Clés publiques et clés privées

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Chaque compte sur un registre distribué est contrôlé par une paire de clés. La clé privée est un très grand nombre aléatoire. La clé publique en est dérivée par une fonction mathématique à sens unique. L'adresse qui apparaît sur le registre est à son tour dérivée de la clé publique. Chacun peut envoyer des jetons à une adresse. Seul le détenteur de la clé privée correspondante peut signer une transaction qui en fait sortir des jetons. La signature prouve le contrôle sans révéler la clé elle-même.

C'est le fait technique le plus important de tout l'ouvrage. La clé privée est la seule chose qui confère un pouvoir de disposition de fait sur un jeton. Il n'existe ni registre des propriétaires, ni décision de justice à laquelle le réseau obéirait, ni exploitant central capable d'annuler un transfert. Celui qui connaît la clé peut dépenser. Celui qui ne la connaît pas ne le peut pas, quoi que disent un contrat ou un jugement. Le droit privé suisse a fondé toute son analyse des crypto-actifs sur ce fait. C'est pourquoi le rapport du Conseil fédéral de 2018 a conclu que les purs jetons de paiement ne sont ni des choses au sens des art. 641 ss du Code civil (CC ; ZGB) ni des créances, mais des positions de contrôle de fait auxquelles le droit attache des conséquences.[1]

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Les juridictions singapouriennes sont parvenues à une conclusion conceptuelle différente à partir du même point de départ. Dans ByBit Fintech Ltd v Ho Kai Xin, la High Court a jugé que l'USDT est un thing in action et donc un bien susceptible d'être détenu en trust. Elle a raisonné à partir de la faculté du détenteur d'exclure les tiers grâce au contrôle de la clé.[2] Le fait technique est identique dans les deux systèmes juridiques. Ce qui diffère, c'est la catégorie doctrinale dans laquelle chaque système le range. La partie D, chapitre I, et la partie J, chapitre I approfondissent la comparaison.

Phrases de récupération, dérivation et sens pratique d'« une clé »

Les portefeuilles modernes ne stockent pas une seule clé privée. Ils stockent une graine (seed), généralement présentée à l'utilisateur sous la forme de douze ou vingt-quatre mots anglais, à partir de laquelle un nombre illimité de paires de clés est dérivé de manière déterministe selon les normes BIP-32 et BIP-39. Quiconque détient la graine détient toutes les adresses qui en sont dérivées, sur toutes les chaînes prises en charge. Pour un exécuteur testamentaire, un liquidateur ou un procureur, cela signifie que la récupération d'une seule phrase de récupération peut donner le contrôle de centaines d'adresses. L'inventaire des avoirs d'un défunt ou d'un failli doit donc partir des graines et non des adresses individuelles.[3]

Exemple

Un fondateur établi à Zoug décède en 2026 en laissant un portefeuille matériel et une enveloppe scellée contenant vingt-quatre mots. Son testament désigne un exécuteur testamentaire à Zurich et lègue « mes bitcoins » à sa fille. L'exécuteur qui traite ces mots comme le mot de passe d'un seul compte passera à côté de l'ether, des stablecoins et des actions tokenisées détenus sous d'autres chemins de dérivation à partir de la même graine. L'exécuteur qui comprend la dérivation analysera tous les chemins courants sur tous les grands réseaux avant d'établir l'inventaire requis par l'art. 553 CC. La partie D, chapitre VIII, et la partie P, chapitre VIII reviennent sur le volet planification de ce problème.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Notes

1. Rapport du Conseil fédéral du 14 décembre 2018, section 5.1.1 (qualification juridique des jetons ; absence de droit réel au sens du Code civil ; pouvoir de disposition de fait comme critère de rattachement). Les conséquences de droit civil sont développées dans la partie D, chapitre I. ↩
2. ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199 (Philip Jeyaretnam J), disponible sur eLitigation sous la référence 2023_SGHC_199 ; l'analyse relative à la qualification de bien figure dans la partie du jugement consacrée à la question de savoir si l'USDT est susceptible d'être détenu en trust. ↩
3. Bitcoin Improvement Proposals BIP-32 (Hierarchical Deterministic Wallets, 2012) et BIP-39 (Mnemonic code for generating deterministic keys, 2013), github.com/bitcoin/bips. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.