公開鍵と秘密鍵

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

分散型台帳上のすべてのアカウントは、鍵ペアによって管理されています。秘密鍵とは、非常に大きな乱数です。公開鍵は、一方向の数学的関数によって秘密鍵から導き出されます。台帳上に表示されるアドレスは、さらにその公開鍵から導き出されます。誰でも、あるアドレスにトークンを送ることができます。しかし、そのアドレスからトークンを移動させる取引に署名できるのは、対応する秘密鍵の保有者だけです。署名は、鍵そのものを明かすことなく、支配していることを証明します。

これは本書全体を通じて最も重要な技術的事実です。トークンに対する事実上の処分権を与えるのは、秘密鍵だけです。所有者の登録簿も、ネットワークが従う裁判所の命令も、移転を取り消せる中央の運営者も存在しません。鍵を知っている者は使うことができます。知らない者は、契約や判決が何と言おうと使うことができません。スイスの私法は、暗号資産に関する分析のすべてをこの事実の上に築いてきました。連邦参事会が2018年の報告書で、純粋なペイメント・トークンは民法典（CC、ZGB）第641条以下にいう物でも債権でもなく、法が一定の効果を結びつける事実上の支配の地位であると結論づけたのは、そのためです。[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.

シンガポールの裁判所は、同じ出発点から異なる概念上の結論に至りました。ByBit Fintech Ltd v Ho Kai Xin事件において、高等法院は、鍵の支配を通じて他者を排除できるという保有者の能力から論じ、USDTは無体動産（thing in action）であり、したがって信託財産として保有可能な財産であると判示しました。[2] 技術的事実は両法体系で同一です。異なるのは、それぞれの法体系がその事実を収める法理上の枠組みです。第D部第I章および第J部第I章では、この比較をさらに掘り下げています。

シードフレーズ、鍵の導出、「一つの鍵」の実際上の意味

現代のウォレットは、一つの秘密鍵を保存しているわけではありません。保存しているのはシードであり、通常は12個または24個の英単語としてユーザーに表示されます。BIP-32およびBIP-39の規格に基づき、このシードから無数の鍵ペアが決定論的に導き出されます。シードを保有する者は、対応するすべてのチェーン上で、そこから導き出されたすべてのアドレスを保有することになります。遺言執行者、清算人、検察官にとって、これは一つのシードフレーズを回収すれば数百のアドレスに対する支配を得られる可能性があることを意味します。また、故人や破産者の保有資産の目録作成は、個々のアドレスからではなく、シードから始めなければならないことも意味します。[3]

事例

ツークを拠点とする創業者が2026年に死亡し、ハードウェアウォレットと、24個の単語が記された封印された封筒を遺しました。遺言ではチューリッヒの遺言執行者が指定され、「私のビットコイン」は娘に遺贈されています。この単語を一つのアカウントのパスワードとして扱う遺言執行者は、同じシードから別の導出パスで保有されているイーサ、ステーブルコイン、トークン化株式を見落とすでしょう。鍵の導出を理解している遺言

© 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.

執行者は、民法典第553条が求める財産目録を作成する前に、主要なすべてのネットワークにおいて一般的なすべてのパスを調べます。第D部第VIII章および第P部第VIII章では、この問題の対策の側面を改めて取り上げます。

注

1. 2018年12月14日付連邦参事会報告書, 第5.1.1節（トークンの法的分類、民法典上の所有権に当たらないこと、連結点としての事実上の処分権）。民事法上の帰結については第D部第I章で詳述している。 ↩
2. ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199 (Philip Jeyaretnam J), eLitigationにて2023_SGHC_199として閲覧可能; 財産性の分析は、USDTが信託財産として保有可能かどうかを論じた判決の節にある。 ↩
3. Bitcoin Improvement Proposals BIP-32 (Hierarchical Deterministic Wallets, 2012) および 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.

© 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.

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.