Crypto policy guideline for online gaming operators

June 2025

Contents

Key Definitions

Virtual Asset Service Provider (VASP): A legal or natural person that conducts one or more of the following activities on behalf of another person: exchange between virtual assets and fiat currencies; exchange between virtual assets; transfer of virtual assets; safekeeping or administration of virtual assets or instruments enabling control over them. Aligned with FATF Recommendation 15.

Unhosted Wallet: A wallet not managed by a VASP and controlled directly by a user through private keys. Unhosted wallet affects risk treatment and Travel Rule applicability.

Wallet Ownership Verification: The process of confirming that a customer controls a specific wallet address, through methods such as test transactions, signed messages, or equivalent mechanisms.

Blockchain Analytics Tools: Systems capable of tracing, analysing, and risk-assessing virtual asset transactions, including identification of exposure to high-risk or prohibited sources.

FATF Travel Rule: The requirement under FATF Recommendation 16 is that originator and beneficiary information must accompany virtual asset transfers between VASPs and be made available to competent authorities upon request.

Compliant VASP: A VASP that demonstrates appropriate standards of AML/CFT compliance, Travel Rule capability, sanctions screening, operational resilience, and transparency — assessed on a risk-based basis by the operator, not determined by jurisdiction label alone.

Introduction

This policy suggests controls for accepting, holding, and paying out crypto-assets in remote gambling operations by Curacao Gaming Authority (CGA) B2C license holders "Licensees". 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 Licensee must independently ensure full compliance with all applicable registration, licensing, reporting, and other regulatory requirements in this respect.

Governance and accountability

This policy should be signed off by the Licensee's Compliance Officer, approved by the board and should state its effective date. Furthermore, the frequency of evaluation of the policy should be stated as well as circumstances that might prompt an unscheduled review.

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.

All Licensees must:

- Undertake necessary blockchain analytics and transaction monitoring tools capable of identifying prohibited assets and transaction patterns. Licensees do not need to be blockchain analysts but cannot operate blindly with regard to the crypto transactions that relate to their operations under their CGA issued license. Risk assessment may be outsourced; visibility and accountability may not;
- Reject, freeze, or return funds where prohibited activity is detected;
- Report relevant incidents in accordance with Article 5.10 (Incident Reporting);
- Maintain documented procedures for identifying and handling prohibited assets;
- Ensure that relevant personnel are trained in digital asset risk identification and assessment.

Not a Financial Institution

In line with other CGA policies including but not limited to AML, Licensees must not themselves function as an exchange, payment services provider, or VASP.

They may accept crypto payments for gambling services only and must make it explicitly clear to the players that they are not responsible for the services of any exchanges used to buy/sell crypto.

Specifically, operators must not:

- Convert crypto to crypto or fiat for users.
- Offer trading, swapping, or exchange services.
- Offer custody, transfer, or wallet services outside gambling-related transactions.

AML/KYC in a Crypto Context

The use of crypto currencies is not a carve-out from AML/CFT or Responsible Gambling obligations. The CGA's AML policy applies equally to fiat and cryptocurrency. Where cryptocurrency transactions are accepted, the operator must explicitly detail the applicable controls within its submitted AML/CFT policy on the portal.

Blockchain Analytics Capability

The CGA recognises that Licensees commonly use blockchain analytics solutions, such as Chainalysis, Elliptic, or TRM Labs, as a single, integrated means of meeting crypto-related AML/CFT obligations.

The CGA does not mandate the use of any specific provider. However, operators must ensure that the full functionality delivered by such tools is achieved, whether through a single solution or a combination of internal systems and external providers.

The Licensee's crypto policy must address functionality such as:

- Trace the origin and destination of funds;
- Identify exposure to high-risk or prohibited sources (e.g. mixers, sanctions, fraud-linked wallets);

- Assess and risk-score wallets and transactions;
- Investigate and evidence suspicious activity for reporting purposes;
- Deposit screening: screen wallet addresses at point of deposit; risk score and flag exposure (darknet, scams, mixers);
- Ongoing transaction monitoring: detect new risk exposure and suspicious patterns over time;
- Source of funds verification: trace fund origins; document for KYC/EDD and audit purposes;
- Withdrawal screening: screen destination wallets before outbound transfers.

Digital Assets and Transaction Sources

Crypto currencies are considered by the CGA as high risk and should be subject to asset-specific risk assessment. It is preferred that the Licensee transacts in fiat-backed regulated stablecoins. However, for other crypto assets, the policy must be commensurate with the risk associated with those asset types.

For example, including, but not limited to the following:

Privacy-Enhancing Cryptocurrencies

The Licensees policy should address assets that obscure transaction data, preventing effective monitoring, blockchain analysis, and source-of-funds verification such as (but not limited to).

- Monero
- Zcash (including shielded transactions)
- Dash (where privacy features are utilised)
- Litecoin's MWEB where privacy is optional.

Pooled / Omnibus Wallet Structures

Pooled or omnibus wallets operated by VASPs are permitted provided that the operator can obtain sufficient data to attribute transactions to individual customers, assess source of funds, and perform monitoring and reporting. Structures that specifically prevent effective attribution or auditability are not permitted.

Meme or Highly Speculative Tokens

Licensees shall carefully address other highly speculative digital asset generally regarded as “meme coins”.

Some so-called “meme coins” are highly liquid and transparent however others exhibit extreme volatility, are susceptible to market manipulation, and do not provide a stable or reliable medium for player funds.

Licensee’s policy should categorize and address these assets based on objective and observable criteria, such as:

1. Liquidity and volatility profile;
2. Governance and ecosystem maturity;
3. Financial-crime risk assessments that consider design features (e.g. anonymity enhancing functionality).

Wrapped Tokens and Bridged Assets of Unverified Origin

Licensees shall not accept deposits or facilitate transactions involving wrapped tokens or bridged assets where the provenance of the underlying asset cannot be clearly established.

This includes wrapped versions of established cryptocurrencies (e.g., wrapped Bitcoin) where the custody, backing, or transactional history of the underlying asset cannot be independently verified. These instruments introduce additional layers of opacity, counterparty risk, and potential disconnection from the original asset’s transaction history.

Expressly Prohibited

Licensees are prohibited from accepting crypto assets that originate from, pass through, or are associated with sanctioned cryptocurrency mixers or tumblers. Nor shall Licensees accept crypto assets linked to wallet addresses appearing on any applicable sanctions list or flagged by recognised blockchain analytics providers.

The CGA reserves the right to designate digital assets, token types, or transaction mechanisms as prohibited where they are deemed to present equivalent risks to transparency, traceability, or regulatory oversight.

FATF Travel Rule Compliance

Licensees must recognize the requirements of the Financial Action Task Force (FATF), including Recommendation 16 (the "Travel Rule"). Where applicable, when crypto-assets are transferred between regulated entities, including exchanges, custodial wallet providers and VASPs, required originator and beneficiary information must accompany the transaction and be made available to competent authorities upon request.

Use of Third-Party VASPs and Payment Providers

The CGA does not mandate the use of any specific providers or jurisdictions. Operators may adopt a risk-based approach to VASP selection, taking into account jurisdictional availability, operational requirements, and market constraints.

For the avoidance of any doubt, the use of third-party providers does not transfer, reduce, or dilute the operator's obligations in respect of AML/CFT, transaction monitoring, player protection, or incident reporting.

The Licensee must ensure that any third-party arrangement is with a VASP(exchange, custodian or payment provider) that is regulated, registered, or otherwise subject to reputable oversight in its home jurisdiction and that demonstrates appropriate AML/CFT controls, Travel Rule capability, sanctions screening, transaction monitoring, operational resilience and transparency. The Licensee must document its due diligence and risk assessment. The CGA may, at its discretion, publish further guidance on acceptable standards or jurisdictions.

Unhosted (Self-Hosted / Non-Custodial) Wallets

Licensees my accept crypo assets from unhosted wallets or DEFI protocols, however the policy must address any specific risk-based control.

- Operators must verify wallet ownership or control;
- Blockchain analytics must be applied to assess transaction risk;

- Enhanced due diligence is required where elevated risk is identified;
- Transactions must not impair the operator's AML/CFT, monitoring, and reporting obligations.

Transaction Management

In principle, the default expectation is that withdrawals should be processed to the same wallet and in the same crypto asset as the original deposit. However, the CGA is aware that this is not always possible in a crypto environment and may cause material volatility exposure and operational inefficiency, particularly at scale.

Permitted alternative approaches are available where equivalent controls can be demonstrated:

- Withdrawals to a different wallet address are permitted where the wallet is whitelisted, can be pre-screened and verified as belonging to the same customer and has passed KYC/AML checks and whitelisting controls;
- Withdrawals in a different crypto asset or stablecoin are permitted where the full transaction flow remains transparent and auditable, conversion is conducted via a regulated VASP, and records are maintained.

Players cannot transfer amounts to each other on the platform.

Operator wallets

All wallets used in connection with the licensed operation must be owned or controlled by the licensed legal entity or an approved group/payment entity. Personal wallets, UBO-linked wallets, employee wallets, or informal wallet arrangements are prohibited. Wallets must be segregated between player-flow, operational and treasury purpose in order to ensure accountability and prevent comingling of player funds and company funds. Player funds should be held in segregated wallets.

Hot, Warm and Cold Wallet Controls

Licensees may use a combination of hot, warm and cold wallets, provided that the wallet architecture is documented, risk-assessed, and subject to appropriate controls.

- Hot wallets may be used for day-to-day player deposits and withdrawals, but balances should be limited to operationally necessary amounts;
- Warm wallets may be used for liquidity management, subject to enhanced access controls and transaction approval procedures;
- Cold wallets may be used for treasury, reserves, or longer-term safeguarding of funds, provided that access, key management, reconciliation, and auditability are maintained;
- Multi-signature controls, withdrawal whitelisting, MFA, HSMs or equivalent security measures should be applied where proportionate to the value and risk of the wallet;
- The Licensee must maintain records sufficient to evidence ownership/control, transaction history, reconciliations, access rights, approvals, and any movement of funds between wallets.

Incident Reporting

In line with the Incident Reporting requirements established under the LOK, Licensees must ensure that all crypto-related incidents are identified, assessed, and reported in accordance with Article 5.10 (Incident Reporting).

Reportable incidents include episodes such as:

- Security breaches, including compromised private keys, wallet access, or unauthorised transactions;
- System failures impacting crypto processing (e.g. exchange outages, blockchain congestion, or failed transactions);
- Detection of fraud schemes involving crypto (e.g. coordinated deposit/withdrawal patterns, chip-dumping, or collusion);
- Material discrepancies in wallet balances or transaction records;
- Any event that may impact the integrity, security, or traceability of crypto transactions;

- Exposure to sanctioned wallets, mixers, or prohibited sources;
- Smart contract failures;
- Blockchain forks or chain-level disruptions.

Transition Period

This policy will enter into force on a phased basis.

1. Immediate effect: prohibitions on sanctioned wallets, mixers, prohibited crypto assets, personal or UBO-linked wallets, and operators acting as exchanges, payment providers or VASPs.
2. Within 3 months (September 2026): The Licensee must upload to the CGA Portal a Crypto policy in line with this document, and this Crypto policy must include a clear timeline of adoption/compliance with the requirements outlined herein, with a particular emphasis on ensuring as a priority the commencement, if necessary of developing (internally or through a hiring process) the necessary level of knowledge and experience that reflects the Licensees crypto business.
3. Within 6 months (December 2026): Licensees must complete documented crypto risk assessments, VASP due diligence, wallet ownership controls, transaction monitoring procedures, and staff training.
4. Within 12 months (June 2027): Licensees must fully implement wallet segregation, blockchain analytics capability, reconciliation processes, withdrawal whitelisting or equivalent controls, and audit-ready record-keeping.

The CGA may require earlier implementation where material risks are identified.