

Les portefeuilles de cryptomonnaies

Dans le monde numérique des cryptomonnaies, le wallet crypto ou portefeuille crypto joue un rôle central pour la gestion et la conservation sécurisées des actifs numériques. Mais concrètement, comment se présente un portefeuille crypto et comment fonctionne-t-il? Dans cet article, nous vous présentons les différents types de wallets crypto disponibles, leur fonctionnement et la manière dont ils permettent de gérer les cryptomonnaies.

Quelques points essentiels à retenir:

- Votre portefeuille est à vous et vous en êtes le seul responsable. Le code d'accès à un wallet est le seul moyen d'accéder au capital qui se trouve à l'intérieur. La perte du code d'accès signifie donc irrémédiablement la perte de votre argent.
- Sécurisez votre portefeuille crypto : optez de préférence pour un wallet physique (hardware wallet) hors ligne, et conservez l'identifiant et le code d'accès de votre wallet en prenant toutes les précautions de sécurité (p. ex. offline, sur un support papier conservé en lieu sûr).
- Ne communiquez jamais l'identifiant ni le code d'accès de votre portefeuille crypto, que ce soit par courriel ou par tout autre moyen que ce soit ; ne les saisissez jamais sur une plateforme ou une application douteuse.

Un wallet crypto vous permet de conserver en toute sécurité vos clés privées (à savoir les mots de passe qui vous permettent d'accéder à vos cryptoactifs) et de les utiliser pour envoyer et recevoir des [cryptomonnaies](https://www.ebas.ch/fr/les-cryptomonnaies/) (https://www.ebas.ch/fr/les-cryptomonnaies/) tels que le Bitcoin ou l'Ethereum.

Ainsi, contrairement à un portefeuille normal qui contient de l'argent en espèces, donc palpable, les wallets crypto n'en contiennent pas. Techniquement parlant, ces derniers ne contiennent en effet que des clés d'accès aux adresses où sont stockées les cryptomonnaies sur la blockchain (sur Internet). Ces clés sont une preuve de propriété de ces actifs numériques et vous permettent d'effectuer des transactions. Si vous perdez votre clé privée, vous perdez donc aussi la possibilité d'accéder à votre argent, d'où l'intérêt de la conserver en toute sécurité.

Comment gérer un portefeuille crypto?

Il existe différentes approches de gestion. La première consiste à conserver soi-même les clés privées. On parle alors de wallet en self-custody ou « auto-gardé ». Dans ce cas, l'utilisateur a le contrôle total de ses clés privées et de son portefeuille crypto. Dans la mesure où vous êtes le seul à pouvoir accéder à vos cryptos, cette méthode peut être considérée comme fiable et sûre, à condition d'appliquer toutes les mesures possibles pour les conserver en toute sécurité.

L'alternative consiste à confier le stockage des clés à des tiers (Custodial Services). Dans ce cas, c'est le prestataire qui s'occupe de conserver vos actifs pour vous. En vous permettant de déléguer la responsabilité de la sécurité à un tiers, cette méthode est certes beaucoup plus confortable que la première, même si vous ne pouvez pas exclure les risques de piratage ou de faillite de votre prestataire. Il peut s'agir par exemple de plateformes d'échange, telles que Coinbase ou Binance.

Comment fonctionne un wallet crypto?

Un portefeuille de cryptomonnaies est constitué d'une clé publique et d'une clé privée. La clé publique est l'équivalent du numéro IBAN des comptes bancaires. D'autres utilisateurs peuvent utiliser cette adresse pour envoyer des cryptos sur ce portefeuille. La clé privée consiste en un code secret qui permet d'accéder aux actifs stockés dans le wallet crypto. Celle-ci doit être conservée de la manière la plus sécurisée possible et ne doit jamais être partagée avec qui que ce soit.

Votre portefeuille crypto vous permet ainsi de conserver ces clés en toute sécurité. Pour recevoir des fonds, vous devez partager votre adresse publique avec d'autres utilisateurs, tandis que pour envoyer vous-même des cryptos à quelqu'un, vous devrez nécessairement utiliser votre clé privée.

Quels sont les différents types de wallets crypto?

Les portefeuilles de cryptomonnaies offrent un large éventail d'options, des applications mobiles simples et intuitives aux solutions les plus complexes et les plus sécurisées. Les principaux types de wallets crypto sont les suivants:

Portefeuilles logiciels

Un portefeuille logiciel est basé sur une application qui doit être installée sur un ordinateur ou un appareil mobile. Parmi les différents wallets logiciels disponibles sur le marché, citons les interfaces Electrum et Exodus pour ordinateur, et Trust Wallet ou Mycelium pour les dispositifs mobiles.

Avantages:

- Les clés privées sont stockées localement sur votre appareil, ce qui vous permet de maintenir le contrôle total.
- Certains wallets logiciels peuvent également être utilisés sans connexion Internet.

Inconvénients:

- Le contrôle total signifie que vous devez également assumer l'entière responsabilité de vos clés. Si votre appareil est perdu ou endommagé, et que vous n'avez pas de sauvegarde (backup), vous perdrez irrémédiablement l'accès à votre portefeuille crypto.
- Il convient par ailleurs de considérer que les appareils connectés à Internet sont susceptibles d'être infectés par des maliciels, avec toutes les conséquences que cela comporte.

Portefeuilles en ligne

Un portefeuille en ligne est, comme son nom l'indique, connecté à Internet. On parle également d'un portefeuille chaud, en référence à la connexion Internet et à l'espace de stockage des données sur le cloud. Ce type de wallet permet d'accéder à vos actifs numériques à partir de n'importe quel appareil à condition que celui-ci soit connecté à Internet. Parmi les principaux wallets en ligne, citons par exemple Coinbase et Blockchain.info.

Avantages:

- Accessibles depuis n'importe quel appareil disposant d'une connexion Internet.
- Faciles à configurer et à utiliser, ils conviennent parfaitement aux néophytes.
- Les données étant stockées sur le cloud, la perte du dispositif ne comporte pas la perte du portefeuille.

Inconvénients:

- Le stockage en ligne des clés privées comporte un important risque de sécurité.
- Dans la mesure où vous dépendez complètement du prestataire, vous devez avoir une confiance totale dans les mesures de prévention contre les cyberattaques.

Portefeuilles physiques

Un wallet physique est un appareil dédié au stockage des cryptomonnaies (généralement une clé USB). Dans la mesure où les clés privées sont stockées hors ligne, à l'abri des risques de piratage, les portefeuilles physiques, qui sont également qualifiés de froids, représentent la méthode la plus sécurisée de conserver et de gérer des actifs numériques. Les solutions les plus répandues de portefeuilles physiques sont Ledger et Trezor.

Avantages:

- Sécurité élevée grâce au stockage offline des clés privées.
- Certains wallets physiques offrent des interfaces possibles avec les wallets logiciels.
- Compatibilité avec de nombreuses cryptomonnaies.

Inconvénients:

- Plus chers que les portefeuilles chauds, puisqu'ils supposent un hardware particulier.
- La perte de l'appareil comporte le risque de perte irrémédiable de vos cryptos si vous n'avez pas prédisposé votre phrase de récupération.
- Utilisation plus complexe que les wallets logiciels ou en ligne.

Portefeuilles papier

Un paper wallet ou portefeuille papier est une méthode de stockage hors ligne des cryptomonnaies. Il s'agit tout simplement d'un document physique (une feuille de papier) contenant toutes les informations concernant vos actifs (clés publiques et privées). Cette solution offre donc une manière sûre de conserver des actifs numériques, à l'abri des risques d'attaques en ligne et des logiciels malveillants.

Avantages:

- Protection élevée contre les cybermenaces et notamment contre les risques de piratage.

- Coût très faible, manipulation très simple.
- Particulièrement adaptée au stockage à long terme des cryptomonnaies.

Inconvénients:

- Si le paper wallet est perdu ou endommagé au point que la clé privée n'est plus lisible, vos cryptomonnaies stockées seront irrémédiablement perdues.
- Fastidieux si vous effectuez régulièrement des transactions. Chaque transaction nécessite la saisie manuelle des clés.

Votre portefeuille est à vous et vous en êtes le seul responsable !

Les cryptoactifs sont stockés sous forme numérique dans des portefeuilles ou wallets dont l'accès est protégé par des codes d'accès. Le code d'accès à un wallet est le seul moyen d'accéder au capital qui se trouve à l'intérieur. La perte du code d'accès signifie donc irrémédiablement la perte de l'argent qu'il contient.

Pour protéger votre portefeuille crypto:

- utilisez de préférence un wallet physique (hardware - wallet) hors ligne.
- conservez soigneusement l'identifiant et le code d'accès de votre wallet en prenant toutes les précautions de sécurité (p. ex. offline, sur un support papier conservé en lieu sûr).
- ne communiquez jamais, que ce soit par courriel ou par tout autre moyen que ce soit, l'identifiant et le code d'accès à votre portefeuille; ne les tapez jamais dans une plateforme ou une application douteuse.

Un portefeuille crypto ou wallet crypto (wallet signifie portefeuille en anglais) est un portefeuille numérique qui permet aux utilisateurs de conserver, recevoir et transmettre, en toute sécurité, différentes cryptomonnaies (Bitcoin, Ethereum, etc.). Il s'agit d'un outil indispensable pour la gestion et l'utilisation des cryptomonnaies.