

## **Cryptocurrency Risk Usage Assessment policy**

### **I. Introduction**

As an online gambling operator licensed under the jurisdiction of Curaçao, 1Win N.V. is committed to ensuring full compliance with applicable Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations and other relevant legislation of Curaçao. Furthermore, 1Win N.V. follows internationally recognized recommendations and best practices, particularly those issued by the Financial Action Task Force (FATF).

The use of cryptocurrencies in online gambling presents unique benefits and operational efficiencies. Some of the advantages of using cryptocurrency in gambling industry include:

- irreversible payments: transactions cannot be reversed, eliminating the risk of chargebacks;
- lower fees and faster settlements: crypto payments typically involve minimal fees and are processed much faster than traditional methods;
- transparency: all transactions are publicly recorded on the Blockchain, ensuring a high level of traceability and auditability;
- pseudonymity: while transactions are visible via public keys, identifying the user behind a transaction requires linking the key to a real-world identity, offering a balance between privacy and transparency;
- enhanced security: due to decentralised, peer-to-peer verification, transactions are highly secure and resistant to tampering, with no single point of failure.

Nevertheless, the use of cryptocurrencies introduces specific regulatory, financial, and reputational risks. These risks include high volatility, enhanced anonymity, traceability challenges, and exposure to illicit financial flows.

This Cryptocurrency Risk Usage Assessment Policy (hereinafter referred to as the “Policy”) outlines the framework used by 1Win N.V. to identify, assess, and mitigate risks associated with accepting cryptocurrencies as a method of payment and withdrawal.

The objective of this Policy is to ensure that all cryptocurrency-related activity conducted on the Website is transparent, traceable, and compliant with Curaçao’s AML/CFT regulations, thereby safeguarding the integrity of our operations, clients, and regulatory standing.

### **II. Definitions**

- 1Win N.V. – is a company incorporated under the laws of Curaçao with Company Number 147039 and licensed by the Curacao Gaming Authority to offer games of chance under license number OGL/2024/587/0621 in accordance with the National Ordinance on Games of Chance, and registered at Dr. H. Fergusonweg 1, Curacao (also referred to as “we” or “us” the as appropriate).

- Blockchain – is the underlying technology used for cryptocurrencies and other use-cases. It consists of a distributed database that maintains a list of ordered records, called blocks. These blocks are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data and is transparently recorded online.
- Client – a person, who uses services provided on the 1Win N.V. Website.
- Cryptocurrency – is a form of virtual asset that uses cryptography to secure financial transactions.
- Website – [lwin.pro](https://lwin.pro), [up-x.cc](https://up-x.cc) or any other website operated by 1Win N.V. under the licence OGL/2024/587/0621.

### **III. Cryptocurrencies used on the Website**

- BTC (Bitcoin)
- ETC (Ethereum)
- LTC (Litecoin)
- BNB (Binance Coin)
- USDT (Tether)
- DOGE (Dogecoin)
- TRX (TRON)
- TON (Toncoin)

### **IV. Risks identification**

As part of our obligations under Curaçao legislation, we identify, assess, and understand the risks associated with the use of cryptocurrencies in our online gambling operations. The following categories of risk are considered and used as indicators:

#### **1. Client risk**

- use of anonymous wallets: anonymous wallets (also known as non-custodial or self-hosted wallets) do not require user identification and often operate outside regulated financial systems; while legitimate clients may use them for privacy or control, they can also be exploited for illicit purposes, such as hiding the origin of funds or avoiding detection;
- clients operating from high-risk jurisdictions (such as countries under international sanctions, with weak AML regulations, or high levels of corruption) which may lack sufficient regulatory oversight or cooperation with international enforcement agencies, making it more difficult to verify client legitimacy;

- clients with inconsistent or unverifiable source of funds: clients who cannot demonstrate a clear, legal, and consistent source of funds may be attempting to use illicitly obtained assets;
- use of privacy-enhancing coins or mixing services: privacy coins (e.g., Monero) and mixing or tumbling services are designed to obscure transaction history and user identities;
- unusual behaviour: the client frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a client.

## **2. Geographic risks**

- unexplained or sudden changes in cryptocurrency transaction geography: a client's transaction origin shifts without explanation to a higher-risk country (e.g., switching from low-risk to high-risk regions);
- cross-border transactions with no economic justification: frequent crypto deposits from jurisdictions with no clear connection to the client's claimed residence or economic activity.
- transactions involving unregistered crypto exchanges: clients' funds originate from, or are sent to, a cryptocurrency exchange that is not registered or licensed in the jurisdiction where either the client or the exchange claims to be located.

## **3. Risks correlated with cryptocurrency and Blockchain nature**

- cryptocurrency volatility: cryptocurrencies are subject to significant price fluctuations over short periods of time due to market instability, speculative activity, low liquidity and other factors;
- irreversibility of cryptocurrency transactions: once confirmed on the Blockchain, cryptocurrency transactions can not be cancelled or reversed;
- delayed acceptance of cryptocurrency payments: cryptocurrency transactions may experience delays due to network congestions or transaction confirmation process (e.g. manual confirmations).

## **V. Preventive and detective measures**

To address the specific risks associated with the use of cryptocurrency in online gambling operations, the 1Win N.V. has implemented a comprehensive set of preventive and detective controls.

The following risk mitigation strategies form part of the 1Win N.V.'s internal control framework and are applied throughout the client's lifecycle: from onboarding and transaction monitoring to the offboarding and reporting stages. These controls aim to prevent money laundering, terrorist financing, and other forms of financial crime by ensuring traceability, transparency, and accountability in all cryptocurrency-related transactions.

Each measure outlined below is tailored to address the specific risk categories previously identified in this Policy and is subject to continuous review, update, and enforcement by the IWin N.V.

### **1. Cryptocurrency Acceptance Policy**

- only well-established cryptocurrencies are accepted;
- privacy coins or non-traceable cryptocurrencies are prohibited;
- all crypto transactions must go through an approved third-party crypto payment processor with integrated KYC/AML screening;
- providing to clients clear user-friendly wallet instructions and confirmation steps;
- rate fixing at the time of transactions based on the exchange rate locked at the moment of client's action (deposit or withdrawal);
- integration of QR codes and automated address validation tools in order to avoid incorrect wallet addresses;
- use of prompts and warnings that inform clients that cryptocurrency transactions are irreversible and encourage them to carefully review wallet addresses and transactions details prior to confirmation;
- availability of customer support to assist clients promptly in case of any issues or uncertainties before a transaction is completed.

### **2. Customer Due Diligence (CDD)**

- enhanced due diligence (EDD) may be performed for clients depositing or withdrawing in cryptocurrency;
- blockchain analytics tools (e.g., Chainalysis, Elliptic) are used to assess the source of funds;
- transactions involving high-risk jurisdictions or flagged wallet addresses are subject to manual review.

### **3. Transaction management and controls**

- cryptocurrency deposits and withdrawals are capped at defined thresholds unless verified through full KYC;
- all transactions are logged and monitored for suspicious patterns (structuring, rapid in/out movements);
- only the verified wallet can be used for both deposits and withdrawals (additional wallets are blocked);

- use of trusted and reputable payment providers that offer real-time confirmation transaction process and automated risk screening and (or) monitoring;
- integration with multiple payment providers;
- offering clients alternative payment providers in case of delay.

#### **4. Wallet management**

- hot wallets are used only for operational purposes with strict access controls;
- majority of crypto funds are stored in cold wallets with multi-signature authentication;
- internal audits of wallet balances are conducted monthly.

#### **5. Ongoing monitoring and review**

- all cryptocurrency transactions are subject to continuous monitoring to detect unusual or suspicious activity (this includes both automated and manual checks);
- monitoring results are logged and retained in accordance with Curaçao's record-keeping obligations and may be reported to the Financial Intelligence Unit (FIU) if necessary;
- periodic risk reviews are conducted to assess the effectiveness of monitoring tools and procedures, ensuring alignment with regulatory updates.




Vivian Ersilia o.b.o. SMES Solutions for Management and Employment Support N.V.