

Cryptocurrency Risk Management and Compliance Policy

Approved by:

Doubled B.V. Executive Board

21/10/2024



Doubled B.V.

Incorporated under the laws of Curaçao

Company Number: 166107

Licensed by the Curaçao Gaming Control Board (License Number: OGL/2024/1015/0870)

Introduction and Objective

The growing adoption of cryptocurrency in gaming operations necessitates robust governance to address its inherent risks and align with regulatory frameworks. This Cryptocurrency Risk Management Policy defines the measures Doubled B.V. employs to ensure secure, compliant, and efficient handling of cryptocurrency transactions. As a licensed operator under Curaçao's Gaming Control Board, Doubled B.V. is committed to maintaining the highest standards of regulatory compliance, risk management, and operational integrity.

This policy applies to all employees, affiliates, contractors, and third-party service providers involved in cryptocurrency operations. Its primary objectives are to mitigate financial, compliance, and cybersecurity risks while enhancing trust and transparency with stakeholders.

Compliance Framework and Legal Standards

Doubled B.V. operates within a stringent compliance framework that integrates national laws, international standards, and best practices:

- Curaçao Anti-Money Laundering Ordinances (NORUT and NOIS):**
The Company adheres to reporting requirements related to suspicious and unusual transactions, ensuring full alignment with Curaçao's Financial Intelligence Unit (FIU) standards.
- Gaming Board Curaçao Guidelines:**
Compliance with gaming-specific cryptocurrency regulations to uphold operational integrity and avoid regulatory breaches.

3. **Financial Action Task Force (FATF) Virtual Asset Guidelines:**
Incorporation of international standards for risk-based monitoring and management of virtual assets.
4. **European Union Directives (AMLD5 and AMLD6):**
Adoption of rigorous KYC, recordkeeping, and reporting protocols, despite Curaçao's non-EU status, as a benchmark for excellence.

To remain at the forefront of regulatory compliance, the Compliance and Legal Department conducts continuous assessments of cryptocurrency laws and standards, providing quarterly updates to the Board of Directors.

Governance Structure

Doubled B.V. has established a robust governance model to ensure accountability and oversight of cryptocurrency operations:

1. **Executive Board:**
The ultimate authority for approving policy changes, monitoring compliance, and evaluating audit findings.
2. **Head of Compliance:**
Responsible for implementing AML/CFT controls, ensuring adherence to regulatory standards, and maintaining direct communication with the FIU.
3. **Risk Oversight Committee:**
This cross-functional team evaluates cryptocurrency risks quarterly, reviews security protocols, and ensures alignment with the latest regulatory guidelines.
4. **Internal Audit Team:**
Conducts independent quarterly audits of cryptocurrency processes, reporting findings directly to the Executive Board.

Risk Identification and Management

Market Volatility and Financial Risk

Cryptocurrency values are inherently volatile, posing risks to deposits, payouts, and reserves. Doubled B.V. mitigates these risks through:

- **Stablecoin Utilization:** High-value transactions are conducted using stablecoins to reduce exposure to price fluctuations.
- **Scheduled Payouts:** Large disbursements are segmented over predefined intervals, buffering against sudden market shifts.
- **Dynamic Monitoring:** The Financial Operations Team tracks real-time market valuations, making necessary adjustments to align transaction values with prevailing rates.

Regulatory and Compliance Risk

Regulatory landscapes governing cryptocurrency are dynamic and require continuous vigilance. Doubled B.V. addresses this through:

- **Real-Time Monitoring of Legal Changes:** A dedicated team ensures operational policies reflect updates in Curaçao's gaming and AML regulations.
- **Comprehensive Recordkeeping:** All transactions and customer interactions are documented and retained for at least five years, ensuring traceability and compliance with FIU standards.

Anti-Money Laundering and Fraud Risk

The pseudo-anonymous nature of cryptocurrency necessitates stringent controls to prevent illicit activities. Key measures include:

- **Enhanced Due Diligence (EDD):** High-value or high-risk transactions require additional scrutiny, including source-of-funds verification.
- **Blockchain Analytics:** Advanced tools are employed to trace transaction origins and detect suspicious patterns.

Cybersecurity and Asset Protection

Doubled B.V. implements industry-leading security protocols to safeguard digital assets:

1. **Cold Wallet Storage:**
90% of the Company's cryptocurrency holdings are stored offline in secure cold wallets, protected by multi-factor authentication.
2. **Hot Wallet Security:**
Operational wallets are used strictly for daily transactions, equipped with real-time monitoring and transaction limits to minimize exposure.
3. **Access Control:**
Only authorized personnel, verified through multi-level authentication, can access wallets. Unauthorized access attempts trigger automatic security reviews.

AML/CFT Due Diligence and Reporting Procedures

Doubled B.V. is committed to robust AML/CFT practices:

1. **Know Your Customer (KYC):**
All users must verify their identity through government-issued ID and proof of address before engaging in cryptocurrency transactions.
2. **Suspicious Activity Reporting (SAR):**
All flagged transactions are reviewed by the Compliance Officer and reported to FIU Curaçao within 24 hours if warranted.
3. **Ongoing Monitoring:**
Transaction patterns are analyzed in real-time to detect and address potential laundering schemes or fraudulent activities.

Operational and Audit Controls

1. **Transaction Monitoring:**

A blockchain analytics system continuously assesses transaction patterns, flagging irregular activities for further investigation.

2. **Quarterly Audits:**

The Internal Audit Team conducts detailed reviews to ensure adherence to AML/CFT standards and internal protocols. Annual audits are supplemented by external experts to provide third-party validation.

Training and Awareness

To maintain operational excellence, all personnel involved in cryptocurrency activities undergo mandatory training in:

- AML/CFT compliance specific to virtual assets
- Cybersecurity measures for protecting digital assets
- Incident response procedures for suspected breaches or fraud

Policy Review and Amendments

This policy is reviewed annually, or more frequently as required by regulatory developments. Updates are disseminated to all relevant personnel to ensure continued compliance and operational efficiency.