Public and private keys

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

Every account on a distributed ledger is controlled by a key pair. The private key is a very large random number. The public key is derived from it by a one-way mathematical function. The address that appears on the ledger is in turn derived from the public key. Anyone may send tokens to an address. Only the holder of the corresponding private key can sign a transaction that moves tokens away from it. Signing proves control without revealing the key itself.

This is the single most important technical fact in the entire book. The private key is the only thing that gives factual power of disposal over a token. There is no register of owners, no court order that the network will obey, and no central operator who can reverse a transfer. A person who knows the key can spend. A person who does not cannot, whatever a contract or a judgment says. Swiss private law has built its entire analysis of crypto assets on this fact, which is why the Federal Council's 2018 report concluded that pure payment tokens are neither things under Art. 641 ff. of the Civil Code (CC; ZGB) nor claims, but positions of factual control that the law attaches consequences to.[1]

Singapore's courts reached a different conceptual destination from the same starting point. In ByBit Fintech Ltd v Ho Kai Xin the High Court held that USDT is a thing in action and therefore property capable of being held on trust, reasoning from the

© 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.

holder's ability to exclude others through control of the key.[2] The technical fact is identical in both legal systems. What differs is the doctrinal box into which each system places it. Part D, Chapter I and Part J, Chapter I take the comparison further.

Seed phrases, derivation and the practical meaning of "one key"

Modern wallets do not store one private key. They store a seed, usually displayed to the user as twelve or twenty-four English words, from which an unlimited number of key pairs is derived deterministically under the BIP-32 and BIP-39 standards. Whoever holds the seed holds every address derived from it on every supported chain. For an executor, a liquidator or a prosecutor, this means that recovering one seed phrase may yield control over hundreds of addresses, and that an inventory of a deceased's or a bankrupt's holdings must start from seeds and not from individual addresses.[3]

Example

A Zug-based founder dies in 2026 leaving a hardware wallet and a sealed envelope with twenty-four words. His will appoints an executor in Zürich and leaves "my Bitcoin" to his daughter. The executor who treats the words as a password to one account will miss the Ether, the stablecoins and the tokenised shares held under other derivation paths from the same seed. The executor who understands derivation will scan every common path across every major network before preparing the inventory required by Art. 553 CC. Part D, Chapter VIII and Part P, Chapter VIII return to the planning side of this problem.

Notes

1. Federal Council report of 14 December 2018, section 5.1.1 (legal classification of tokens; no property right in the sense of the Civil Code; factual power of disposal as the connecting factor). The civil-law consequences are developed in Part D, Chapter I. ↩

© 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.

2. ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199 (Philip Jeyaretnam J), available on eLitigation as 2023_SGHC_199; the property analysis is in the section of the judgment on whether USDT is capable of being held on trust. ↩

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