



PATRIMOINE Comment sécuriser son portefeuille de cryptomonnaies

La faillite de la plateforme FTX touche des centaines de milliers de clients.

La faillite de la plateforme FTX, spécialisée dans l'échange de cryptomonnaies, a provoqué une chute des cours de ces actifs numériques. Les investisseurs ont été surpris par la rapidité de la dégradation de la plateforme, qui avait été présentée comme l'un des plus importants acteurs du marché. Les investisseurs ont été surpris par la rapidité de la dégradation de la plateforme, qui avait été présentée comme l'un des plus importants acteurs du marché.

Les plateformes d'échange de cryptomonnaies, en anglais les crypto exchanges, ont connu une croissance fulgurante ces dernières années. Elles permettent aux investisseurs de acheter et vendre des cryptomonnaies. Cependant, la faillite de FTX a remis en question la sécurité de ces plateformes.

Comment sécuriser son portefeuille de cryptomonnaies ? Les investisseurs doivent être vigilants et privilégier les plateformes réputées. Il est également important de diversifier son portefeuille et de ne pas investir trop d'argent dans un seul actif.

Les plateformes d'échange de cryptomonnaies sont soumises à des réglementations strictes. Les investisseurs doivent vérifier que la plateforme qu'ils utilisent est agréée par les autorités compétentes.

Il est également important de privilégier les plateformes qui offrent des services de stockage sécurisés. Les investisseurs doivent également être conscients des risques liés à la volatilité des cryptomonnaies.

En conclusion, la faillite de FTX a souligné l'importance de la sécurité et de la transparence dans le secteur des cryptomonnaies. Les investisseurs doivent être vigilants et privilégier les plateformes réputées.



blan. Les principes de base de la sécurité sont de ne pas divulguer sa clé privée, de ne pas la stocker sur un ordinateur ou un téléphone portable, et de ne pas la partager avec quelqu'un. Les portefeuilles matériels sont une solution pour éviter ces risques. Ils sont conçus pour être utilisés via un ordinateur ou un téléphone portable, mais la clé privée est stockée sur un support physique, généralement une clé USB. Cela permet de signer les opérations sans révéler la clé privée à l'ordinateur ou au téléphone. Les portefeuilles matériels sont également plus résistants aux attaques physiques, car ils sont souvent conçus pour être utilisés dans des environnements non sécurisés.



« Pour avoir accès à votre portefeuille, vous aurez besoin d'être connecté via votre ordinateur ou votre téléphone portable. Vous devenez une cible potentielle pour un hacker désireux de s'emparer de votre clé privée, observe Guillaume Eyssette, directeur associé du cabinet de gestion en patrimoine Gefinéo. La solution consiste à utiliser un hardware wallet ou portefeuille matériel. Ce dispositif, de la forme d'une clé USB, permet, via un mécanisme cryptographique, de signer ses opérations, de prouver que vous êtes bien le propriétaire du wallet, sans toutefois révéler votre clé privée à votre ordinateur. »