Cryptomonnaies

Février 2023

ITSAP.00.650

Les cryptomonnaies sont des actifs virtuels qui utilisent la cryptographie pour protéger et confirmer la propriété d'actifs. Les cryptomonnaies se divisent en unités, comme « bitcoin » et « ether », et les transactions connexes sont généralement enregistrées dans leurs chaînes de blocs respectives. Les « jetons » représentent une certaine valeur de « monnaie » et servent à acheter des biens et services. Les cryptomonnaies sont échangées sur des systèmes pair à pair et ne sont pas gérées par une autorité centrale, comme une banque, un gouvernement ou un pays. Il existe aujourd'hui des milliers de cryptomonnaies actives, ce qui en complique la réglementation. L'achat, la vente, le transfert et le stockage de cryptomonnaies sont gérés par l'entremise de courtiers conventionnels, de plateformes d'échange ou de particuliers.

Qu'est-ce qu'une chaîne de blocs?

Une chaîne de blocs est un registre public décentralisé et distribué en format numérique dans lequel sont enregistrées les transactions de cryptomonnaies. Les registres distribués sont des systèmes de stockage auxquels on ajoute des données, mais desquels il est impossible de les supprimer. Les données sont stockées à divers points (ou nœuds) sur un réseau partagé et prennent souvent la forme d'une chaîne de blocs.

Les chaînes de blocs servent à enregistrer les transactions de cryptomonnaies. Ces transactions sont enregistrées sur des blocs comportant des signatures cryptographiques et sont irréversibles. De nombreuses copies du registre sont détenues à divers endroits par différentes entités, et un grand nombre de celles-ci sont appelées à valider collectivement l'exactitude des données du nouveau bloc avant de l'ajouter à la chaîne. Une fois que les transactions du bloc sont vérifiées et ajoutées à la chaîne, l'information ne peut plus être modifiée ou trafiquée.

Chaque bloc inclut une confirmation du bloc précédent, ce qui renforce la vérification de l'ensemble de la chaîne de blocs. Les utilisateurs doivent authentifier leurs transactions à l'aide de clés cryptographiques et peuvent accéder à leurs actifs une fois leur identité vérifiée.

Cryptominage

On peut acheter de la monnaie directement avec d'autres cryptomonnaies ou d'autre monnaie légale, mais on peut également avoir recours au cryptominage pour obtenir de la cryptomonnaie. Les utilisateurs se font ainsi concurrence pour résoudre des problèmes qui nécessitent une forte intensité de calcul, souvent au moyen d'ordinateurs très puissants ou de calcul distribué, et pour vérifier les transactions dans le but d'ajouter un nouveau bloc à la chaîne. Ils obtiennent alors une part de la cryptomonnaie en question. Ce processus correspond à la **preuve de travail**. Les cryptomonnaies n'utilisent pas toutes cette méthode. Certaines ont recours à la **preuve d'enjeu**, un mécanisme qui sélectionne au hasard des utilisateurs qui doivent alors valider leurs transactions.

Ce qu'il faut savoir

L'investissement dans les cryptomonnaies soulève sa part d'incertitudes et de risques, notamment :

- des fluctuations de prix attribuables à toute une gamme de facteurs imprévisibles comme la spéculation et la compétition, peuvent fréquemment avoir un impact sur la valeur de votre investissement en crypto-monnaies;
- de la difficulté à liquider les actifs en argent et à utiliser sa cryptomonnaie, car peu de commerçants au Canada acceptent ce type de paiement;
- un manque d'accès aux mêmes protections, car la monnaie fiduciaire réduit la capacité de soumettre des plaintes liées aux transactions;
- si vous utilisez un portefeuille de cryptomonnaie, c'est-à-dire un dispositif inviolable facultatif permettant de stocker vos translations et vos justificatifs d'identité comme votre clé privée et votre mot de passe, mais que vous le perdez, il pourrait être impossible de récupérer vos actifs;
- l'assurance-dépôts d'institutions comme la Société d'assurance-dépôts du Canada (SADC) s'applique uniquement aux dollars canadiens, et aucun régime d'assurance-dépôts fédéral ou provincial ne couvre la cryptomonnaie. Le propriétaire des actifs numériques en assume la seule responsabilité;
- les transactions sont irréversibles, ce qui risque de causer des problèmes si vous n'avez pas reçu votre produit ou si vous souhaitez arrêter un paiement.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-650-2022F-PDF
ISBN 978-0-660-45917-2

Quels sont les risques liés à la cybersécurité?

Hameçonnage et arnaques

- Les attaques par hameçonnage reposent sur une fausse représentation d'une entreprise légitime, comme une plateforme d'échange de cryptomonnaie. L'objectif est de mettre la main sur les justificatifs d'ouverture de session d'utilisateurs.
- Des arnaques offrant gratuitement des cryptomonnaies sont également très courantes. Les auteurs de menace se font alors passer pour des vedettes ou des investisseurs bien connus qui offrent à de nouveaux investisseurs la possibilité d'accroître leurs gains.
- Les auteurs de menace peuvent avoir recours à toute une gamme de stratagèmes de fraude liés aux cryptomonnaies, comme de fausses plateformes d'échange, des pyramides de Ponzi et des arnaques de soutien technique, dans le but de duper leurs victimes et d'accéder à leurs portefeuilles de cryptomonnaie.

Services tiers

- Les investisseurs en cryptomonnaie peuvent utiliser des applications tierces pour gérer leurs actifs numériques. Si un auteur de menace réussit à s'introduire dans l'application, l'information du compte d'utilisateur sera alors compromise..

Maliciels de minage et robots d'échange

- Les auteurs de menace utilisent des maliciels de minage pour miner clandestinement de la cryptomonnaie sur l'appareil d'un utilisateur. Le maliciel est déployé au moyen d'attaques par hameçonnage ou de publicités Web malveillantes et se sert ensuite des ressources d'un appareil pour générer des cryptomonnaies pouvant être échangées.
- Les auteurs de menace peuvent également effectuer du cryptominage pirate en volant les clés privées du portefeuille d'un utilisateur pour accéder à ses actifs numériques.
- Les investisseurs en cryptomonnaie utilisent souvent des robots d'échange qui permettent d'automatiser les opérations d'échange. Or, les auteurs de menace peuvent donner à leur maliciel l'apparence d'un programme ou d'un logiciel de robot d'échange. Lorsque l'utilisateur télécharge le faux robot, le maliciel infecte son appareil.

Plateformes d'échange frauduleuses

- De nouvelles plateformes d'échange permettant d'investir dans les cryptomonnaies ou de les échanger continuent d'être lancées, mais elles ne sont pas toutes légitimes. Dans certains cas, des entreprises de cryptomonnaie semblaient dignes de confiance à première vue, mais on a fini par découvrir qu'il s'agissait d'arnaques de marketing à paliers multiples.

Atténuer les risques

Il est important de bien comprendre les risques liés à la cybersécurité dans le contexte de la cryptomonnaie pour se protéger contre la fraude, les maliciels et les cyberattaques. Vous pouvez appliquer plusieurs stratégies afin d'atténuer les risques et de protéger votre portefeuille numérique.

- Stockez et chiffrez vos clés privées et justificatifs d'ouverture de session sur un dispositif matériel inviolable conçu à cette fin pour gérer les transactions et les justificatifs d'identité associés à la cryptomonnaie.
- Utilisez un antivirus, tenez les logiciels et les systèmes d'exploitation à jour et utilisez des mots de passe robustes.
- Faites des recherches approfondies sur les entreprises et leurs cryptomonnaies avant d'investir et tenez-vous au courant de l'actualité et des annonces dans le domaine de la cryptomonnaie en consultant des sources fiables.
- Désinstallez les logiciels que vous n'utilisez pas et surveillez votre appareil et les activités sur votre réseau pour détecter toute anomalie.
- Ignorez les offres non sollicitées qui vous invitent à investir dans des cryptomonnaies, de même que les publicités et liens suspects.
- Installez des extensions anti-minage clandestin et des bloqueurs de publicité pour protéger votre appareil.
- Assurez-vous de sécuriser les applications tierces, par exemple au moyen de listes d'applications autorisées et de listes de rejet, et en séparant les données personnelles et les données professionnelles.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.