

Cryptocurrency & Digital Asset Policy

Curaçao Gaming Authority (CGA) — B2C Remote Gaming Licence

Document control	
Policy owner	Compliance Officer, Zozo Technology B.V
Version	1.0
Effective date	July 13, 2026
Approved by	Board of Directors, Zozo Technology B.V. — July
Review frequency	Annual, or upon a triggering event (see Section 4)
Regulatory basis	CGA Crypto Policy Guideline for Online Gaming Operators (final, June 2026); National Ordinance on Games of Chance (LOK)

1. Policy Statement

This Cryptocurrency & Digital Asset Policy (the "Policy") establishes Zozo Technology B.V.'s (the "Company") framework for the acceptance, custody, processing, and distribution of crypto-assets in connection with its licensed online gaming activities. The Policy reflects the Company's commitment to operating in accordance with the requirements of the Curaçao Gaming Authority ("CGA"), including the CGA Crypto Policy Guideline for Online Gaming Operators, the National Ordinance on Games of Chance (LOK), and all applicable anti-money laundering ("AML") and counter-terrorist financing ("CTF") legislation.

The Policy applies to every aspect of the Company's crypto-asset operations, including deposits, wagering, withdrawals, treasury management, and any related activities undertaken by affiliated entities or payment service providers supporting the licensed gaming business. It is binding on all directors, officers, employees, contractors, agents, payment processors, and third-party service providers who participate in or support the Company's crypto-asset operations.

Nothing in this Policy is intended to supersede, diminish, or exempt the Company from any applicable legal, regulatory, or licensing obligations, including those relating to Virtual Asset Service Providers (VASPs) in Curaçao. The Company remains solely responsible for ensuring compliance with all applicable registration, licensing, reporting, and other regulatory requirements.

2. Purpose & Scope

The purpose of this Policy is to establish a comprehensive, risk-based framework governing the Company's use and management of crypto-assets. It is designed to safeguard the integrity of the licensed gaming operation, mitigate the risk of the platform being exploited for money laundering, terrorist financing, sanctions evasion, or other illicit activities, and ensure that crypto-related risks are appropriately identified, assessed, monitored, escalated, and reported.

This Policy applies to all crypto-asset transactions and activities associated with the licensed operation. Its scope includes player deposits and withdrawals, crypto-assets maintained in operational or treasury wallets, and all crypto transactions processed through affiliated companies,

payment service providers, cryptocurrency exchanges, custodians, or other Virtual Asset Service Providers ("VASPs") engaged by or on behalf of the Company.

3. Key Definitions

Term	Meaning
Virtual Asset Service Provider (VASP)	A person or entity that conducts activities on behalf of another person involving the exchange of virtual assets for fiat currency or other virtual assets, the transfer of virtual assets, or the custody, administration, or control of virtual assets or the instruments used to access or manage them, in accordance with the definition set out in FATF Recommendation 15.
Unhosted wallet	A wallet not managed by a VASP and controlled directly by a user through private keys.
Wallet ownership verification	Verification that a customer has ownership or effective control of a particular wallet address, which may be established through a test transaction, a signed message, or another reliable verification method.
Blockchain analytics tools	Systems capable of tracing, analysing and risk-assessing virtual-asset transactions, including exposure to high-risk or prohibited sources.
FATF Travel Rule	The obligation under FATF Recommendation 16 requiring specified information relating to the originator and beneficiary to accompany virtual asset transfers between Virtual Asset Service Providers (VASPs) and to be made available to competent authorities upon request.
Compliant VASP	A VASP that can demonstrate effective AML/CFT controls, the ability to comply with Travel Rule requirements, robust sanctions screening procedures, operational resilience, and adequate levels of transparency, with its suitability determined through a risk-based assessment conducted by the Company rather than solely based on its jurisdiction of registration or operation.

4. Governance, Accountability & Review

This Policy is approved by the Company's Compliance Officer and formally adopted by the Board of Directors. The effective date of the Policy is recorded in the document control table above, and the Policy shall be subject to a review at least once every twelve (12) months.

An unscheduled review of this Policy will be triggered by any of the following events:

- A change in CGA guidance, the LOK, or applicable AML/CFT or sanctions law;
- The addition or removal of an accepted crypto-asset, VASP, exchange, custodian, wallet provider or payment provider;
- A material change to the Company's crypto business model, products or transaction volumes;
- A crypto-related incident, regulatory finding, or material control failure;
- A change to a risk threshold or the outcome of a risk assessment indicating that controls are no longer adequate.

All amendments to this Policy must be properly documented, reviewed, and implemented through an appropriate change management process. Any decision to add or remove an approved crypto-

asset, VASP, or risk threshold must be supported by a documented risk assessment and obtain the required approvals before implementation.

4.1 Roles & Responsibilities

Function	Responsibility
Board of Directors	Approves the Policy; provides oversight and resources.
Compliance Officer	Owns the Policy; signs off; oversees risk assessments, VASP due diligence, monitoring, escalation and reporting; approves changes.
Finance / Treasury	Manages operational and treasury wallets, reconciliations and segregation of funds.
Operations / Payments	Executes deposit/withdrawal controls, whitelisting and screening at transaction level.
IT / Security	Maintains wallet security, key management, MFA/HSM and access controls.
Management	Ensures resourcing, training and timely remediation of identified gaps.

The Company must ensure relevant personnel are trained in digital-asset risk identification and assessment. Risk assessment may be outsourced; visibility and accountability may not.

5. The Company Is Not a Financial Institution or VASP

The Company shall not operate as a cryptocurrency exchange, payment service provider, Virtual Asset Service Provider ("VASP"), or any other type of virtual asset intermediary. The Company's role is limited to accepting crypto-assets as a payment method solely for the provision of licensed gambling services. Players shall be clearly informed that the Company does not provide, control, or assume responsibility for any exchange, conversion, or other virtual asset services provided by third parties that players may use to acquire, dispose of, or exchange crypto-assets. In particular the Company shall not:

- Convert crypto to crypto, or crypto to fiat, for players;
- Offer trading, swapping or exchange services;
- Offer custody, transfer or wallet services outside gambling-related transactions;
- Permit players to transfer amounts to one another on the platform;
- Allow the platform to be used as a money-movement or exchange mechanism.

The Company's player terms and conditions shall contain a prominent disclosure confirming that the Company is not responsible for, and does not provide any guarantee or oversight of, third-party exchanges, wallets, or other virtual asset service providers used by players to purchase, sell, exchange, or convert crypto-assets.

6. AML / KYC in a Crypto Context

The acceptance and use of crypto-assets does not exempt the Company from any of its AML/CFT, responsible gaming, or regulatory compliance obligations. The Company's AML/CFT framework applies equally to both fiat currency and crypto-assets. All crypto-specific measures and controls established under this Policy are integrated into, and appropriately referenced within, the AML/CFT

Policy submitted through the CGA regulatory portal. Crypto-related risks and activities are also incorporated into the Company's Business Risk Assessment, Customer Risk Assessment, transaction monitoring framework, and compliance training programme.

Where the Company permits crypto-asset transactions, it shall maintain the ability to demonstrate, at a minimum, the implementation of the following controls:

- Customer due diligence measures conducted prior to onboarding or at relevant transaction thresholds, as applicable;
- Screening of wallet addresses associated with deposits and withdrawals;
- Sanctions screening of relevant customers, transactions, and counterparties;
- Ongoing transaction monitoring to identify unusual or potentially suspicious activity;
- Source of Funds ("SoF") and Source of Wealth ("SoW") assessments where required based on risk factors;
- Enhanced Due Diligence ("EDD") measures for higher-risk crypto activity;
- Appropriate investigation, escalation, and record-keeping of unusual or suspicious transactions;
- Submission of reports to the Financial Intelligence Unit ("FIU") where legally required; and
- Effective measures to prevent tipping-off or the unauthorised disclosure of compliance investigations.

7. Blockchain Analytics Capability

The Company shall maintain appropriate blockchain analytics and crypto transaction monitoring capabilities to identify, evaluate, manage, and demonstrate control over risks associated with crypto-asset transactions. These capabilities may be provided through a single specialised solution, such as Chainalysis, Elliptic, or TRM Labs, or through a combination of internal systems and third-party service providers. While the CGA does not require the use of any particular provider or technology, the Company must ensure that its chosen solution provides functionality sufficient to meet applicable regulatory expectations.

The Company's blockchain analytics and monitoring framework shall, at a minimum, enable it to:

- Trace and analyse the movement of crypto-assets, including the source and destination of funds;
- Detect and assess exposure to high-risk, illicit, or prohibited sources, including mixers, sanctioned entities, fraud-related wallets, and other identified risk categories;
- Assign appropriate risk ratings to wallet addresses and crypto transactions;
- Investigate, document, and retain evidence relating to potentially suspicious crypto activity for compliance and reporting purposes;
- Conduct wallet screening at the time of deposit and evaluate exposure to risks such as darknet activity, scams, fraud, mixers, or other illicit sources;

- Perform continuous transaction monitoring to identify changes in risk exposure or emerging suspicious patterns;
- Support Source of Funds ("SoF") verification and maintain appropriate records for KYC, Enhanced Due Diligence ("EDD"), and audit requirements; and
- Screen recipient wallet addresses before processing outbound crypto-asset transfers, including player withdrawals.

8. Accepted Assets & Asset-Specific Risk

Crypto-assets are classified by the Company as inherently high-risk payment instruments and shall be subject to a specific risk assessment before being approved for use within the licensed operation. The Company prioritises the use of fiat-backed and appropriately regulated stablecoins due to their relative stability and reduced volatility risk.

Any other crypto-asset may only be accepted where the Company has completed a documented asset-specific risk assessment and implemented appropriate controls that are proportionate to the identified risks. The assessment shall consider the characteristics, risk profile, regulatory considerations, and operational implications of the relevant crypto-asset.

The following categories of crypto-assets shall be subject to specific consideration and assessment:

Category	Description	Company position
Privacy-enhancing coins	Monero, Zcash (shielded), Dash (privacy features), Litecoin MWEB — obscure transaction data and impair monitoring.	Prohibited by default. Any exposure requires documented, very strong compensating controls and Compliance Officer approval.
Pooled / omnibus wallets	VASP-operated wallets combining multiple customers' funds.	Permitted only where the Company can attribute transactions to individual customers, assess source of funds and perform monitoring/reporting. Structures preventing attribution or auditability are not permitted.
Meme / highly speculative tokens	Tokens with extreme volatility, thin governance or immature ecosystems.	Assessed on objective criteria — liquidity/volatility, governance/ecosystem maturity, financial-crime risk. Acceptance must be justified and documented, not merely listed.
Wrapped / bridged assets	Wrapped or cross-chain assets (e.g. wrapped BTC) whose provenance cannot be established.	Not accepted where custody, backing or transaction history of the underlying asset cannot be independently verified.
Expressly prohibited sources	Assets linked to sanctioned wallets, sanctioned mixers/tumblers or sources flagged as prohibited.	Prohibited. Funds are rejected, frozen or returned in accordance with Section 9.

9. Prohibited Assets & Handling of Funds

The Company shall not accept crypto-assets that originate from, have exposure to, or are connected with sanctioned cryptocurrency mixers, tumblers, or other anonymisation services, nor any crypto-assets associated with wallet addresses listed on applicable sanctions registers or identified as high-risk by recognised blockchain analytics providers.

Where prohibited, suspicious, or high-risk crypto activity is identified, the Company shall take appropriate action, which may include rejecting the transaction, restricting or holding the relevant funds, or returning the assets where permissible and appropriate. All such decisions shall be documented, supported by appropriate records, and managed in accordance with Section 13 of this Policy and the Company's AML/CFT Policy, including any applicable reporting obligations.

The Company shall maintain documented procedures for the identification, assessment, and management of prohibited or restricted crypto-assets. The Company further acknowledges that the CGA may, from time to time, identify additional crypto-assets, token categories, technologies, or mechanisms that are prohibited or subject to enhanced controls.

10. FATF Travel Rule & Use of Third-Party VASPs

Where crypto-assets are transferred between regulated entities, including cryptocurrency exchanges, custodial wallet providers, and Virtual Asset Service Providers ("VASPs"), the Company shall recognise and comply with the principles of the FATF Travel Rule under Recommendation 16. Accordingly, required originator and beneficiary information must accompany relevant crypto-asset transfers and be capable of being provided to competent authorities upon request.

The Company may apply a risk-based approach when selecting and engaging VASPs or other crypto-asset service providers. The involvement of a third-party provider shall not transfer, limit, or reduce the Company's obligations relating to AML/CFT compliance, transaction monitoring, player protection, regulatory reporting, or incident management.

Before engaging any third-party crypto-asset service provider, the Company shall ensure that such provider is regulated, registered, licensed, or otherwise subject to appropriate supervisory oversight within its jurisdiction of operation. The provider must demonstrate effective AML/CFT controls, Travel Rule compliance capabilities, sanctions screening processes, transaction monitoring measures, operational resilience, and appropriate levels of transparency.

The Company shall maintain documented due diligence records and risk assessments for each VASP or crypto-asset service provider engaged in connection with the licensed operation.

11. Unhosted (Self-Hosted / Non-Custodial) Wallets

The Company may permit transactions involving crypto-assets originating from unhosted wallets or decentralised finance ("DeFi") protocols, provided that appropriate risk-based controls are applied to manage the associated risks. In such cases:

- The Company verifies wallet ownership or control (e.g. test transaction, signed message or equivalent);
- Blockchain analytics are applied to assess transaction risk;
- Enhanced due diligence is applied where elevated risk is identified;

- Transactions must not impair the Company's AML/CFT, monitoring and reporting obligations.

12. Transaction Management & Wallet Governance

12.1 Withdrawals

As a general principle, crypto-asset withdrawals shall be processed to the same wallet address and in the same crypto-asset used for the original deposit. Where this is not technically or operationally feasible, the Company may permit alternative withdrawal arrangements only where equivalent risk controls are implemented and maintained.

The following controls shall apply:

- Withdrawals to a different wallet address may be permitted where the destination wallet has been appropriately whitelisted, screened, and verified as being controlled by the same customer, and where all applicable KYC and AML requirements have been satisfied;
- Withdrawals involving a different crypto-asset or stablecoin may be permitted where the complete transaction path remains transparent, traceable, and auditable, any conversion is performed through a regulated or appropriately assessed VASP, and sufficient records are retained to evidence the transaction and associated controls.

The Company shall not permit players to transfer crypto-assets or monetary value between each other through the platform.

12.2 Operator Wallets

All crypto-asset wallets utilised in connection with the licensed operation must be owned, controlled, or formally managed by the licensed entity or an approved group or payment entity authorised by the Company. The use of personal wallets, wallets associated with beneficial owners ("UBOs"), employee-controlled wallets, or any informal or unauthorised wallet arrangements is strictly prohibited.

The Company shall maintain appropriate wallet segregation based on operational purpose, including separate wallets for player transaction flows, operational activities, and treasury management. This segregation is intended to maintain clear accountability, support effective reconciliation, and prevent the commingling of player funds with Company assets.

Player funds shall be maintained in designated segregated wallets and managed separately from the Company's operational or treasury holdings.

12.3 Hot, Warm & Cold Wallet Controls

The Company may implement a combination of hot, warm, and cold wallet solutions, provided that the overall wallet architecture is formally documented, subject to risk assessment, and supported by appropriate security and governance controls.:

- Hot wallets — day-to-day player deposits/withdrawals, with balances limited to operationally necessary amounts;
- Warm wallets — liquidity management, subject to enhanced access controls and transaction-approval procedures;
- Cold wallets — treasury, reserves and longer-term safeguarding, with access, key management, reconciliation and auditability maintained;

- Multi-signature controls, withdrawal whitelisting, MFA, HSMS or equivalent measures are applied where proportionate to value and risk.

The Company shall maintain adequate records to demonstrate ownership or control of all wallets, including transaction histories, wallet reconciliations, access permissions, approval records, and documentation of any transfers or movements of crypto-assets between wallets

13. Incident Reporting

Consistent with the incident-reporting obligations established under the LOK, all crypto-related incidents shall be identified, assessed, escalated, managed, and reported in accordance with Article 5.10 (Incident Reporting).

Reportable crypto-related incidents include, but are not limited to:

- Security incidents involving compromised private keys, unauthorised access to wallets, or unauthorised crypto-asset transactions;
- System failures or operational disruptions affecting crypto-asset processing;
- Identification of crypto-related fraud, abuse, or fraudulent schemes;
- Material inconsistencies between wallet balances, transaction records, or reconciliation data;
- Any event that may impact the integrity, security, availability, or traceability of crypto-asset transactions;
- Exposure to sanctioned wallet addresses, cryptocurrency mixers, tumblers, or other prohibited sources;
- Smart contract vulnerabilities, failures, or related operational issues; and
- Blockchain forks, network disruptions, or other chain-level events affecting crypto-asset operations.

The applicable escalation procedures, reporting timelines, and designated responsible persons shall be established and maintained in the Company's incident management and reporting procedures.

14. Implementation Timeline

This Policy shall become effective through a phased implementation process in accordance with the applicable CGA guideline requirements. Notwithstanding the phased approach, the CGA may require the Company to implement specific provisions earlier where material risks are identified or where regulatory concerns require accelerated adoption.

The Company shall ensure that all applicable controls, procedures, and requirements under this Policy are implemented within the timelines prescribed by the CGA or otherwise determined necessary based on the Company's risk assessment and regulatory obligations.

Phase	Deadline	Actions
Immediate	In force	Prohibitions on sanctioned wallets, mixers/tumblers, prohibited assets, personal/UBO/employee/informal wallets, operator-as-VASP activity and player-to-player transfers; player disclosure regarding third-party exchanges.
Phase 1	Sep 2026	Board-approved, CO-signed Crypto Policy uploaded to the CGA portal with an adoption timeline; commence building internal crypto knowledge/expertise.
Phase 2	Dec 2026	Complete documented crypto risk assessments, VASP due diligence, wallet-ownership controls, transaction-monitoring procedures and staff training.
Phase 3	Jun 2027	Fully implement wallet segregation, blockchain-analytics capability, reconciliation processes, withdrawal whitelisting or equivalent controls and audit-ready record-keeping.

15. Record-Keeping

The Company shall maintain comprehensive records relating to this Policy and its governance, including evidence of approvals, crypto-asset risk assessments, due diligence conducted on VASPs and other service providers, wallet ownership and control arrangements, transaction screening activities, alerts and investigations, reconciliations, approval processes, employee training, and crypto-related incidents.

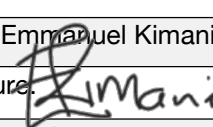
All records shall be retained in accordance with applicable Curaçao laws and regulatory requirements, as well as the Company's AML/CFT Policy and record-keeping procedures. Such records shall be maintained in a manner that enables effective audit, review, and regulatory inspection, and shall be made available to the Curaçao Gaming Authority ("CGA") upon request.

16. Related Policies & References

- Anti-Money Laundering (AML) & Counter-Terrorist Financing (CTF) Policy
- Player Complaints & Dispute Resolution Policy
- Age Verification & Underage Gambling Prevention Policy
- Responsible Gaming Policy
- CGA Crypto Policy Guideline for Online Gaming Operators (final, June 2026)
- National Ordinance on Games of Chance (LOK)

17. Approval & Adoption

This Cryptocurrency & Digital Asset Policy has been reviewed and endorsed by the Company's Compliance Officer and formally approved by the Board of Directors of Zozo Technology B.V.

Compliance Officer	Management Approval
Name: Emmanuel Kimani	Name: Yeh Tai Chun
Signature: 	Signature: 
Date: 13 July 2026	Date: 13 July 2026