Açık ve özel anahtarlar

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

Dağıtık bir defterdeki her hesap bir anahtar çifti tarafından kontrol edilir. Özel anahtar çok büyük, rastgele bir sayıdır. Açık anahtar, ondan tek yönlü bir matematiksel fonksiyonla türetilir. Defterde görünen adres de açık anahtardan türetilir. Herkes bir adrese token gönderebilir. Ancak o adresten token çıkaran bir işlemi yalnızca karşılık gelen özel anahtarın sahibi imzalayabilir. İmza, anahtarın kendisini açığa çıkarmadan kontrolü kanıtlar.

Bu, kitabın tamamındaki en önemli teknik olgudur. Bir token üzerinde fiilî tasarruf yetkisi veren tek şey özel anahtardır. Ne bir malikler sicili vardır, ne ağın uyacağı bir mahkeme kararı ne de bir transferi geri alabilecek merkezî bir işletici. Anahtarı bilen kişi harcayabilir. Bilmeyen kişi ise, bir sözleşme veya mahkeme kararı ne derse desin, harcayamaz. İsviçre özel hukuku, kripto varlıklara ilişkin tüm analizini bu olgu üzerine kurmuştur. Federal Konseyin 2018 raporunun, saf ödeme tokenlerinin ne İsviçre Medeni Kanununun (ZGB/CC) 641 vd. maddeleri anlamında eşya ne de alacak olduğu, bunların hukukun sonuç bağladığı fiilî kontrol konumları olduğu sonucuna varmasının nedeni budur.[1]

Singapur mahkemeleri aynı başlangıç noktasından farklı bir kavramsal sonuca ulaştı. ByBit Fintech Ltd v Ho Kai Xin davasında Yüksek Mahkeme (High Court), USDT'nin bir alacak hakkı (thing in action) ve dolayısıyla trust kapsamında

© 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.

tutulabilen bir mülk olduğuna hükmetti. Mahkeme gerekçesini, token sahibinin anahtarı kontrol ederek başkalarını dışlayabilmesine dayandırdı.[2] Teknik olgu her iki hukuk sisteminde de aynıdır. Farklı olan, her sistemin onu yerleştirdiği doktrinel kategoridir. D. Kısım, I. Bölüm ve J. Kısım, I. Bölüm karşılaştırmayı daha ileri götürür.

Kurtarma ifadeleri, türetme ve "tek anahtarın" pratik anlamı

Modern cüzdanlar tek bir özel anahtar saklamaz. Kullanıcıya genellikle on iki veya yirmi dört İngilizce kelime olarak gösterilen bir tohum (seed) saklarlar. BIP-32 ve BIP-39 standartlarına göre bu tohumdan deterministik olarak sınırsız sayıda anahtar çifti türetilir. Tohumu elinde tutan kişi, desteklenen her zincirde ondan türetilen tüm adreslere sahiptir. Bir vasiyeti tenfiz memuru, tasfiye memuru veya savcı için bu şu anlama gelir: Tek bir kurtarma ifadesinin ele geçirilmesi yüzlerce adres üzerinde kontrol sağlayabilir. Ölen ya da iflas eden bir kişinin varlıklarının envanteri de tek tek adreslerden değil, tohumlardan başlamalıdır.[3]

Örnek

Zug'da yaşayan bir girişimci 2026'da ölür ve geride bir donanım cüzdanı ile yirmi dört kelimenin yazılı olduğu mühürlü bir zarf bırakır. Vasiyetnamesi Zürih'te bir vasiyeti tenfiz memuru atar ve "Bitcoin'lerimi" kızına bırakır. Kelimeleri tek bir hesabın şifresi olarak gören vasiyeti tenfiz memuru, aynı tohumdan farklı türetme yollarıyla tutulan Ether'i, stablecoin'leri ve tokenize payları gözden kaçırır. Türetme mantığını anlayan memur ise Medeni Kanun md. 553'ün öngördüğü envanteri hazırlamadan önce tüm büyük ağlarda yaygın kullanılan her yolu tarar. D. Kısım, VIII. Bölüm ve P. Kısım, VIII. Bölüm bu sorunun planlama boyutuna geri döner.

Notlar

1. Federal Konseyin 14 Aralık 2018 tarihli raporu, bölüm 5.1.1 (tokenlerin hukuki niteliği; Medeni Kanun anlamında mülkiyet hakkı bulunmaması; bağlama

© 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.

noktası olarak fiilî tasarruf yetkisi). Medeni hukuk sonuçları D. Kısım, I. Bölümde ele alınmaktadır. ↩

2. ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199 (Philip Jeyaretnam J), eLitigation'da 2023_SGHC_199 olarak erişilebilir; mülkiyet analizi, kararın USDT'nin trust kapsamında tutulup tutulamayacağına ilişkin bölümündedir. ↩

3. Bitcoin Improvement Proposals BIP-32 (Hierarchical Deterministic Wallets, 2012) ve 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