THRONE
ENTERTAINMENT

Cryptocurrency Acceptance and Risk Policy

Document Control:

Document Owner	Role	Contact Details
B Van Leeuwen	Compliance Officer	mlro@throneentertainment.com

Document Revision History:

Version	Effective Date	Summary of Change	Author	Approved by
1.0	June 2026	First Draft	Compliance Dept	Board of Directors

Contents

1. Introduction:

The aim of this Cryptocurrency Acceptance and Risk Policy is to establish the Company's approach to accepting, managing and utilising Cryptocurrencies and mitigating the risks associated with doing so.

This policy sets out the minimum controls for handling deposits and withdrawals paid in crypto assets and the handling of customer balances from funds received in crypto assets.

This policy has been created to ensure compliance with the Curacao Gaming Authority's Crypto Policy Guidelines, associated laws and regulations and to manage the AML/CTF risks associated with crypto assets.

This policy is to be read in conjunction with the Company AML/CTF Policy and associated internal policies and procedures.

2. Scope

This policy applies to all Company employees and third-party service providers involved in cryptocurrency related activity. This policy applies to all crypto related activity including deposits and withdrawals in addition to other forms of transactional activity.

3. Senior Management Responsibility

The Board of Directors retains ultimate responsibility for adherence to this Policy. Whilst the Company Compliance Officer has been delegated with day-to-day oversight of the requirements of this policy, the board retains overall accountability.

The Board of Directors and Senior Management of Throne Entertainment are fully engaged and involved in all stages of the development of Company policies and procedures ensuring that the approach taken is in line with the company's risk appetite.

4. Current Status

Throne Entertainment does not currently offer Cryptocurrency as a direct funding method for customer transactional activity, nor does it offer gambling activity or withdrawals using crypto assets.

The Company currently offers customers the ability to make deposits in supported cryptocurrencies; however, these payments, offered via a regulated Virtual Asset Service Provider ("VASP"), are converted to FIAT currency for the purpose of customer deposits, withdrawals and gambling activity.

As part of the onboarding process for such service providers, the Company Due Diligence procedure ensures that the VASP can demonstrate;

- Their regulated status
- That they have robust AML and CFT controls in place
- They comply with the FATF travel rule
- They carry out ongoing transaction monitoring, including the use of blockchain analytics tools
- They have a robust screening program in place

All service providers are obliged to provide the Company with a copy of their AML/CTF policy as part of their onboarding Due Diligence process and the Company's Compliance and Legal functions review such documentation as part of the risk assessment process for new suppliers.

5. Requirements for Curacao Licensed Online Gaming Operators

In December 2025, the Curacao Gaming Authority published a consultation document outlining the minimum control requirements for operators. This Policy details these requirements and ensures that the Company's approach, complies with the guidelines.

5.1. Prohibited Cryptocurrencies

Under the guidelines the following cryptocurrencies are prohibited for transactions;

- Privacy coins such as Monero (XMR), Zcash (ZEC) and Dash (DASH)
- Meme coins such as Dogecoin (DOGE), Shiba Inu (SHIB) and Pepe (PEPE)
- Wrapped tokens such as wBTC (Wrapped Bitcoin) or wETH (Wrapped Ether)
- Deposits via sanctioned mixers/tumblers e.g. Tornado Cash, Sinbad.io and Blender.io

5.2. Preferred Currencies

The CGA recommends that gambling operators transact in FIAT backed regulated Stablecoins.

Stablecoins are less volatile than other cryptocurrencies due to being tied to an asset to help control the variation in price. Examples of regulated Stablecoins would be USDC (US Dollar Coin) and EURC (Euro Coin).

Whilst being the most commonly known Stablecoin, USDT (US Dollar Tether) is not currently regulated under the main digital asset regulatory frameworks. Use of this type of asset requires heightened reviews in comparison to regulated stablecoins.

5.3. Further Considerations

In addition to the above, the CGA advises operators to consider setting transaction limits, cooling off and on hold periods proportionate to the risks posed by these currencies.

5.4. Transaction and Wallet Management

Withdrawals must only be made to the same wallet from which the original deposit was received. Furthermore, withdrawals must be processed via the same currency used for the initial deposit.

Shared wallets are not permitted. Controls are to be in place to ensure that wallets used on more than one account are identified. Transferring funds between accounts is not permitted whether the activity is in FIAT or cryptocurrency.

5.5. Prohibition on Exchange Services

Gambling operators are prohibited from offering exchange services, only permitting a link to crypto exchanges on a separate website. The CGA further requires that wallets are held on only regulated crypto exchanges. Throne Entertainment does not offer this facility.

6. AML/CTF Controls

Due to the pseudonymous nature of cryptocurrency[1], there may be occasions when additional AML/CTF related measures are required over and above the Company's standard procedures to mitigate the risks identified.

6.1. Enhanced Measures

The measures to mitigate the risks include but are not limited to;

- Verification of identity at an earlier stage. Where internal indicators suggest elevated risk, the Company's risk department are to verify the identity of the account holder and where appropriate obtain evidence of wallet ownership.
- Reviewing details in the back office of payment solution providers. The Company's risk and payments teams have access to the providers back-office system to assist with investigations.
- Thresholds for account reviews are lower for higher risk payment methods such as cryptocurrency and pre-paid instruments. This ensures that customers posing a greater risk are reviewed at an earlier stage and with increased frequency.
- AML/CTF reviews consider customer transactional activity and crypto related typologies. Any suspicious activity is escalated to the MLRO at the earliest possible stage for review and external reporting of suspicion to the FIU.
- Obtaining details on the origin of funds for the activity in question. This will include obtaining information and evidence of the source of funds for deposits into the Crypto wallet.
- Undertaking Enhanced Due Diligence for those customers depositing larger amounts, especially when doing so using higher risk payment methods such as cryptocurrency.

6.2. Business Risk Assessment

The Company adopts a risk-based approach to AML/CFT. This approach is essential for identifying and mitigating ML/TF risks specific to the online gaming industry. When carrying out the Business Risk Assessment ("BRA"), the risks posed to the Company by the use of cryptocurrency are included and the effectiveness of the mitigating controls assessed. The BRA process aims to identify any new or identified risks and continuously monitors the effectiveness of the mitigating controls. Where any new or identified risks relating to cryptocurrency are identified, the BRA will be revisited and updated.

The BRA process is explained in detail in the Company AML Policy.

6.3. Customer Risk Assessment

As with the BRA process, the Customer Risk Assessment ("CRA") considers the risks posed by Customers against a number of factors. These factors include the use of higher risk payment method such as cryptocurrency. Where the customer is deemed to be higher risk, measures such as those referred to in section 6.1 are undertaken.

The CRA process and details of the action to be taken for customers deemed to be higher risk are explained in detail in the Company AML Policy.

[1] https://www.cointracker.io/learn/pseudonymous

7. Training

Employees involved in cryptocurrency transactions will receive regular training on this policy, including AML/CTF obligations, regulatory updates and risk management strategies.

Where appropriate, educational resources will be provided to customers to help them understand the risks and benefits of using cryptocurrencies for transactions.

8. Record Keeping

Customer transactional records, KYC and DD information for both customers and service providers, related AML/CFT records and employee training records will be retained and maintained for auditing and compliance purposes. Full details of the record retention requirements are provided in the Company Data Protection and Retention Policy and the Company AML Policy.

9. Quality Assurance

Compliance with this policy and associated Company Policies and Procedures will be reviewed as part of the Company's audit program. Both Internal and External audits will be carried out periodically to identify any gaps or weaknesses in the Company's controls and to identify opportunities for improvement.

10. Policy Maintenance and Review

Regular reviews of this policy will be undertaken to ensure compliance with regulations and guidelines. As a minimum, following publication, this policy will be reviewed at the latest 6 months after initial release. Thereafter the policy will be reviewed as a minimum on an annual basis.