CGA
Curaçao Gaming Authority

Crypto policy guideline for online gaming operators

December 2025

Introduction

This policy sets minimum controls for accepting, holding, and paying out crypto-assets in remote gambling. It applies to all crypto-asset workflows (deposit, wagering, withdrawal, treasury) and all group entities supporting the licensed operation.

It does not replace or limit any other legal, regulatory, or licensing obligations in this regard, including, for example, VASP-related laws and regulations applicable in Curaçao. The operator must independently ensure full compliance with all applicable registration, licensing, reporting, and other regulatory requirements in this respect.

This policy should be signed-off by the compliance officer, approved by the operator's board and should state its effective date. Further the frequency of evaluation of the policy should be stated as well as circumstances that might prompt an unscheduled review.

Governance and accountability

- The operator's board retains ultimate accountability. Day-to-day is delegated to the Compliance Officer and the payments team for compliance including any on-chain risk screening.
- Any change must be documented and managed. Any addition/removal of an accepted crypto asset, virtual asset service provider (e.g. exchange and wallet provider), or risk threshold requires documented risk assessment and appropriate sign-off.

Permitted and Prohibited Assets and Flows

Crypto currencies are considered generally by the CGA as high risk and should be subject to asset-specific risk assessment.

The CGA does not permit transactions in the following crypto currencies:

- Privacy coins: such as Monero (XMR), Zcash (ZEC) and Dash.
- Meme coins: such as DOGE, SHIP and PEPE.
- Wrapped tokens of unknown origin, such as wrapped BTC.
- Deposits routed via sanctioned mixers/tumblers (e.g., Tornado Cash, Blender.io, Sinbad.io) or wallets on sanctions lists.

Operators should give consideration to the following:

Velocity and limits: Setting asset-specific deposit/withdrawal limits, cooling-off, and hold periods proportionate to on-chain risk.

Fees and slippage: Disclose network and other fees, and any conversion or gas-fee handling rules.

Stablecoins

It is preferred that the operator transacts in fiat-backed regulated stablecoins. A separate and heightened review applies to unregulated or algorithmic stablecoins.

Transaction Management

The operator must process withdrawal requests by the player to the same wallet from which the deposit was received.

Withdrawals must be processed in same cryptocurrency as the deposit.

Players cannot transfer amounts to each other on the platform.

Wallets, Custody and Exchanges

Wallet Ownership & Segregation

- Only entity-owned wallets (operator itself or payment subsidiary) are permitted. Use of personal or UBO-linked wallets is strictly prohibited.
- Wallet architecture must clearly segregate:
  - Operational wallets: for day-to-day transactional flows.
  - Treasury wallets: for strategic reserves and capital management.
  - Player-flow wallets: for customer-facing deposits and withdrawals.

Exchange and VASP Standards

- All crypto transactions must be routed through regulated and/or registered exchanges or Virtual Asset Service Providers (VASPs).

- VASPs must demonstrate:
    - Robust AML/CFT controls.
    - FATF Travel Rule compliance
    - Transaction monitoring capabilities.

Access security controls must include:

- Multi-Factor Authentication (MFA) and/or Hardware Security Modules (HSMs).
- Withdrawal whitelists to restrict outbound transfers.
- Multi-signature protocols for treasury wallet operations.

The operator must not itself offer exchange or other services. The CGA only permits a link to a crypto exchange on a separate website.

The CGA expects that the licensed Curacao operators hold wallets only on regulated crypto exchanges.

AML/KYC in crypto context

The AML policy governs both fiat and crypto currency and in the event an operation accepts cryptocurrency transactions, the handling therein must be expressly disclosed as part of the submitted policy on the portal. In general CGA expects that the operator has a heightened approach to management of cryptocurrency transactions given the elevated risk. This includes but is not limited to the following:

- KYC:

Verify customer identity and beneficial ownership in accordance with the AML/CFT policy. Where on-chain indicators suggest elevated risk, enhanced due diligence must be applied.

- Wallet ownership and origin checks:

Obtain appropriate evidence of wallet control (e.g., Satoshi test/return transaction, signed message, or Travel Rule payloads where the counterparty is a VASP). Conduct on-chain tracing to assess exposure to high-risk sources such as darknet markets, mixers, sanctioned entities, or wallets linked to fraud.

° FATF Travel Rule:

Where applicable, ensure that required originator and beneficiary information accompanies crypto transfers to and from VASPs, in line with Travel Rule requirements.

° Monitoring and reporting

Establish monitoring thresholds appropriate for crypto-related activity, including player verification triggers, suspicious activity escalation, and reporting to the FIU. Maintain updated typology libraries relevant to crypto use (e.g., self-transfer chip-dumping, high-velocity deposit/withdrawal patterns, mixer adjacency).

° Responsible gambling in a crypto context

Equivalent RG controls apply irrespective of tender: markers of harm, affordability, time-outs, self-exclusion, bonus restrictions. Monitor behavioural signals of problem gambling that may be masked by high-velocity, on-chain micro-deposits.

° Incident, fraud and cyber response

The operator must consider and define policies for crypto-specific issues such as compromised keys, suspicious deposit rings, smart-contract failures, chain forks, or exchange outages.

Record-keeping and audit trail

Retain Travel Rule payloads, on-chain risk reports, KYC, and transaction logs for the statutory period. Ensure reconciliation between blockchain explorers, exchange statements, and internal ledgers; enable independent audit reproduction.

Consultation period

Any comments on this draft policy guideline should be received within a month after release for consultation.

Transition Period

This policy will enter into force within 6 months after release of the final version.