

Investissement en Actifs Numériques

Cartographie des risques pour l'investisseur

Stablecoins · DeFi · Protocoles · Émetteurs · Plateformes MiCA

Une architecture de risques en 3 Couches

Tout investissement via une plateforme DeFi expose l'investisseur à une chaîne de risques imbriqués, indépendants et cumulatifs.



COUCHE 1 — Protocole DeFi

Hack de smart contract · Bug de protocole · Perte totale non couverte par MiCA

NON RÉGULÉ



COUCHE 2 — Plateforme intermédiaire (ex. Wigl)

Faillite · Hack de la plateforme · Non-ségrégation des actifs · Risque opérationnel

MiCA (partiel)



COUCHE 3 — Émetteur de stablecoin

Faillite de l'émetteur · Réserves insuffisantes · Décote · Dépeg · Délai de procédure

MiCA (fort)

Les 3 couches sont indépendantes : un événement sur l'une n'est pas couvert par les protections des autres.

Risque Technologique — Protocole DeFi

Le smart contract est la loi, mais il peut être exploité



Hack de smart contract

Exploitation d'une vulnérabilité dans le code du protocole. Les fonds sont volés ou détruits. Aucun mécanisme légal automatique de remboursement.



Bug de protocole

Erreur de logique entraînant un dysfonctionnement : blocage des dépôts, incapacité de retrait, perte partielle des rendements accumulés.



Risque de liquidité

En cas de ruée sur les retraits, le protocole peut ne pas disposer de liquidités suffisantes pour honorer toutes les demandes simultanément.



Absence de couverture MiCA

Les protocoles DeFi “entièrement décentralisés” ne sont pas encadrés par MiCA. Aucune obligation de divulgation ou de réserve ne s'applique.

⚠ En cas de hack DeFi : votre protection dépend uniquement des CGU de la plateforme (assurance, fonds de réserve). MiCA ne garantit pas le remboursement (hors scope)



Risque Plateforme — Faillite et Ségrégation

✓ Compte Ségrégué

(Modèle MiCA conforme)

- Vous êtes propriétaire direct des stablecoins
- Actifs séparés du bilan de la plateforme
- En cas de faillite : restitution prioritaire
- La plateforme agit comme simple dépositaire (custody)
- Analogie : compte-titres chez un intermédiaire financier

✗ Compte Non Ségrégué

(Risque créancier)

- La plateforme détient les tokens en son nom propre
- Vous n'avez qu'une créance sur la plateforme
- En cas de faillite : vous passez en procédure collective
- Remboursement incertain, avec décote et délais longs
- Analogie : dépôt dans une banque qui fait faillite (sans FGDR)

Ce que MiCA impose : ségrégation obligatoire des crypto-actifs clients · Solidité prudentielle · Mécanismes de plainte

Ce que MiCA n'impose pas : garantie de dépôt type FGDR pour les crypto-actifs (peut être dans un MICA 2)

Risque Émetteur — Stablecoin et Réserves

Ce que MiCA garantit

Couverture 1:1

Les réserves de l'émetteur doivent couvrir 100% des tokens émis

Séparation des réserves

Réserves isolées des fonds propres de l'émetteur

Droit de rachat

Tout porteur peut exiger le rachat à valeur nominale

Supervision

Supervision par ABE pour les grands émetteurs, autorité nationale sinon

Audits réguliers

Rapports périodiques et transparence sur la composition des réserves

Risques résiduels en cas de faillite

Réserves insuffisantes

Fraude ou mauvaise gestion : un haircut reste possible malgré MiCA

Actifs illiquides

Réserves investies en obligations ou dépôts eux-mêmes en difficulté

Lenteur procédurale

Faillite : procédures judiciaires longues avant tout remboursement

Risque de dépeg

Perte de confiance → perte de valeur même sans faillite formelle

Gel réglementaire

Autorités peuvent geler les comptes (AML, sanctions) sans faillite

MiCA : Périmètre de protection

Comprendre ce que le cadre réglementaire européen couvre — et ce qu'il ne couvre pas

✓ MiCA protège

- Émetteurs de stablecoins : réserves 1:1, audits, droit de rachat
- Plateformes CASP : ségrégation des actifs clients obligatoire
- Solidité prudentielle minimale des opérateurs régulés
- Information préalable sur les risques (duty de transparence)
- Supervision coordonnée ABE / autorités nationales
- Mécanismes de plainte et de recours pour les clients

✗ MiCA ne protège pas

- Protocoles DeFi 'entièrement décentralisés' (hors périmètre)
- Garantie de dépôt type FGDR : aucun équivalent crypto
- Hacks de smart contracts (risque technologique pur)
- Risques opérationnels des plateformes (hack, erreur clé)
- Fraude ou mauvaise gestion des réserves de l'émetteur
- Lenteur ou décote en procédure de faillite



Bonnes Pratiques — Comment se protéger

01

Vérifier la ségrégation des actifs

Lire les CGU et la documentation juridique : les stablecoins sont-ils conservés en compte ségrégué (custody) ou mutualisés ? Vous êtes-vous propriétaire direct ou simple créancier ?

02

Valider le statut MiCA de l'émetteur

Vérifier que le stablecoin est un e-money token ou ART autorisé sous MiCA. Contrôler la nature des réserves (cash, dépôts bancaires), les rapports d'audit et le rating éventuel.

03

Diversifier les expositions

Ne pas concentrer sur un seul émetteur, une seule plateforme ou un seul protocole DeFi. La diversification réduit le risque cumulatif des 3 couches.

04

Calibrer l'exposition au risque DeFi

Distinguer stablecoins 'simples' (risque émetteur seul) vs coffres DeFi (risques cumulés : émetteur + protocole + plateforme). Adapter le montant à votre tolérance.

05

Vérifier les couvertures assurantielles

Certaines plateformes proposent des assurances sur les pertes DeFi. Non imposées par MiCA — vérifier plafonds et conditions d'application.

06

Anticiper la liquidité de sortie

S'assurer d'un accès direct à l'émetteur ou un exchange partenaire pour convertir les stablecoins en euros, hors plateforme intermédiaire.

Strategic Advisory on the Future of Programmable Money

Julien Achard

Fondateur & CEO — OpenbanQ

Transaction Banking · Payments · Trade Finance · Digital Assets · Regulatory Intelligence

Ce document est produit à titre informatif. Il ne constitue pas un conseil en investissement.