

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

Approval

Date	Version	Title	Signature
07/01/2025	1.0	Director	DocuSigned by: <i>Kristel Slagter</i> 95B70EC596BD4E6...

Contents

Introduction 4

Summary of inherent AML/CFT risk 4

Cryptocurrency acceptance 4

Withdrawals 5

PSP screening controls (wallet verification) 6

Potential red flags 7

Blocking and freezing of accounts 7

Record keeping 7

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.

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 as assessed as such.

Cryptocurrency acceptance

The Company provides customers with the option to deposit utilising one of several cryptocurrencies and transactions are processed through Cryptopay, a payment service provider licensed in the EU, to offer virtual currency services. It operates under supranational EU regulatory oversight and adheres to comprehensive compliance with EU legislative frameworks. Additionally, the business complies with common FATF standards, operating within reputable jurisdictions.

Customers choosing to deposit funds onto the site utilising an accepted cryptocurrency are transferred to an integrated payment screen in the client and are given a unique target address to deposit their crypto to.

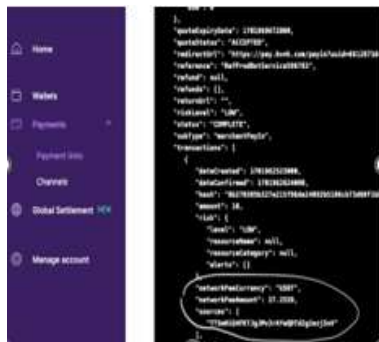
Upon receipt of the transaction, the provider screens the transaction (further details in the '[PSP screening controls](#)' section below) and if this is in order immediately converts the funds into fiat currency. Providing the customer's gaming account is not subject to any restrictions or breach any assigned limits, funds are then applied to the customer's account.

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:

-

Channel reference	Amount	Merchant ID	Date	Status
channel_Swisscof8_LTC	0.4 LTC	9290321c-68ba-4534-a148-6847db799a10	08 Nov 2023	Complete
channel_Ultich_BAH_AlnsaifFirstClass_USDT	928.58 USDT	9290321c-68ba-4534-a148-6847db799a10	07 Nov 2023	Complete

The portal details the depositing wallet address in the sources field, as highlighted below: -



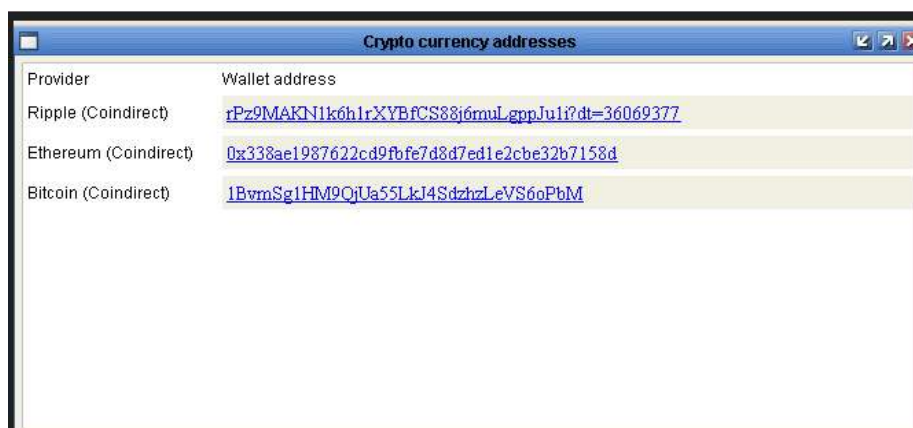
It should be noted that wallet providers such as Coinbase and Binance maintain 'custodial wallets' which they utilise to send transactions when processing their customers' withdrawals. As such it cannot be presumed that the remitting address in the above field is the customers unique wallet address.

Withdrawals

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 Cryptopay, 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)	rPz9MAKN1k6h1rXYBfCS88j6rmuLgppJuli?dt=36069377
Ethereum (Coindirect)	0x338ae1987622cd9fbfe7d8d7ed1e2cbe32b7158d
Bitcoin (Coindirect)	1BvmSg1HM9QjUa55LkI4SdzHzLeVS6oPbM

PSP screening controls (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 for 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 suspicions where locally licensed.

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

Further information on Cryptopay'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 Cryptopay.

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

The Company adheres to record keeping requirements in accordance with Curacao law.