RISK WARNING ON CRYPTO-ASSETS

Version: 1.0 · Effective from: 1 August 2026

The Czech version of this document is binding; the English version is for information only.
Závazná je česká verze tohoto dokumentu; anglická verze je pouze informativní.

Crypto-assets are associated with significant risks. Their value may rise and fall significantly and, in an extreme case, the client may lose the entire amount invested. Crypto-assets are not bank deposits and are not covered by the deposit insurance scheme.

This document provides a clear explanation of the main risks associated with the purchase, sale, custody, administration and transfers of crypto-assets through Coinero, including staking provided as part of custody. Its purpose is to help the client understand these risks before using the relevant service.

Main risks in brief

- The value of crypto-assets may fluctuate significantly. Neither a return nor the preservation of the amount invested is guaranteed.
- Blockchain transfers are generally irreversible. An error in the address, network or other details may cause a permanent loss.
- The staking reward is not guaranteed and crypto-assets may be temporarily unavailable during staking or unstaking.

How risks can be reduced

The risks associated with crypto-assets cannot be eliminated entirely. However, the following measures may help to reduce them:

- Get to know the crypto-asset. Study its white paper, if available, and verify information on the project, the persons behind it, the rights attached to the crypto-asset, the way any return is generated and its liquidity from other trustworthy sources.
- Assess information critically. Do not base your decisions solely on advertising, information from social networks, recommendations by influencers, the popularity of the project, time pressure or a promise of a guaranteed or unusually high return.
- Consider your financial situation. Put into crypto-assets only funds whose potential loss will not jeopardise your regular expenses, the repayment of your obligations or your financial reserve.
- Protect your account and devices. Use a unique strong password and multi-factor authentication. Never share your password or one-time verification code with anyone. Access your account only through the official Application or the Coinero website, keep your devices and software up to date and check your account activity regularly.
- Check transfers carefully. Before confirming each transfer, verify the type of crypto-asset, the recipient address, the blockchain network and all required additional details, for example MEMO or TAG. When transferring a more significant amount to a new address for the first time, you may consider sending a smaller test amount first.
- Consider a suitable method of custody. For long-term holding, in particular if you do not need to trade crypto-assets regularly or use related services, you may consider transferring them to your own

hardware wallet or other wallet whose private keys are not normally connected to the internet. Self-custody reduces some of the risks associated with the provider, but it transfers to you the responsibility for protecting the private keys, the recovery phrase, backups and the device used. Their loss or disclosure to another person may lead to an irreversible loss of crypto-assets.

- Consider the risks of staking. Before committing crypto-assets to staking, familiarise yourself in particular with the activation and unstaking periods, the possibility of these periods being extended, the variability of the reward and the risks relating to the staking provider.
- Follow important announcements. Pay attention to information from Coinero on changes to the supported crypto-assets and blockchain networks, the availability of services and the staking conditions.

A more detailed description of the individual risks is set out in the following chapters.

1. Nature of crypto-assets and scope of protection

Crypto-assets are a digital representation of value or rights using distributed ledger technology or a similar technology. They are neither legal tender nor bank deposits.

The value of crypto-assets is not covered by the bank deposit insurance scheme. The scope of legal protection may vary depending on the type of crypto-asset and the service used.

Coinero provides crypto-asset services on the basis of an authorisation granted by the Czech National Bank and is subject to its supervision. The authorisation relates to the activities of Coinero; it does not constitute an approval of individual crypto-assets or a guarantee of their value.

2. Market risk and the possibility of total loss

The prices of crypto-assets may fluctuate significantly within minutes or seconds in response to demand, regulatory announcements, technological events, media information, the conduct of major holders or developments in global markets. The value may fall significantly or even approach zero.

- A return is not guaranteed and a loss may occur even within a very short period of time.
- Fees and the difference between the buy price and the sell price may increase the loss.
- A historical price, popularity or high past returns are no guarantee of further growth.

3. Liquidity and transaction execution risk

For some crypto-assets, there may not be sufficient supply or demand. It may therefore not be possible to execute an order within the expected time, in the expected volume or at the expected price. Low liquidity may lead to a significant spread between the buy price and the sell price, price slippage or temporary or permanent unsaleability. In the event of extraordinary volatility, market congestion or a failure of an external trading platform, an order may be delayed, restricted or suspended.

4. Currency, price and fee risk

Currency risk. If the price is determined or settled in another currency, a change in the exchange rate may affect the actual profit or loss.

Price data risk. The rates displayed may be indicative, delayed or affected by a technical error or by third-party data. The final price may therefore differ.

Fees and network costs. The result is affected by Coinero fees, the spread and blockchain network fees, which may increase significantly when the network is congested.

5. Project, issuer and information risk

Failure of the project or the issuer. The value may depend on the issuer, the developers, the community, the network operators or other persons. The project may lose its funding or support, be terminated, be split or prove to be technically or economically unviable.

Concentration and governance. A significant part of the crypto-asset or of the voting rights may be controlled by a limited number of persons. Their decisions or the sale of a large volume may affect the price, the functioning of the project or the rights of other holders.

White paper and other information. The white paper may contain incomplete, one-sided, outdated or incorrect information. For most crypto-assets, its content may not have been reviewed on its merits or approved by a supervisory authority. The availability of a crypto-asset on Coinero is no guarantee of its quality, its future value or its suitability for a particular client.

Fraudulent projects. Some projects may show signs of fraud, market manipulation, a so-called rug pull or a Ponzi scheme. Information disseminated by anonymous persons, influencers or holders who have their own financial interest may also be misleading.

6. Risks of custody and third parties

The security of systems and the protection of client crypto-assets are among the main priorities of Coinero. Coinero adopts technical and organisational security measures and keeps client crypto-assets separately from its own crypto-assets.

However, the custody of crypto-assets, like other digital financial services, is exposed to cyber, technological and operational risks which no security measures can entirely exclude. These may include, in particular, a cyber attack, fraud, an operational or technical error, the loss or misuse of the means of access to crypto-assets, legal restrictions or the insolvency of a person involved in their custody. These events may cause delays, temporary unavailability or, in an extreme case, the loss of some or all of the crypto-assets held in custody.

Third-party risks. In providing its services, Coinero may use banks, trading platforms, providers of custody or staking services, providers of technological infrastructure and other third parties. Their operational or security failure, restriction of services, fraud or insolvency may affect the availability of crypto-assets or funds. The use of a third party does not affect the liability of Coinero to the extent laid down by legal regulations and the contractual documentation.

Self-custody may reduce some of the risks associated with custody by a provider. A client who intends to hold crypto-assets in the long term and does not need to trade them regularly or use related services may consider transferring them to their own hardware wallet or other wallet whose private keys are not normally connected to the internet.

However, self-custody transfers to the client the responsibility for protecting the private keys, the recovery phrase, backups and the device used. Their loss, damage or disclosure to another person may lead to an irreversible loss of crypto-assets. An own wallet therefore reduces some of the risks associated with the provider, but at the same time creates other risks.

7. Technological and blockchain risks

The functioning of crypto-assets depends on blockchain networks, software, cryptographic methods and, in some cases, also on smart contracts. An error in, an attack on or a change to these technologies may affect the value or availability of a crypto-asset and the ability to carry out transactions.

- Errors and vulnerabilities. The protocol, a smart contract, the cryptography or the software used may contain an error or vulnerability. Its exploitation may cause the network to malfunction, unauthorised transactions to be carried out or crypto-assets to be lost.
- Attack on or outage of the network. An attack on the method of confirming transactions, a change to blocks already recorded or a long-term outage of validators may lead to the delay, rejection or temporary suspension of transactions.
- Blockchain changes. A split of the network (fork), a change to the protocol, a token swap, a migration to another network or the distribution of new tokens may affect the characteristics, value or rights associated with the crypto-asset. Coinero may not support such a change or a newly created crypto-asset.
- Network congestion. An increased number of transactions may cause long waiting times for confirmation, a significant increase in network fees or a temporary restriction of transfers.
- Termination of support. Network operators, developers, wallet providers or other third parties may terminate support for a particular network, token or technical standard. Coinero may therefore restrict or terminate support for the crypto-asset concerned and the client may be asked to transfer or sell it.

8. Cyber security and fraud

Accounts, devices and wallets used for dealing with crypto-assets are frequent targets of cyber attacks and fraud. If an attacker gains access to the client's account or security credentials, they may carry out a transaction which it may no longer be possible to cancel, or the crypto-assets obtained may no longer be recoverable.

- Fraudulent communication. An attacker may impersonate Coinero, a bank, technical support or another trustworthy person. They may use a fraudulent e-mail or message (phishing), a telephone call (vishing), a fake website or a fake application.
- Account takeover. An account may be misused as a result of the theft of a password or a one-time verification code, the compromise of an e-mail account or telephone number, or the unauthorised issue of a new SIM card.
- Malicious software. Malware may monitor the data entered, change the recipient address or enable an attacker to control the client's device.
- Fraudulent offers. An increased risk is posed by offers of a guaranteed return, requests to transfer crypto-assets to an allegedly "safe" wallet, time pressure or requests to install a program for remote access to the device.

Never share your password or one-time verification code with anyone. If you use your own wallet, do not share its private key or recovery phrase with another person. Use a unique strong password and multi-factor authentication and, before confirming a transaction, always check the domain, the recipient address, the blockchain network and the other details.

9. Risks of crypto-asset transfers

Once sent to the relevant network, blockchain transfers are generally irreversible. It may therefore not be possible to cancel an incorrectly executed transaction and recover the crypto-assets sent.

- Incorrect details. Sending to an incorrect address, to an incorrect blockchain network or to an address intended for another crypto-asset may cause a permanent loss. For some transfers, an additional identifier must also be provided, for example MEMO or TAG, which is used to allocate the payment to a specific account.
- Change of the deposit address. The deposit address may be individual or temporary, or it may change. The client should therefore display and verify it in the Application immediately before each transfer.
- Unsupported assets and technologies. It may not be possible to credit or return crypto-assets sent via an unsupported network, an unsupported smart contract or in a form not supported by Coinero.
- Delay or restriction of a transfer. A transfer may be delayed, suspended or rejected, in particular for legal, regulatory or security reasons, due to the verification of the sender or the recipient, congestion of the blockchain network or an outage of a third party.

Before confirming a transfer, always check the crypto-asset, the recipient address, the blockchain network and all required additional details.

10. Operational risk and availability of services

The provision of services depends on the proper functioning of the Application, internal processes, banking systems, blockchain networks and third-party infrastructure. Scheduled maintenance, a technical error, a cyber incident, a telecommunications or power outage, a failure of a third party or another extraordinary event may cause the temporary unavailability of a service, delays or the incorrect display or processing of data.

The client may therefore not be able, at the intended moment, to place or cancel an order, respond to a price change, transfer crypto-assets or withdraw funds. The settlement of a transaction may take longer than the client expected.

Restriction or termination of support for a crypto-asset. Coinero may, for legal, security, operational or liquidity reasons, restrict or terminate support for a particular crypto-asset, blockchain network or related function. In such a case, the client may be required to transfer, sell or otherwise deal with the crypto-asset within a specified period.

11. Specific risks of stablecoins

A crypto-asset whose value is intended to track a currency or another asset may fail to maintain that value. There may be a loss of the peg (depeg), a shortage or impairment of reserves, a restriction of redemption, the insolvency of the issuer, the freezing of tokens or a regulatory intervention. The designation “stablecoin” therefore does not mean that the price is stable or free of risk.

12. Specific risks of staking

Staking is available as part of custody only for selected crypto-assets. It does not guarantee a return or the preservation of the value of the crypto-asset, and in providing it Coinero may use staking providers or other third parties.

Non-guaranteed and variable return. The staking reward may be lower than the client expected, may be credited later or may not be credited at all. The annual rate stated is indicative only and may change, in particular depending on the rules of the blockchain network, the number of validators, the volume of crypto-assets committed to staking or the conditions of the staking provider.

Staking activation. For some crypto-assets, the reward starts to accrue only after the activation of the staking position has been completed. The activation period is indicative only and may be extended. While waiting for staking to be activated, the reward may not accrue.

Temporary unavailability and unstaking period. Crypto-assets may be entirely or partially unavailable for the duration of staking and of their release. In particular, for the Bonded type, it may not be possible to deal with them, transfer them or sell them after an unstaking order has been placed, even in the event of a significant fall in their price.

The unstaking period stated in the Application is indicative only and compliance with it is not guaranteed. The actual release of crypto-assets may take longer, in particular as a result of the rules of the relevant blockchain network, the validator queue, congestion or an outage of the network, a technical or security incident or a delay on the part of the staking provider. Coinero generally cannot influence these circumstances or shorten the unstaking period. The reward may not accrue during unstaking.

Network penalties (slashing). On some blockchain networks, misconduct or unavailability of a validator may, under the rules of the network, lead to a reduction or loss of the reward and, in some cases, also to the loss of part of the crypto-assets committed to staking. Coinero does not itself operate validator nodes and provides staking through a third party; however, this risk cannot be entirely excluded.

Third-party and blockchain network risk. The staking provider may restrict, suspend or terminate the programme. Its insolvency, operational or security failure or problems with the blockchain network may cause delays in activation, rewards or unstaking, temporary unavailability or the loss of crypto-assets.

Market risk persists. For the duration of staking, the crypto-asset remains exposed to price fluctuations. A fall in its value may exceed the staking reward received and the client may suffer a significant or total loss.

13. Legal, regulatory and tax risk

Legal and regulatory risk. The legal framework for crypto-assets and its interpretation may change. Changes in legal regulations, regulatory requirements or decisions of public authorities may affect the tradability, transferability, custody or availability of a particular crypto-asset or service, including staking.

Tax risk. The purchase, sale, transfer or staking of crypto-assets may have tax or reporting consequences for the client. Their assessment depends on the client’s individual situation and the tax rules may change. The client is responsible for assessing and fulfilling their tax and reporting obligations. Unless a legal regulation provides otherwise, Coinero does not calculate or remit tax on behalf of the client.

14. Risk of an uninformed decision

Crypto-assets may be complex and their functioning may not be easy to understand. The client should not rely solely on advertising, information from social networks, recommendations by influencers or anonymous persons, or on the expectation of a high return. Such information may be incomplete, misleading or motivated by the author’s own benefit.

15. Other and unforeseeable risks

The crypto-asset market, the technologies used and the regulatory environment are evolving rapidly. Other significant risks may therefore arise which are not described in this document or which could not be foreseen at the time of its publication.