

Cryptocurrency Risk Policy — Slotbox N.V.

Field	Detail
Document Title	Cryptocurrency Risk Policy
Operator	Slotbox N.V.
Version	V2
Effective Date	July 2026
Review Date	June 2027
Classification	Confidential
Owner	Compliance Officer / MLRO
Approved By	Board of Directors — Slotbox N.V.
Regulatory Jurisdiction	Curaçao (CGA / LOK)

1. Introduction and Purpose

This Cryptocurrency Risk Policy (“the Policy”) establishes the Company’s framework for managing the legal, operational, financial, and reputational risks arising from the acceptance and processing of cryptocurrency as a payment channel in connection with its licensed gaming activities.

This Policy does not replace or limit any other legal, regulatory or licensing obligations. The Company ensures full compliance with all applicable registration, licensing, reporting and other regulatory requirements.

Fiat-operator model — The Company operates as a fiat-based operator. Cryptocurrency deposits are converted to euro by the Company’s payment service providers (PSPs) at the point of receipt; the resulting fiat value is credited to the player’s gaming balance, which is held and managed in fiat currency. No cryptocurrency is held on the player’s behalf following the initial conversion. All gaming activity — including betting, limits, and bonus calculations — is conducted in fiat. The Company accepts cryptocurrency as a deposit channel and, in limited cases, as a withdrawal method; **it is not a crypto casino**. This distinction is central to the Company’s risk profile and shapes the controls set out in this Policy.

2. Scope

This Policy applies to:

- All business lines, systems, and processes of Slotbox N.V. and any subsidiaries, branches, agents, or third-party service providers operating on its behalf.
- All directors, officers, employees, contractors, and compliance personnel of the Company.
- All cryptocurrency deposits and on-platform credits processed by or on behalf of players.
- All Virtual Asset Services Providers (VASPs), payment processors, and technology partners engaged in relation to cryptocurrency functionality.

This Policy does not replace the Company's general AML/CFT, Customer Acceptance, or Data Protection Policies. It supplements and cross-references those documents

3. Regulatory and Legal Framework

3.1 CGA / LOK Regime

This Policy is submitted to the CGA as a standalone cryptocurrency risk governance document, forming an integral part of the Company's broader AML/CFT Compliance Programme in accordance with:

1. The CGA Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (effective 9 January 2025; mandatory compliance from 10 April 2025);
2. The National Ordinance on Identification when Rendering Services (NOIS, N.G. 2017 no. 92);
3. The National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017 no. 99);
4. The Sanctions National Ordinance (N.G. 2014, no. 55) and Kingdom Sanction Act (N.G. 2016, no. 54); and
5. FATF Recommendations 15 (New Technologies) and 16 (Wire Transfers / Travel Rule), and the FATF 2021 Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs; Caribbean Financial Action Taskforce (CFATF) standards applicable to Curaçao.

3.2 FATF Recommendation 15 and Virtual Assets

FATF R.15 requires AML/CFT measures to be applied to virtual asset activities and VASPs. The Company commits to implementing the FATF risk-based approach to virtual assets at the standard applicable to equivalent financial institutions.

4. Governance and Accountability

4.1 Board of Directors

The Board approves this Policy, as it relates to virtual assets. The Board receives at minimum annual updates on crypto-related AML/CFT risks, enforcement trends, and programme effectiveness or when any material changes are made.

4.2 Compliance Officer / MLRO

The MLRO — in a dual role as Compliance Officer — is a senior officer independent of gaming operations holding primary responsibility for day-to-day oversight of this Policy. The MLRO responsibilities specific to cryptocurrency include:

- Maintaining and annually reviewing the Company's crypto-specific Business Risk Assessment.
- Approving or escalating high-risk crypto player relationships and EDD decisions.

- Reviewing and filing Unusual Transaction Reports (UTRs) with FIU Curaçao via goAML.
- Liaising with the CGA and FIU Curaçao regarding crypto-related compliance inquiries.
- Ensuring annual crypto-specific AML/CFT training is delivered.
- Maintaining records for the minimum statutory retention periods.

4.3 Payments Team

The Payments team is responsible for operational implementation of crypto-specific controls.

4.4 Third Parties

Any VASP, payment processor, or technology provider engaged in relation to cryptocurrency functionality must contractually agree to comply with standards equivalent to this Policy. The Company reserves the right to audit or terminate third-party relationships where compliance standards are not met.

5. Permitted Cryptocurrencies and Prohibited Assets

5.1 Permitted Assets

The Company accepts the following cryptocurrencies, subject to the controls set out in this Policy:

Cryptocurrency	Primary VASP
Bitcoin	Bitpace
Ripple	Bitpace
Tether	Bitpace
USD Coin	Bitpace
Litecoin	Bitpace
Binance Coin	Bitpace
Link	Bitpace
Solana	Bitpace

Before any new asset is added to the permitted list, the MLRO completes a written technological risk assessment (per CGA AML Regulations §II.3).

5.2 Prohibited Assets and Transactions

The following asset types and transaction patterns are unconditionally prohibited:

- **Privacy coins:** Monero (XMR), Zcash (ZEC) and Dash.

- **Meme coins:** DOGE, SHIB and PEPE.
- Wrapped tokens of unknown origin.
- Deposits routed via sanctioned mixers/tumblers or wallets on sanctions lists.

6. Wallet, Custody and Exchanges Management and VASP Requirements

6.1 Company Wallets

The Company maintains corporate cryptocurrency wallets exclusively in the name of Slotbox N.V. The use of personal or UBO wallets is prohibited.

6.2 Player Wallet Attribution

Each player depositing cryptocurrency must provide the originating wallet address. The Company records and stores all wallet addresses associated with each player account.

6.3 Fiat Conversion, Withdrawal Process, and Same-Wallet Rule

Fiat conversion (standard model)

When a player deposits cryptocurrency, the Company's PSP converts the crypto to fiat currency at the point of receipt. The converted fiat value is credited to the player's gaming balance. All balances, play, and transactions are denominated in fiat (Euro). No cryptocurrency is held on the player's behalf at any point following the initial conversion. Withdrawals default to fiat rails via the player's registered payment methods.

Same-wallet rule — direct crypto withdrawal scenarios

Where a player specifically requests a cryptocurrency withdrawal, that withdrawal must be directed to the same wallet address and in the same cryptocurrency as was used for the original deposit. Where a different wallet is required, approval is needed, the alternative wallet must be screened and attributed to the player's verified identity, and the reason documented.

6.4 VASP Due Diligence

The Company processes cryptocurrency transactions via VASPs, who are required to apply AML/CFT screening to all transactions.

Prior to engaging any VASP (including renewals), the MLRO must complete due diligence covering licence status, AML/CFT policies and controls, sanctions screening capabilities, Travel Rule compliance, and ongoing monitoring.

7. Blockchain Analytics and Chain-Level Screening

7.1 Current Screening Arrangement

The Company currently processes all cryptocurrency transactions via Bitpace, which applies blockchain analytics screening.

7.2 Screening at Deposit & Withdrawal

Cryptocurrency deposits are screened before funds are credited to the player's gaming balance. Prior to processing any cryptocurrency withdrawal, the destination wallet address is screened.

7.3 Unhosted Wallet Due Diligence

Where a player uses an unhosted wallet, the Company must take reasonable steps to attribute it to the player's verified identity, including requiring cryptographic proof of ownership (message signing). If attribution cannot be established, the Company may refuse deposits from that wallet.

8. Customer Due Diligence for Cryptocurrency Users

CDD is undertaken in line with the Company's Customer Acceptance and Risk Assessment Policy.

9. Transaction Monitoring and Unusual Transaction Reporting

9.1 Monitoring Rules

Customer accounts are reviewed periodically based on risk level:

Risk Level	Review Frequency
High Risk	Annually
Medium Risk	Every 2 years
Low Risk	Every 3 years

Notwithstanding that the standard account review cycle is annual, this is supplemented by daily transaction monitoring applied across all customers. Given the heightened risk associated with cryptocurrency transactions, enhanced monitoring is applied to this method. Deposits and withdrawals are reviewed on an ongoing basis as they occur.

Periodic reviews include scrutiny of transactional activity, IP addresses, identification documents, and expected customer behavioural assessment. Reviews are also triggered by events outside the periodic schedule, including:

- **Suspicious transactions:** High velocity, no apparent reason, high-risk jurisdiction transfers, same patterns between customers, amounts inconsistent with known income.
- **Suspicious customer behaviour:** Refusal to provide information, requesting reporting thresholds, linked accounts, adverse media, account closure after information request.
- **Single Transaction of NAf 5,000 (€2,500):** Any single transaction of this amount must be reported to FIU Curaçao via goAML within 48 hours. No suspicion is needed — it is a regulatory requirement.
- **High-value transactions:** Transactions exceeding internal EDD thresholds.

9.2 Alert Review and UTR Filing

Alerts are reviewed by the compliance team and escalated to the MLRO as soon as reasonably possible. UTRs are filed with FIU Curaçao without delay via goAML in English. All UTR decisions are documented.

10. Sanctions Compliance

All players are screened against UN and EU sanctions lists at onboarding and on an ongoing basis. The Company does not conduct business with any sanctioned person or entity. All cryptocurrency wallet addresses are screened against OFAC SDN and relevant sanctions lists. A match triggers automatic transaction rejection, account freeze, immediate UTR filing, and MLRO notification, per the Curaçao Process for the Freezing of Resources (N.G. 2016).

11. Record Keeping

The Company retains all records relating to cryptocurrency activity for a minimum of:

- **Five years** for AML/CFT records (CDD, EDD, UTRs, wallet screening results, compliance decisions).
- **Seven years** for player account data and transaction records.

Records include transaction details (hash, wallet addresses, asset, amount, Naf equivalent, date/time), blockchain analytics results, CDD/EDD documentation, UTRs, VASP due diligence records, and staff training records. Records are stored in a secure, access-controlled system and are available to the CGA or FIU Curaçao upon lawful request.

12. Staff Training and Awareness

AML/CFT training with cryptocurrency-specific content is delivered to all relevant personnel at least annually, or whenever there is a material regulatory or operational change. Content covers virtual asset ML/TF risks, CGA crypto requirements, red flags (structuring, mixing, chain-hopping), UTR filing via goAML, and the prohibition on tipping off. Training records are retained for five years.

13. Version History

Version	Date	Changes
1.0	June 2026	First Draft
2.0	July 2026	Broadened scope as group policy and aligned with Group AML/CFT and Customer Acceptance Policies