

DIGITAL ASSET RISK MANAGEMENT POLICY

HALCYON SUPER HOLDINGS BV

Status: FINAL

Version: 1.0

Date: 11 Nov 2025

Change/Approval History

Version	Date	Author	Approver	Notes
0.1	03 Nov 2025	LT		First Draft
1.0	11 Nov 2025	LT	AM/CC	First Draft Approved

TABLE OF CONTENTS

SECTION 1. INTRODUCTION & POLICY STATEMENTS	3
1.1 INTRODUCTION	3
1.2 BREACHES AND EXCEPTION HANDLING	3
1.3 ADMINISTRATION	4
SECTION 2. ROLES AND RESPONSIBILITIES	5
2.1 SENIOR MANAGEMENT	5
2.2 PAYMENTS AND CUSTODY MANAGEMENT TEAM	5
2.3 ASSET MANAGEMENT TEAM	5
2.4 FINANCE OPERATIONS TEAM	6
2.5 COMPLIANCE TEAM	6
SECTION 3. WALLET ARCHITECTURE	7
3.1 HOT WALLET	7
3.2 WARM WALLET	7
3.3 COLD WALLET	7
3.4 ASSETS FLOW	7
SECTION 4. WALLET MANAGEMENT	10
4.1 CUSTOMER ASSETS SEGREGATION	10
4.2 CUSTOMER DA HANDLING	10
4.3 COLD STORAGE MANAGEMENT	11
4.4 HOT AND WARM WALLET MANAGEMENT	12
4.5 HARD FORKS AND AIRDROPS HANDLING	14
4.6 CUSTODY TESTING AND DEPLOYMENT	14
4.7 RECONCILIATION PROCESS	14
4.8 SUPPORTED DA SELECTION, ONGOING REVIEW AND DEPRECIATION	14
SECTION 5. FRAUD AND SECURITY MONITORING	16
5.1 BLOCKCHAIN ANALYTICS	16
5.2 BLOCKCHAIN ATTACKS HANDLING	16
SECTION 6. DA VOLATILITY MANAGEMENT	17
APPENDIX 1. DEFINITIONS	18
APPENDIX 2. WITHDRAWAL HOT WALLET MINIMUM BALANCES AND TOP UP ALERT THRESHOLD	19

SECTION 1. INTRODUCTION & POLICY STATEMENTS

1.1 INTRODUCTION

- (a) Halcyon Super Holdings BV, is a company incorporated with limited liability in Curacao, (“Halcyon” or the “Company”). It owns and operates cloudbet.com - a gaming website offering an online sportsbook and casino where customers can place bets primarily in digital assets (“Crypto” or “DA”). Halcyon is licensed by the Curacao Gaming Authority (“CGA”) under license number OGL/2024/328/0599.
- (b) The purpose of this document is to establish the governance framework for the secure management of Halcyon controlled DA wallets, including the safe custody and transfer of DAs by Halcyon. This ensures operational integrity and ensures the safekeeping of customer assets.
- (c) Implementation of the standards and controls set out in this Policy is essential to effectively managing DA custody risks and ensuring the safekeeping of DAs. Failure to implement these controls can result in irreversible asset loss, unauthorized access to wallets, compromised private keys, and significant financial and reputational harm to the Company.
- (d) The Policy applies to all activities of Halcyon, including its subsidiaries, and forms part of Halcyon’s governance framework. It is applicable to all staff of the Company, inclusive of all officers, directors, managers, administrators and support staff and is not limited to individuals working under a contract of employment but also includes temporary/contract staff and consultants.
- (e) Non-compliance with this Policy is a serious matter that may lead to disciplinary action, up to and including dismissal.

1.2 BREACHES AND EXCEPTION HANDLING

- (a) Any breaches of this Policy must be reported as soon as possible to the Compliance Officer (“CO”). The CO will be responsible for notifying senior management, as well as any regulatory reporting or mitigation plans resulting from the breach.
- (b) Applications for exceptional handling regarding this Policy may be made to the CO. Applications must be made in writing and outline the proposed approach, including any risk mitigation. As a general rule such applications will only be approved in rare circumstances, where there is no resulting breach of local regulatory requirements and risk mitigation is in place.

1.3 ADMINISTRATION

- (a) This Policy is owned by the CO and will be reviewed at least annually or more frequently when there are significant regulatory or business changes that will impact the Company.
- (b) This Policy must be reviewed and approved by senior management prior to implementation. All subsequent material amendments to this Policy will similarly require senior management review and approval.
- (c) This Policy is effective as of the date set forth in this document.
- (d) This Policy has been communicated to all relevant employees and all questions regarding this Policy should be directed at the CO, who can be contacted at compliance@cloudbet.com.

SECTION 2. ROLES AND RESPONSIBILITIES

2.1 SENIOR MANAGEMENT

- (a) The ultimate responsibility for ensuring the Company's policies, procedures and controls for the secure management of Halcyon controlled DA wallets, including the safe custody and transfer of DAs by Halcyon, remains with the Company and its senior management team.
- (b) The senior management team is responsible for the implementation of this Policy, in particular:
 - (i) Approving this Policy and ensuring it is reviewed on an annual basis and any changes are reported to the Board for approval;
 - (ii) Identifying, assessing and effectively mitigating the risks associated with processing DA transfers and the safe custody of DA;
 - (iii) Promoting and enforcing high standards of integrity;
 - (iv) Ensuring that all employees responsible for carrying out the standards in this Policy are adequately trained and provided with sufficient resources;
 - (v) Ensuring that relevant appropriate controls and monitoring procedures are in place;
 - (vi) Establishing mechanisms for appropriate escalation of issues;
 - (vii) Ensuring that independent testing is carried out to assess the effectiveness of the wallet management and custody framework; and
 - (viii) Reacting promptly and effectively to any issues that arise.

2.2 PAYMENTS AND CUSTODY MANAGEMENT TEAM

- (a) This team is responsible for daily operations involving customer assets, including:
 - (i) Deposit and withdrawal processing;
 - (ii) Wallet management, custody and security oversight;
 - (iii) Blockchain monitoring and transaction verification;
 - (iv) Payment gateway and provider management;
 - (v) Reconciliation and financial controls;
 - (vi) Customer support for payment related issues;
 - (vii) Fee optimization; and
 - (viii) System maintenance and incident response.

2.3 ASSET MANAGEMENT TEAM

- (a) This team is responsible for ensuring the sound and effective management of DA deposited onto the platform, including:
 - (i) Treasury, liquidity and reserve management; and

- (ii) Financial planning, portfolio diversification and investment strategy;

2.4 FINANCE OPERATIONS TEAM

- (a) This team is responsible for managing the Company's trading risk and settlements, as well as the manual withdrawal review workflow in order to minimize fraudulent activity on the Platform.

2.5 COMPLIANCE TEAM

- (a) This team is responsible for ensuring that the Company's processes for wallet management and custodial DA meet all applicable regulatory standards, as well as ensuring adherence to external reporting requirements.
- (b) The team is also responsible for reviewing transactions flagged by the Company's blockchain analytics tool and filing unusual transaction reports ("UTR") to the Curacao Financial Intelligence Unit ("FIU"), as necessary.

SECTION 3. WALLET ARCHITECTURE

3.1 HOT WALLET

- (a) These wallets are designed for high availability and swift transactions. They are connected to the internet, so the private keys required to sign transactions are always online. Transactions can be created and recorded on the blockchain in an automated way, without the need for human involvement.
- (b) The Company utilizes hot wallets to process customer withdrawals. The Fireblocks wallet infrastructure and platform is used by the Company to securely manage its hot wallet set up.

3.2 WARM WALLET

- (a) These wallets are designed to combine the transaction speed of hot wallets with an additional level of security, similar to cold wallets. The keys are held online and transactions can be created automatically, but human involvement is needed to sign the transaction and send it to the blockchain.
- (b) The Company utilizes warm wallets to hold the majority of customer assets (i.e. Treasury Wallets), as well as its own assets (i.e. Accounting Wallets). The Fireblocks wallet infrastructure and platform is used by the Company to securely manage its warm wallet set up.

3.3 COLD WALLET

- (a) These wallets are designed to maximise security at the expense of access speed. The private keys are stored completely offline on a device that is not connected to the internet and that needs a password/PIN to open it. Human involvement is required to digitally sign each transaction so it can be broadcasted and recorded on the blockchain.
- (b) The Company maintains its Bitcoin (“BTC”) reserves that it does not need for its day-to-day operations in deep cold storage. The Company manages its cold wallet infrastructure internally, with the device and sharded private keys kept in separate safety deposit boxes.

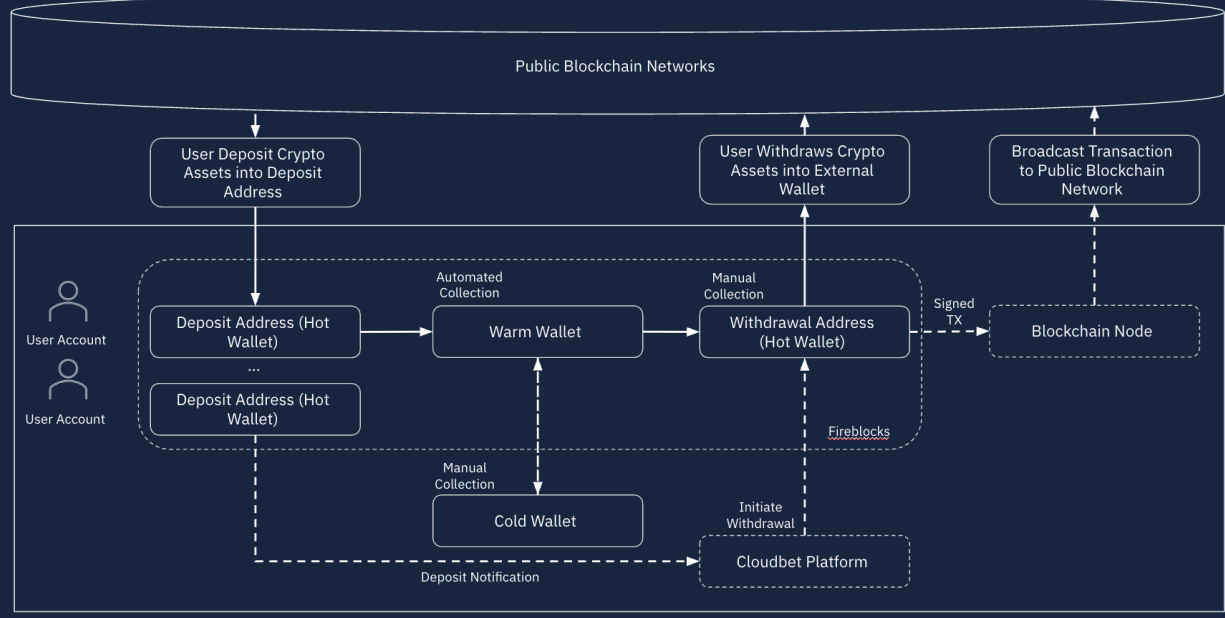
3.4 ASSETS FLOW

- (a) Once a customer has completed registration, a unique blockchain address will be created and allocated to the customer for each of the supported blockchains (these may be updated from time to time for security reasons, but the customer will only have one unique blockchain address

per blockchain at any one time). These addresses will act as the customers' dedicated individual deposit addresses.

- (b) When the customer makes a deposit from an external blockchain address, Fireblocks will monitor the deposit address and notify Cloudbet's internal system to credit the balance to the customer's account when a sufficient number of confirmations of the blockchain transaction is noted.
- (c) The balance held in the deposit addresses will automatically be swept to treasury warm wallets on a scheduled basis. This automated sweep can be reconfigured anytime by the Custody System Manager or the CFO.
 - (i) Depending on operational needs, funds can be manually transferred in and out of the cold wallet by the CEO, CFO and Senior Marketing Executive (i.e. it needs a multi-signature from all 3 to perform a transaction out of the cold wallet).
- (d) The majority of customer funds and day-to-day working capital is held in the treasury warm wallet. The withdrawal hot wallets are topped up with set minimum balances and when these balances go below a certain threshold, an alert will be triggered, and the Finance Team or Custody System Manager will be able to perform the top up from the treasury warm wallet, subject to two approvals from either the CFO, CEO, CPO or Senior Marketing Executive (see Appendix 2 for the withdrawal hot wallet minimum balances and alert top up levels).
- (e) When a customer requests for a withdrawal on the Cloudbet platform, the Company will perform all mandatory risk control checks. Once approved, the Company will send the customer assets to their external wallet from a hot wallet.
- (f) The Company will charge customers a withdrawal fee as part of the withdrawal process, in order to cover gas fees.
- (g) A high level overview of the customer asset flow and Company's customer asset custody architecture can be found in the diagram below:

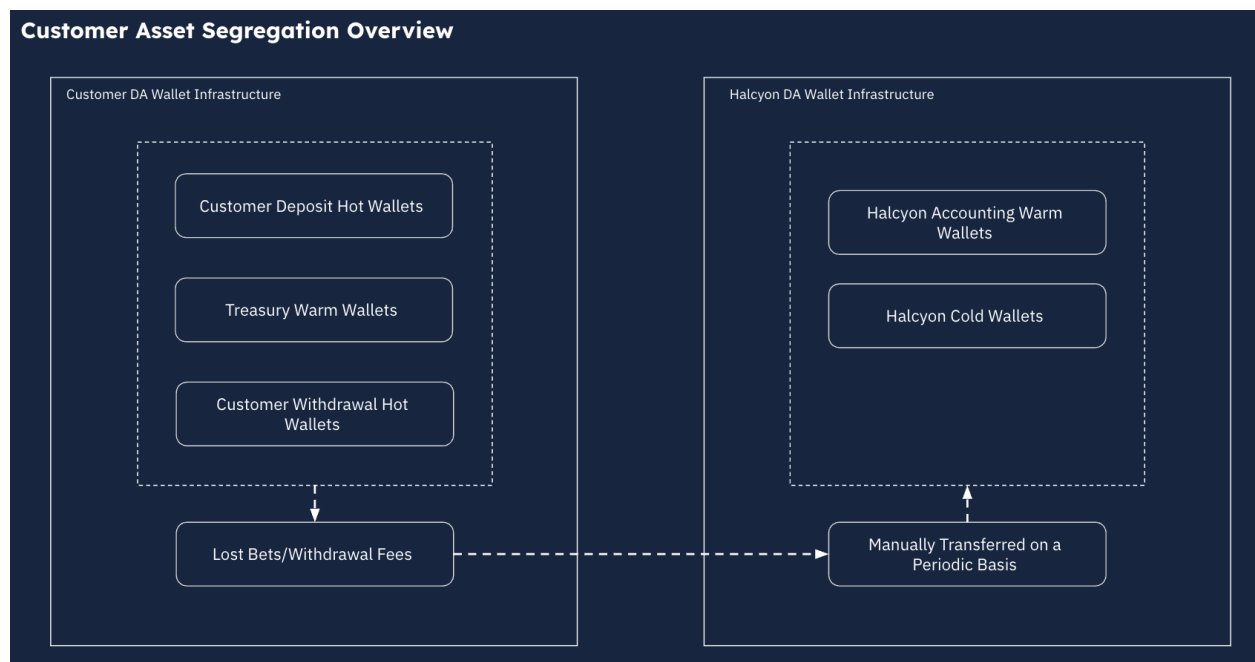
Customer Asset Custody Architecture Overview



SECTION 4. WALLET MANAGEMENT

4.1 CUSTOMER ASSETS SEGREGATION

- (a) Company assets are segregated from customer assets and working capital needed to match and pay out customer bets.
- (b) Lost bets and withdrawal fees are transferred to the Company's Accounting Warm Wallets manually on a periodic basis. The Company also maintains its BTC reserves in its Cold Wallet infrastructure for added security.
- (c) A high level overview of the Company's customer asset segregation architecture can be found in the diagram below:



4.2 CUSTOMER DA HANDLING

- (a) Deposits:
 - (i) Fireblock's helps the Company to monitor for customer deposits into the customer deposit hot wallets. When a transaction is identified, the Company will wait for a sufficient number of confirmations to ensure that the transaction is final and legitimate. Once sufficient confirmations are received, the customer's account on Cloudbet is credited and an automated email notification confirming the deposit is sent to the customer.

- (ii) The transaction will be screened and risk-profiled by the Company's blockchain analytics tool (i.e. Chainalysis) as part of the transaction monitoring process (detailed in Halcyon's AML Policy).

(b) Withdrawals:

- (i) Customers are able to initiate withdrawal requests for their DA's at any time. If the customer has turned on two-factor authentication ("2FA"), they will be required to complete this as part of the withdrawal request process. The request is then queued for processing.
- (ii) To ensure the legitimacy of each transaction, the Company conducts the following checks:
 - (1) Verification of sufficient available balance for the withdrawal.
 - (2) Assessment against predefined thresholds and tags - where thresholds are exceeded or users are tagged for manual withdrawal, manual review and approval will be required before the transaction is processed.
 - a) Withdrawals over EUR 20k require Sports Team Approval, Casino Team Approval and CFO approval.
 - b) Withdrawals over EUR 50k require additional CFO or CEO approval within the fireblocks application.
 - c) Manual withdrawal review tags can be placed by the Sports Team, Casino Team or Compliance Team. These tags will trigger a manual review of the withdrawal regardless of the threshold amount.
 - d) The transaction will be screened and risk-profiled by the Company's blockchain analytics tool (i.e. Chainalysis) as part of the transaction monitoring process (detailed in Halcyon's AML Policy).
- (iii) Once approved, the transaction will be processed and broadcasted to the public blockchain network. The withdrawal fee will also be deducted from the customers' account and an email notification will be sent to the customer confirming the withdrawal.

4.3 COLD STORAGE MANAGEMENT

- (a) The Company maintains its BTC reserves that are not needed for day-to-day operations in deep cold storage. The private key for the cold wallet is sharded three ways between the CEO, CFO and Senior Marketing Executive (i.e. the 24 word mnemonic phrase is split into 3 sets of 8 words) and

kept in separate safety deposit boxes along with the cold storage device that is protected with a password.

- (b) The CEO, CFO and Senior Marketing Executive all need to be present and multi-sign a transaction with their part of the private key in order to process a transaction from the cold wallet.

4.4 HOT AND WARM WALLET MANAGEMENT

- (a) The Company has engaged Fireblocks to help create and manage the Company's hot and warm wallet infrastructure. Fireblocks wallet infrastructure is a secure, institutional-grade platform built on multi-party computation ("MPC") and offered as a wallet-as-a-service ("Waas"). It enables the Company to securely custody, manage, and transfer DAs by splitting the private key into three parts, which are stored in different locations and never come together even during the transaction signing process. This eliminates the single point of failure associated with a single private key and makes it difficult for bad actors to reconstruct the full private key and interact directly with the blockchain, as they would need to compromise three separate systems independently.
- (b) The Fireblocks application also allows the Company to set its own policies and rules around who can request transactions, who needs to approve transactions and where transactions can be automated.
- (c) Hot wallets are utilized by the Company to receive customer deposits and process customer withdrawals.
 - (i) Deposit Hot Wallet Transactions:
 - (1) Transactions from the customer deposit wallets to the treasury warm wallets are programmed to automatically sweep funds on a periodic basis when certain thresholds are met. These transactions are signed by an API user hosted by the Company and two Fireblocks co-signers hosted on separate cloud servers. The settings can be adjusted by the Custody System Manager or CFO through the Fireblocks application.
 - (2) The Finance Team also has the ability to manually transfer funds from the deposit wallets to the treasury wallets. Their requests are subject to two approvals from either the CEO, CFO, CPO or Senior Marketing Executive. Once approved, the Custody System Manager or CFO will sign the transaction through the Fireblocks app, along with two Fireblocks co-signers hosted on separate cloud servers also signing the transaction.

- (3) The authorisation settings for the Deposit Hot Wallets restricts the API or human user to process transactions only to the Treasury Warm Wallet. This set up manages the risk around if these wallets were ever compromised, the bad actor would only be able to send funds to the Treasury Warm Wallet and not to an external wallet address outside of the Company's wallet infrastructure.
- (ii) Withdrawal Hot Wallet Transactions:
 - (1) Once withdrawals are approved in the Company's internal system, withdrawal transactions are automated and processed from the withdrawal address hot wallets. These transactions are signed by an API user hosted by the Company and two Fireblocks co-signers hosted on separate cloud servers. The settings can be adjusted by the Custody System Manager or CFO through the Fireblocks application.
 - (2) The Withdrawal Hot Wallets have minimal balances and are separated from the Treasury Warm Wallets because if these wallets were compromised, the bad actor would only be able to drain the funds in the Withdrawal Hot Wallets and would not be able to access any other of the Company's funds.
- (d) Warm wallets are utilized by the Company to hold the majority of customer assets along with the day-to-day working capital used for matching bets and paying out winners.
 - (i) Transactions out of the warm wallet can only be processed manually by the Finance Team or Custody System Manager and are subject to two approvals from either the CEO, CFO, CPO or Senior Marketing Executive. Once approved, the Custody System Manager or CFO will sign the transaction through the Fireblocks app, along with two Fireblocks co-signers hosted on separate cloud servers also signing the transaction.
 - (1) Where the CEO, CFO, CPO or Senior Marketing Executive processes a transaction, only one approval is needed from another of the three officers who did not process the transaction.
 - (ii) The authorisation settings for the Deposit Hot Wallets restricts human users to processing transactions only to the Halcyon Accounting Wallet or Withdrawal Hot Wallets. This helps to control the risk around if these wallets were ever compromised, the bad actor would only be able to send funds from these wallets to the Halcyon Accounting Wallet or Withdrawal Hot Wallets and not to an external wallet address outside of the Company's wallet infrastructure.

4.5 HARD FORKS AND AIRDROPS HANDLING

- (a) The Custody System Manager and Payments Team will monitor for any hard fork or airdrop announcements.
- (b) Where there is a scheduled hard fork or airdrop tied to a supported DA, the Company will handle them on a case-by-case basis.

4.6 CUSTODY TESTING AND DEPLOYMENT

- (a) The Custody System Manager and Payments Team are responsible for managing the Fireblocks integration and payments related systems.
- (b) All payment system deployments and updates go through rigorous testing before they are deployed. This is a critical phase of system development that involves verifying the system's functionality and then transitioning it to a live, operational state.

4.7 RECONCILIATION PROCESS

- (a) The Finance Team is responsible for the monthly reconciliation process. The reconciliation process is a critical component for ensuring the accuracy and integrity of customer assets and transactions. It encompasses multiple layers of checks and balances to align blockchain transactions with internal ledger entries.

4.8 SUPPORTED DA SELECTION, ONGOING REVIEW AND DEPRECATON

- (a) The Company maintains a list of supported DA's for customer deposits and withdrawals based on a set evaluation criteria. Potential new DA's are assessed against several key factors including blockchain security and stability, market liquidity and trading volume, regulatory status and compliance considerations (i.e. Chainalysis compatibility), technical integration complexity and customer demand. The Custody System Manager and CTO are jointly responsible for evaluating proposed additions to the supported asset list and recommending approval or rejection based on these criteria. All new DA additions must undergo thorough technical testing before being made available to customers.
- (b) The Custody System Manager and CTO conduct periodic reviews of all supported DA's to assess whether continued support remains appropriate. This review evaluates each asset against current risk metrics including blockchain security incidents or vulnerabilities, declining transaction volumes or customer usage, material changes in regulatory treatment, technical issues or network instability, and liquidity constraints. Where a DA no longer meets the Company's risk standards or demonstrates negligible customer usage, the Custody System Manager and CTO will recommend deprecation. The deprecation process includes providing

adequate notice to affected customers, establishing a timeline for final deposits and withdrawals, and ensuring all customer holdings are safely withdrawn or converted before support is fully discontinued.

SECTION 5. FRAUD AND SECURITY MONITORING

5.1 BLOCKCHAIN ANALYTICS

- (a) Blockchain analytics screening is a key feature of the Company's AML/CFT program and is overseen by the CO. The Company utilizes a third party blockchain analytics screening tool (i.e. Chainalysis) to screen all DA deposits and withdrawal transactions into and out of the Company's wallet infrastructure. This allows the Company to detect transactional activity to or from risky service categories, such as sanctioned entities, terrorist financing and child abuse material.
- (b) Alerts are given a risk score based on counterparty risk exposure, the transaction amount and whether the transaction exhibits direct or indirect exposure.
- (c) Any alerts are reviewed by the CO.

5.2 BLOCKCHAIN ATTACKS HANDLING

- (a) The Custody Systems Manager and the CTO are responsible for preventing, detecting and responding to any blockchain attacks. In order to achieve this, they implement preventative measures focusing on network security, consensus mechanisms, and node diversity. They also conduct regular reviews of the payments systems and operations to incorporate learnings from past incidents and changes in the blockchain threat landscape.

SECTION 6. DA VOLATILITY MANAGEMENT

- (a) To manage the volatility of DA's, the Company only allows customers to bet in the currency that they deposit into the Platform. This means if a customer deposits BTC, they will only be allowed to bet in BTC. They are also not allowed to swap their BTC into another DA on the Platform.
- (b) When a bet is placed, the Company reserves an amount of its working capital in the bet currency equal to the potential payout. For example, if a customer bets 1 BTC at even money (with a potential payout of 1 BTC), the Company will hold an additional 1 BTC from its working capital in reserve until the bet is settled. This ensures that the Company is not subject to any price movement risks between the time that the bet is placed and the time that it is settled.

APPENDIX 1. DEFINITIONS

(a) The following terms shall have the following meaning:

- (i) “2FA” means two-factor authentication;
- (ii) “AML” means Anti-Money Laundering;
- (iii) “AML/CFT Regulations” means the Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction issued by the Curacao Gaming Authority;
- (iv) “BTC” means Bitcoin
- (v) “CFT” means Counter Financing Terrorism;
- (vi) “CGA” means Curacao Gaming Authority;
- (vii) “CO” means the formally designated Compliance Officer of the Company;
- (viii) “Company” means Halcyon Super Holdings BV, and “Halcyon” shall have the same meaning;
- (ix) “Cryptocurrency / Cryptocoin / Crypto / Digital Asset / DA / Digital Currency / Virtual Asset / Virtual Currency” means a digital representation of value that can be digitally traded and functions as (1) a medium of exchange, and/or (2) a unit of account, and/or (3) a store of value, but does not have legal tender status (i.e. when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction and fulfills the above functions only by agreement within the community of users of the cryptocurrency;
- (x) “FIU” means Curacao Financial Intelligence Unit;
- (xi) “MPC” means multi-party computation;
- (xii) “UTR” means Unusual Transaction Report; and
- (xiii) “WaaS” means wallet-as-a-service.

APPENDIX 2. WITHDRAWAL HOT WALLET MINIMUM BALANCES AND TOP UP ALERT THRESHOLD

Coin	Network	Alert will be triggered when balance goes below (USD equivalent)	Refill Amount (USD equivalent)
BTC	Bitcoin	500,000	1,000,000
ETH	Ethereum	50,000	200,000
USDT	Ethereum	70,000	300,000
USDT	Tron	70,000	300,000
BUSD	BSC	10,000	10,000
ADA	BSC	8,000	8,000
AVAX	BSC	8,000	8,000
EOS	EOSIO	8,000	8,000
ETC	Ethereum Classic	8,000	8,000
DOGE	BSC	8,000	8,000
DOT	BSC	8,000	8,000
DAI	BSC	8,000	8,000
FTM	BSC	8,000	8,000
LINK	BSC	8,000	8,000
LTC	BSC	8,000	8,000
MATIC	BSC	8,000	8,000
SHIB	BSC	8,000	8,000
SOL	BSC	8,000	8,000
stETH	Ethereum	8,000	8,000
UNI	BSC	8,000	8,000

UNI	Ethereum	8,000	8,000
ZEC	Zcash	6,000	6,000
All other altcoins	All other chains	15,000	30,000