

MODULE 2 / 6

Créer et sécuriser votre portefeuille numérique

Wallets, clés privées et bonnes pratiques de sécurité.

1. Qu'est-ce qu'un portefeuille crypto (wallet) ?

Un portefeuille numérique ne « contient » pas physiquement vos cryptomonnaies : il stocke les clés cryptographiques (publique et privée) qui prouvent votre propriété sur les actifs enregistrés sur la blockchain et vous permettent de signer des transactions.

Les deux grandes catégories de wallets

- Wallet chaud (hot wallet) : connecté à internet (application mobile, extension navigateur, plateforme d'échange). Pratique pour un usage courant, mais plus exposé aux risques en ligne.
- Wallet froid (cold wallet) : stockage hors ligne (clé matérielle type Ledger/Trezor, ou papier). Recommandé pour la conservation à long terme de montants importants.

2. Clé publique vs clé privée

La clé publique fonctionne comme un numéro de compte que vous pouvez partager pour recevoir des fonds. La clé privée, elle, agit comme un mot de passe absolu : quiconque la détient peut disposer librement des actifs associés.

■ **Point de vigilance** — Ne partagez jamais votre clé privée ni votre phrase de récupération (seed phrase), même avec un support technique. Aucun interlocuteur légitime ne vous la demandera jamais.

3. Étapes de création d'un portefeuille sécurisé

- Choisir un wallet réputé et vérifier ses avis/évaluations avant installation.
- Générer la phrase de récupération et la noter uniquement sur support physique.
- Conserver cette phrase dans un lieu sûr, jamais en photo ni dans le cloud.
- Activer l'authentification à deux facteurs (2FA) sur tous les comptes liés.
- Effectuer un premier test avec un petit montant avant tout transfert important.

4. Réflexes de sécurité au quotidien

- Vérifier systématiquement l'URL des sites avant de saisir des identifiants.
- Se méfier des messages non sollicités promettant des gains rapides.
- Mettre à jour régulièrement les applications et systèmes utilisés.
- Utiliser une adresse e-mail dédiée à vos activités crypto.

Auto-évaluation

Répondez à ces questions pour vérifier votre compréhension avant de passer au module suivant.

1. Que se passe-t-il si quelqu'un obtient votre clé privée ?

- Rien, elle sert uniquement à recevoir des fonds
- Cette personne peut disposer librement de vos actifs
- Le wallet la régénère automatiquement chaque jour

Réponse : Cette personne peut disposer librement de vos actifs.

2. Quel type de wallet est recommandé pour conserver des montants importants sur le long terme ?

- Un wallet chaud connecté en permanence
- Un wallet froid hors ligne
- Aucune protection n'est nécessaire

Réponse : Un wallet froid hors ligne.

Étape suivante : **Module 3 — Découvrir la plateforme Vertex Capital Smart**