

Blue Pepper B.V. Cryptocurrency Policy

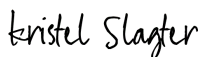
Document Information

Subject	Cryptocurrency Policy
Purpose	To set out the policy stance and the controls in relation to Cryptocurrency use.
Document Owner	Compliance
Review	Upon a significant business change concerning cryptocurrency acceptance
Involvements	All operational departments.
Approval	Director
Document Classification	Internal Use Only

Version Control

Date	Version	Title	Description
03.01.25	1.0	Compliance Officer	Document creation
24.06.2026	2.0	Compliance Officer	Addition of details from the CGA's Crypto policy guideline for online gaming operators

Approval

Date	Version	Title	Signature
7/1/2026	2.0	Director	Signed by:  95B70EC596BD4E6

Contents

Introduction3

Summary of inherent AML/CFT risk.....4

Cryptocurrency acceptance and the requirements of the CGA.....4

Transaction Management (Withdrawals) – CGA requirements.....5

Withdrawals – Operational practice6

Operator Wallets – CGA requirements6

Hot, Warm and Cold Wallet Controls – CGA requirements7

Blockchain Analytics Capability(wallet verification)7

Potential red flags8

Blocking and freezing of accounts8

Record keeping – CGA requirements.....8

Other Crypto assets – CGA requirements.....9

Incident Reporting – CGA requirements.....9

Introduction

This policy outlines the Company stance and controls specific to cryptocurrency transactions to mitigate the risk of illicit financial transactions being made on site following guidance from the [Curacao Gaming Authority's Crypto Policy \(June 2026\)](#). The Company must independently ensure full compliance with all applicable registration, licensing, reporting, and other regulatory requirements in this respect.

The Company offers customers the ability to utilise certain cryptocurrencies to transfer to our PSP, before they are converted into fiat currency and utilised for gameplay. All customers deposits and gameplay are in fiat currency, namely Euro's and Turkish Lira.

The Company is cognizant of the inherent risks associated with cryptocurrencies and acknowledges that it can never be certain of the identity of an owner of a crypto wallet and acts on a commensurate risk-based approach to mitigate these risks.

The acceptance of cryptocurrencies is considered and included in the Company's Business Risk Assessment.

Summary of inherent AML/CFT risk

The company considers that transactions made in cryptocurrency may represent a higher inherent risk than transactions conducted using traditional non-cash payment methods such as debit cards and bank transfers.

The key inherent risks are as follows:

- non-centralised "accounts" may be opened with limited customer due diligence checks;
- difficulty in linking an "account" to a real-world identity;
- potential use of anonymity software such as coin mixers and IP mixers;
- difficulties in establishing source of funds and source of wealth;
- lack or limited AML/CFT controls for crypto use in most jurisdictions.

It is important to note that cryptocurrency use is one factor in the entire assessment of the customers risk factors and whilst its use may be considered an inherent high risk in isolation, this does not necessarily mean the customer is assessed as such.

Cryptocurrency acceptance and the requirements of the CGA

The CGA prohibits licensed companies from accepting crypto assets that originate from, pass through, or are associated with sanctioned cryptocurrency mixers or tumblers. Nor shall crypto assets linked to wallet addresses appearing on any applicable sanctions list or flagged by recognised blockchain analytics providers be accepted.

The Company provides customers with the option to deposit utilising one of several cryptocurrencies and transactions are processed through a payment service provider licensed in the EU, to offer virtual

It is important to note that the Company does not function as an exchange, payment service provider or VASP, therefore, customers choosing to deposit funds onto the site utilising an accepted cryptocurrency are transferred to an integrated payment screen and are given a unique target address to deposit their crypto to. Players are explicitly made aware that the Company is not responsible for the services of any exchanges used to buy/sell crypto through the General Terms and Conditions accepted upon account registration.

The Company has full control and visibility over the specific transactions with operational access to the PSP portal, which provides appropriate transactional data – example screenshot below for reference:

Home

Wallets

Payments

Payment links

Channels

Cross border

Manage account

Generate a unique identifying channel for your customers to re-use and send cryptocurrency top-ups to.

Create a channel

Manage channels

Latest activity

Search payment

Filters

Export

Channel reference	Amount	Merchant ID	Date	Status
channel_Sierinico18_LTC	0.4 LTC	9290331c-88ca-4534-a148-4847bb766e10	08 Nov 2023	Complete
channel_Ulrich_BAH_ArmanFirstClass_USDT	926.59 USDT	9290331c-88ca-4534-a148-4847bb766e10	07 Nov 2023	Complete

[illegible]

It should be noted that wallet providers such as Coinbase and Binance maintain ‘custodial wallets’ which they utilise to send transactions when processing their customers’ withdrawals. As such it

cannot be presumed that the remitting address in the above field is the customers unique wallet address.

Transaction Management (Withdrawals) – CGA requirements

In principle, the default expectation of the CGA 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. 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.

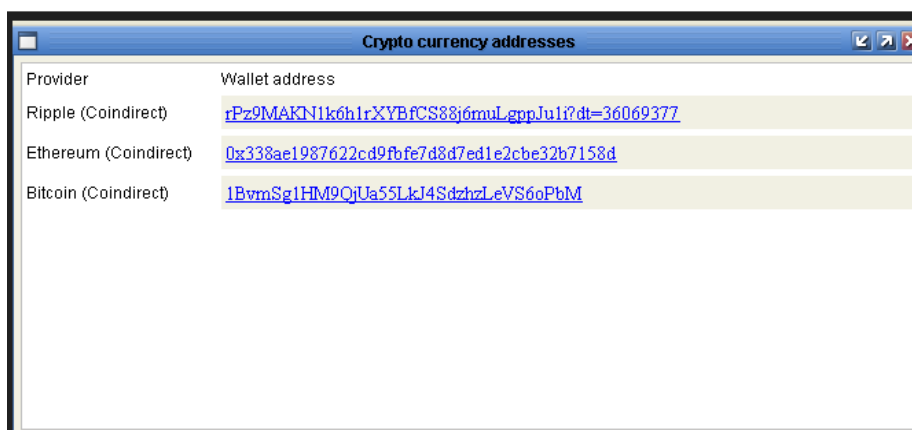
The CGA does not allow players to transfer funds to each other on the platform.

Withdrawals – Operational practice

Subject to gameplay having occurred and there being no account restrictions, a customer can withdraw the account proceeds from fiat currency back to a crypto wallet.

The transaction is again facilitated by the VASP, who automatically screen the wallet address with severe risk transactions being blocked and high-risk transactions being investigated.

Details of the customers wallet addresses which have been utilised for withdrawals are stored in the eBET back-office system and retained in accordance with record keeping requirements. See below for a visual example.



Provider	Wallet address
Ripple (Coindirect)	rPz9MAKN1k6h1rXYBfCS88j6mulgppJuli?dt=36069377
Ethereum (Coindirect)	0x338ae1987622cd9f0fe7d8d7ed1e2cbe32b7158d
Bitcoin (Coindirect)	1BvmSg1HM9QjUa55LkI4SdzhzLeVS6oPbM

Operator Wallets – CGA requirements

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 to ensure accountability and prevent co-mingling of player funds and company funds. Player funds should be held in segregated wallets.

The Company does not own or control any wallets. Wallets are owned solely by the VASP with fiat currency being paid to and from the Company.

Hot, Warm and Cold Wallet Controls – CGA requirements

The CGA have specific requirements in relation to hot, warm and cold wallets. However, as previously stated the Company does not own or control any wallets. In the event a change of business practice is considered, then reference should be made to the CGA's Crypto policy guideline.

Blockchain Analytics Capability (wallet verification)

Each crypto transaction has a unique transaction identifier, which is assigned when the transaction is started and is visible, permanent, and auditable.

The PSP utilizes a blockchain data analysis provider, to carry out crypto transaction monitoring for AML/CFT and Sanctions compliance. All deposits and withdrawal requests are screened for the following indicators and factors (*list not exhaustive*): -

- Identification of severe-risk parties including Sanctions lists, child abuse material related entities, and terrorist financing;
- Alerts for specific behavioral patterns;
- Continuous monitoring for every registered transaction, automatically alerting changes and developments in either blockchain analysis providers' data or user's transaction history.

In the event a wallet sending a depositing transaction to the Company is assessed as a high risk by the blockchain analysis provider, then the transaction is pended and manually reviewed by the PSP. If the exposure is direct (i.e., from the immediate transferring wallet), the transaction is stopped. If the exposure is indirect, a risk-based approach is taken with a decision made to either stop the transaction or allow it to proceed.

Deposits and withdrawals flagged as a severe risk are not processed by the PSP. The provider is subject to SAR reporting requirements and reports of suspicion where locally licensed.

The Compliance team has a line of contact with the PSP's Risk Team in case of need.

Further information on the PSP's wallet screening measures is maintained by Compliance.

Potential red flags

Whilst all account activity should be considered on its merit, the following crypto activity may indicate potential concern and warrant further investigation (*this list is not exhaustive*): -

- Crypto deposits made but funds attempted to be withdrawn without gameplay;
- Crypto deposits made but funds not utilised for gameplay for a significant period of time;
- Crypto deposits which are significantly greater in value and/or frequency when compared to the typical account activity;
- Customer indicates that the crypto wallet concerned in the transaction belongs to a third party;
- Transactions rated a high or severe risk by the PSP.

Blocking and freezing of accounts

In the event of any unusual activity the account will be deactivated while it is reviewed. Information and/or documentation may be requested such as obtaining a transactional screenshot of the crypto payer so that a specific crypto transaction can be matched.

In the event of the knowledge of suspicion of ML/TF is present, then a Suspicious Activity Report will be submitted to Compliance. Guidance on making a SAR is detailed on the [Compliance Hub](#).

On a risk-based approach, the following blocking and freezing options are available and can be applied on a customer's account in relation to their crypto use: -

- Account restriction;
- Blocking the specific use of cryptocurrencies (*applied on eBET by selecting the 'no Crypto Methods' option in Customer Groups*);
- Account closure.

Record keeping – CGA requirements

The Company must maintain records sufficient to evidence ownership/control, transaction history, reconciliations, access rights, approvals, and any movement of funds between wallets, while also adhering to record keeping requirements in accordance with Curacao law.

All staff receive appropriate training upon induction and periodic refresher training to ensure they understand their responsibilities and comply with all policy requirements. Access to internal policies is available on [the Confluence page](#) at all times and bespoke training is also conducted where necessary.

Other Crypto assets – CGA requirements

The CGA Crypto policy details that Crypto assets are considered higher risk and are subject to an asset-specific risk assessment with its preference towards fiat-backed regulated stablecoins. At present, the Company currently makes use of a small number of established crypto asset types. Risk assessments are conducted accordingly, and introduction of any new assets are all subject to assessment.

Accordingly, we do not hold any of the following assets mentioned in the CGA Crypto policy, namely:

- Pooled / Omnibus Wallet Structures
- Meme or Highly Speculative Tokens
- Wrapped Tokens and Bridges Assets of Unverified Origin
- Unhosted (Self-Hosted / Non-Custodial) Wallets.

Incident Reporting – CGA requirements

In line with the Incident Reporting requirements established under the LOK (National Ordinance on Games of Chance), 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.

Any such reports will be made by the Compliance officer.