

Lone Rock Holdings N.V.

Crypto Risk Policy

Table of Contents

Key Information	3
Policy History.....	3
1. Purpose	4
2. Policy Implementation	4
2.1. Scope and Application	4
2.2. Audience	4
3. Permitted Cryptocurrencies.....	4
4. Risk Categories and Controls	5
4.1. Regulatory Risk.....	5
4.2. AML/CFT Risk	5
4.3. Operational Risk	6
4.4. Security Risk.....	6
5. Roles & Responsibilities	7
6. Monitoring and Reporting.....	7
7. Policy Review	8

Key Information

Approving Official(s):

Nenad Stojkoski, Director

Responsible Office:

Compliance Department

Effective Date:

June 19, 2025

Next Review Date:

On a case-by-case basis

Policy History

Date	Version	Change	Requestor	Sign Off
19.06.2025	v. 1	N/A	Jasna Stojanova	Nenad Stojkoski

1. Purpose

This policy sets out the framework adopted by Lone Rock Holdings N. V. (hereafter “**the Company**”) for managing the risks associated with the use of cryptocurrencies in its operations. Given the anonymity, borderless nature, and rapid evolution of crypto assets, a structured and proactive approach is essential to ensure full compliance with the Curaçao Gaming License obligations, anti-money laundering and counter-terrorism financing (AML/CTF) laws, and the internal risk appetite of the company. This policy is critical to protecting the integrity of the platform, preventing misuse for illicit purposes, and maintaining stakeholder trust.

2. Policy Implementation

2.1. Scope and Application

This policy regulates all areas where cryptocurrency is accepted or used within the sportsbook brokerage service, including:

- Deposits, withdrawals, and internal crypto-to-fiat conversions.
- All customer interactions involving crypto, including onboarding, wallet verification, and payout requests.

This policy supports Lone Rock N.V.'s broader AML/CTF framework and strengthens operational integrity across its platform. Where a specific crypto-related matter is not regulated within this Policy, the general AML rules apply.

2.2. Audience

This Policy is applicable to all employees, officers, and other stakeholders directly or indirectly associated with the Company. It is incumbent upon each individual to familiarize themselves with the principles and procedures outlined within this Policy and to actively participate in its implementation.

Specific individual roles directly involved with crypto-handling responsibilities:

- Compliance, Risk, and AML officers
- Payment processing staff
- IT and infrastructure security teams.
- Customer support and onboarding agents.

3. Permitted Cryptocurrencies

Based on their high liquidity, widespread usage, and compatibility with secure custody solutions, the Company accepts the following cryptocurrencies:

- Bitcoin (BTC)
- Ethereum (ETH)
- USDT (ERC-20 & TRC-20)
- USDC (Ethereum)
- Cardano (ADA)
- Solana (SOL)
- Litecoin (LTC)
- Tron (TRX)
- Dogecoin (DOG)
- Ripple (XRP)
- DAI (Ethereum)

Each of these coins must be regularly evaluated for risks including transaction traceability, usage in illicit finance, and vulnerability to rapid value fluctuations.

4. Risk Categories and Controls

4.1. Regulatory Risk

Cryptocurrency regulation is rapidly evolving and varies by jurisdiction. In order to fulfil the industry requirements and keep up with the potential threats, the Company is dedicated to:

- Ensuring all crypto transactions are compliant with local and international AML/CTF laws, especially as per the requirements of Curaçao eGaming and any applicable FATF guidance.
- Blocking and geofencing users from regions where crypto gambling is prohibited or under strict regulatory scrutiny
- Maintaining a regulatory watchlist and conduct periodic reviews of updates issued by the FIU Curaçao and international regulatory bodies.

4.2. AML/CFT Risk

Crypto's pseudo-anonymous nature poses significant AML/CTF concerns, particularly in the betting context where funds may be rapidly deposited and withdrawn. The following measures apply:

- Mandatory blockchain wallet screening through reputable blockchain analytics tools before accepting any deposit or executing withdrawals (e.g., Chainalysis, Elliptic).
- Implementation of the FATF Travel Rule, where applicable, to ensure the minimum identification requirements are maintained.
- Crypto deposits are only accepted from wallets owned by the player.
- Deposits originating from high-risk entities, or high-risk jurisdictions are blocked.
- KYC before any withdrawal.
- EDD triggered by thresholds: own platform wallets $\geq$ €2,000, third-party wallets $\geq$ €5,000, or any unusual behavioural pattern.

4.3. Operational Risk

Day-to-day crypto operations can be disrupted due to transaction delays, blockchain congestion (non-liquidity), market volatility or internal mismanagement. To mitigate the risk, the Company applies the following measures:

- All crypto payments flow through approved wallets managed through secure infrastructure (e.g., Fireblocks).
- Conducting daily reconciliations of crypto wallets, linked to user balances by responsible teams.
- Appropriate escalation channels for anomalies or delays in blockchain settlements.
- Not speculating with crypto balances.
- Mandatory conversion to stable fiat equivalents within 24 hours where possible.
- Treasury limits per currency are set and monitored weekly

4.4. Security Risk

The Company's crypto systems may become attractive targets for cybercrime at any time, considering the industry it operates in. To reduce this risk the company undertakes the following measures:

- Strict data security protocols are established and maintained across the whole organization, and upkeeping the same security standards when any data is shared to a trusted third party as part of the day-to-day operations of the organization.
- Private keys are always held in secure custodial systems and never exposed.
- Two-factor authentication and strict access controls must be applied to all systems handling crypto.
- Regular penetration testing and security audits are performed by the IT team.
- Staff training on crypto risks and safe handling procedures.

5. Roles & Responsibilities

The Company's stance is that all crypto-related roles within the organisation must undergo training on digital asset risks, transaction validation, and compliance procedures.

The detailed breakdown of roles and responsibilities is as follows:

Department	Responsibilities
Compliance/AML Compliance officer	Ongoing risk assessments, regulatory monitoring, FIU reporting
Payments/ Finance	Daily processing, reconciliation, liquidity management, fiat conversion
IT / Security	Custodial controls, cybersecurity, monitoring
Customer Support	Frontline checks (including KYC, EDD), flagging red-flag behaviour or complaints

This division of responsibilities ensures that every stakeholder assumes a certain scope of tasks. These together help the organisation to mitigate any potential risks and handle crypto-related operations within the scope of regulations and risk appetite of the Company.

6. Monitoring and Reporting

Effective monitoring and timely reporting are essential to ensure that cryptocurrency-related activities remain within the Company's risk appetite, are fully compliant with legal and regulatory obligations, and are not being exploited for illicit purposes. Due to the dynamic nature of the crypto landscape, it is imperative to have both **automated systems and human oversight working** simultaneously to detect and respond to potential risks promptly.

All incoming and outgoing crypto transactions are monitored in real-time using **blockchain analytics tools** in combination with the general AML Transaction monitoring tools as described in the AML policy.

Alerts are triggered when a red flag arises. The detailed process of which red-flags are considered and the escalation channels are elaborated in the AML Policy.

7. Policy Review

To ensure the ongoing effectiveness and relevance of the company's AML/CFT policies and risk management procedures, the review process will be done as necessary, such as when there are substantial applicable regulatory updates, or upon audit findings and/or risk assessments, or any other event that may require the need of a policy review.

Signatures:



Nenad Stojkoski

Director

Date: June 19, 2025