocollo

Le operazioni di Staking dipendono dal corretto funzionamento del protocollo *blockchain* sottostante. *Bug*, vulnerabilità, attacchi informatici, *hard fork* o altre modifiche tecniche del protocollo possono influire negativamente sullo Staking, sulle ricompense o sulla disponibilità delle Cripto-attività.

Rischio di controparte

Sebbene la Società adotti tutte le misure di sicurezza e operative previste dalla normativa applicabile, l'Utente è esposto al rischio che eventuali inadempimenti, malfunzionamenti o eventi avversi riguardanti la Società o i suoi fornitori tecnologici possano incidere sulle operazioni di Staking.

Rischio regolamentare

L'evoluzione del quadro normativo e regolamentare applicabile alle cripto-attività e ai servizi di Staking potrebbe comportare limitazioni, divieti o modifiche alle condizioni del servizio, anche con effetto sulle operazioni in corso.

Rischio fiscale

Le ricompense derivanti dallo Staking possono essere soggette a imposizione fiscale secondo la normativa applicabile. L'Utente è responsabile degli adempimenti fiscali connessi alle ricompense ricevute e si consiglia di consultare un consulente fiscale qualificato.

5. Presidi adottati dalla Società

La Società adotta misure tecniche e organizzative volte a minimizzare i rischi connessi alle operazioni di Staking, tra cui:

- (i) la selezione di validatori affidabili e con comprovata esperienza;
- (ii) il monitoraggio continuo delle performance dei nodi validatori;
- (iii) l'implementazione di sistemi di *alert* per anomalie operative;
- (iv) la diversificazione tra più validatori ove tecnicamente possibile;
- (v) procedure di gestione degli incidenti e piani di continuità operativa.

La Società effettua un monitoraggio costante dei protocolli *blockchain* utilizzati per lo Staking e si riserva di sospendere o interrompere il servizio su determinate Cripto-attività qualora emergano rischi significativi per la sicurezza o l'integrità delle operazioni.

6. Informativa e trasparenza

Le informazioni contenute nel presente Allegato B, unitamente ai dettagli specifici relativi a ciascuna Cripto-attività ammessa allo Staking (tempi, costi, ricompense stimate, rischi specifici), sono pubblicate e rese accessibili in modo chiaro e comprensibile sul sito *web* della Società all'indirizzo <https://www.cryptosmart.it>, nella sezione dedicata ai servizi di Staking.

La Società si impegna a mantenere aggiornate le presenti informazioni sul sito *web* e a comunicare tempestivamente agli Utenti eventuali modifiche significative alle condizioni del servizio di Staking, ai rischi connessi o alle Cripto-attività ammesse.

L'Utente può in ogni momento consultare sulla Piattaforma il dettaglio delle proprie posizioni in Staking, lo stato delle operazioni, le ricompense maturate e accreditate, nonché le informazioni aggiornate su tempi e costi applicabili.

L'Utente riconosce che le ricompense dello Staking non sono garantite e che le stime di rendimento indicate sulla Piattaforma hanno carattere meramente indicativo.

L'Utente conferma di comprendere che le Cripto-attività in Staking potrebbero non essere immediatamente disponibili in ragione dei periodi di *lock-up* e *unbonding* applicabili e di accettare tale limitazione.