

Ywin Cryptocurrency Payments Policy

Prepared in accordance with CGA Crypto Policy Guidelines for Online Gaming Operators

Document owner	Ivan Georgiev Sinitchiyski, Compliance / AML Officer (including Money Laundering Reporting Officer function)
Approved by	Board of Directors
Version	1.0
Effective date	01.01.2026
Review frequency	Annual, or following material change
Classification	Confidential — Internal Use

1. Purpose and Scope

This policy establishes the minimum controls Ywin applies when accepting, holding, and paying out crypto-assets in connection with its online gaming operations. It covers all crypto-asset workflows — deposit, wagering, withdrawal, and treasury — and applies to all group entities that support the licensed operation.

This policy does not replace or limit any other legal, regulatory, or licensing obligation. Ywin must independently satisfy all applicable registration, licensing, reporting, and other regulatory requirements, including VASP-related laws and regulations applicable in Curaçao.

This policy has been prepared to meet the requirements set out in the Curaçao Gaming Authority (CGA) Crypto Policy Guideline for Online Gaming Operators (December 2025).

2. Governance and Accountability

The operator's board retains ultimate accountability for this policy and for Ywin's compliance with crypto-related regulatory obligations. Day-to-day responsibility is delegated to the Compliance Officer, supported by the payments team, who together own on-chain risk screening and operational oversight.

2.1 Change management

Any change to the list of accepted crypto-assets, any addition or removal of a Virtual Asset Service Provider (VASP) or wallet provider, or any adjustment to a risk threshold must be:

- documented in writing before implementation;
- subject to a formal risk assessment; and
- signed off by the Compliance Officer and, where material, escalated to the board.

2.2 Policy governance

This policy must be:

- signed off by the Compliance Officer;
- approved by the board; and
- reviewed at least annually, or earlier where circumstances warrant an unscheduled review (e.g. new asset listing, regulatory change, significant incident).

The effective date is recorded on the cover page. Each review produces a new version entry in the document history.

3. Permitted and Prohibited Assets and Flows

Crypto-currencies are high-risk instruments. Each asset accepted by Ywin must pass an asset-specific risk assessment before it is enabled.

3.1 Prohibited assets

The following assets are not permitted under any circumstances, in line with CGA requirements:

- Privacy coins — including Monero (XMR), Zcash (ZEC), and Dash.
- Meme coins — including DOGE, SHIB, and PEPE.
- Wrapped tokens of unknown or unverifiable origin (e.g. wrapped BTC from non-standard bridges).
- Deposits routed via sanctioned mixers or tumblers — including Tornado Cash, Blender.io, and Sinbad.io — or wallets appearing on any applicable sanctions list.

3.2 Stablecoins

The preferred instruments for crypto transactions are fiat-backed, regulated stablecoins (e.g. USDC, USDT where appropriately regulated). Algorithmic or unregulated stablecoins are subject to a separate and heightened review process before any transaction is permitted.

3.3 Velocity, limits, and fees

Before enabling any asset, Ywin must define:

- asset-specific deposit and withdrawal limits, cooling-off periods, and hold periods proportionate to assessed on-chain risk;
- disclosure obligations covering network fees, gas-fee handling, and any conversion rules; and
- slippage tolerances and how price differences at the point of settlement are treated.

These parameters must be documented, approved by the Compliance Officer, and communicated clearly to players before they transact.

4. Transaction Management

The following rules apply to all crypto transactions processed on behalf of players:

- Withdrawals must be sent to the same wallet address from which the corresponding deposit was received.
- Withdrawals must be processed in the same cryptocurrency as the original deposit. Cross-asset conversion is not permitted without explicit regulatory approval.
- Player-to-player transfers on the platform are prohibited.

Any exception to these rules requires documented Compliance Officer approval and must be reported to the CGA where required by applicable obligations.

5. Wallets, Custody, and Exchanges

5.1 Wallet ownership and segregation

Only entity-owned wallets are permitted — wallets must be held in the name of Ywin or an authorised payment subsidiary. Use of personal wallets or wallets linked to any Ultimate Beneficial Owner (UBO) is strictly prohibited.

The wallet architecture must clearly segregate funds across three categories:

- 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.

Segregation must be maintained at all times. Mixing funds across wallet categories is not permitted.

5.2 Exchange and VASP standards

All crypto transactions must be routed through regulated and/or registered exchanges or Virtual Asset Service Providers. Any VASP engaged by Ywin must be able to demonstrate:

- AML/CFT controls that meet or exceed FATF standards;
- compliance with the FATF Travel Rule; and
- transaction monitoring capabilities sufficient to identify suspicious activity.

Ywin must not itself offer exchange or conversion services. The CGA permits only a link to a crypto exchange hosted on a separate website. Wallets may be held only on regulated crypto exchanges.

5.3 Access security controls

All wallet and exchange access must be protected by:

- Multi-Factor Authentication (MFA) and/or Hardware Security Modules (HSMs) on all accounts;
- withdrawal whitelists that restrict outbound transfers to pre-approved addresses; and
- multi-signature protocols for all treasury wallet operations.

6. AML/KYC in Crypto Context

The AML policy governs both fiat and crypto currency. Where Ywin accepts cryptocurrency transactions, the handling of those transactions must be expressly disclosed as part of the AML policy submitted to the CGA portal. Ywin applies a heightened approach to crypto transactions given the elevated risk profile. This includes the following obligations:

6.1 KYC and beneficial ownership

Customer identity and beneficial ownership must be verified in accordance with the AML/CFT policy before any crypto transaction is processed. Where on-chain indicators suggest elevated risk, Enhanced Due Diligence (EDD) must be applied before funds are accepted or released.

6.2 Wallet ownership and origin checks

Ywin must obtain appropriate evidence that the depositing player controls the wallet from which funds are sent. Acceptable verification methods include:

- a Satoshi test or return transaction;
- a signed message from the wallet address; or
- a Travel Rule payload where the counterparty is a VASP.

On-chain tracing must be conducted to assess exposure to high-risk sources including darknet markets, mixers, sanctioned entities, and wallets linked to fraud.

6.3 FATF Travel Rule

Where applicable, Ywin must make sure that required originator and beneficiary information accompanies crypto transfers to and from VASPs, in line with Travel Rule requirements. This obligation applies to transfers that meet or exceed the applicable threshold set by the relevant jurisdiction.

6.4 Monitoring and reporting

Ywin must maintain monitoring thresholds appropriate for crypto-related activity. This includes:

- triggers for enhanced player verification based on transaction behaviour;
- escalation pathways for suspicious activity; and
- reporting to the Financial Intelligence Unit (FIU) where required.

Typology libraries must be kept current and must cover crypto-specific patterns including self-transfer chip-dumping, high-velocity deposit/withdrawal patterns, and mixer adjacency.

6.5 Responsible gambling in a crypto context

Standard responsible gambling controls apply regardless of payment method. Ywin must monitor for markers of harm, apply affordability checks, enforce time-outs, self-exclusion, and bonus restrictions in the same way as for fiat transactions.

Particular attention must be paid to behavioural signals that may be masked by high-velocity, on-chain micro-deposits — a pattern associated with problem gambling. Where such patterns are detected, standard harm-reduction protocols must be triggered.

6.6 Incident, fraud, and cyber response

Ywin must maintain documented response procedures for crypto-specific operational incidents. These must address at minimum:

- compromised private keys or wallet access credentials;
- suspicious deposit rings or coordinated wallet activity;
- smart-contract failures or unexpected on-chain behaviour;
- chain forks or network disruptions affecting settled transactions; and
- exchange outages affecting access to player funds.

Incidents must be escalated per the existing incident management framework and reported to the CGA where required.

7. Record-keeping and Audit Trail

Ywin must retain the following records for the full statutory period:

- Travel Rule payloads for all qualifying transfers;
- on-chain risk reports and blockchain tracing outputs;

- KYC documentation and wallet ownership evidence; and
- complete transaction logs including wallet addresses, timestamps, amounts, and asset types.

Records must be maintained in a way that supports reconciliation between blockchain explorer data, exchange statements, and internal ledgers. The audit trail must be sufficient to allow independent reproduction of any transaction history.

8. Policy Review

This policy is subject to formal review at least once every 12 months. An unscheduled review must be initiated where any of the following occur:

- a new crypto-asset or VASP is proposed for onboarding;
- a material regulatory change affects crypto operations;
- a significant operational incident involves crypto payments; or
- the CGA issues updated guidance that affects the scope of this policy.

All reviews must be documented and signed off by the Compliance Officer. Material changes require board approval before implementation.

9. Sign-off

Compliance Officer	Ivan Georgiev Sinitchiyski	Date: 01/05/2026	
Chief Executive Officer	Anton Atanasov	Date: 01/05/2026	
Board approval date	01/05/2026		
Next scheduled review	01/05/2027		

Appendix A — Permitted and Prohibited Asset Register

This register must be maintained by the payments team and reviewed by the Compliance Officer at each periodic review. Any addition or removal requires the documented approval process set out in Section 2.1.

Asset / Token	Category	Status
BTC	Layer 1	Permitted (subject to risk assessment)
ETH	Layer 1	Permitted (subject to risk assessment)
USDC	Stablecoin	Permitted (subject to risk assessment)
USDT	Stablecoin	Permitted (subject to risk assessment)
XMR (Monero)	Privacy coin	PROHIBITED
DOGE	Meme coin	PROHIBITED