Öffentliche und private Schlüssel

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

Jedes Konto in einem verteilten Register wird über ein Schlüsselpaar kontrolliert. Der private Schlüssel ist eine sehr große Zufallszahl. Der öffentliche Schlüssel wird daraus über eine mathematische Einwegfunktion abgeleitet. Die Adresse, die im Register erscheint, wird wiederum aus dem öffentlichen Schlüssel abgeleitet. Jeder kann Token an eine Adresse senden. Nur wer den zugehörigen privaten Schlüssel hält, kann eine Transaktion signieren, die Token von dort wegbewegt. Die Signatur beweist die Kontrolle, ohne den Schlüssel selbst preiszugeben.

Das ist die wichtigste technische Tatsache des gesamten Buches. Der private Schlüssel ist das Einzige, was tatsächliche Verfügungsmacht über einen Token verschafft. Es gibt kein Eigentümerregister, keine gerichtliche Anordnung, der das Netzwerk gehorcht, und keinen zentralen Betreiber, der eine Übertragung rückgängig machen kann. Wer den Schlüssel kennt, kann verfügen. Wer ihn nicht kennt, kann es nicht, gleichgültig, was ein Vertrag oder ein Urteil sagt. Das Schweizer Privatrecht hat seine gesamte Analyse von Kryptowerten auf dieser Tatsache aufgebaut. Deshalb kam der Bundesrat in seinem Bericht von 2018 zu dem Schluss, dass reine Zahlungstoken weder Sachen im Sinne von Art. 641 ff. des Zivilgesetzbuches (ZGB) noch Forderungen sind. Sie sind Positionen tatsächlicher Herrschaft, an die das Recht Folgen knüpft.[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.

Die Singapurer Gerichte gelangten vom selben Ausgangspunkt zu einem anderen dogmatischen Ergebnis. In ByBit Fintech Ltd v Ho Kai Xin entschied der High Court, dass USDT ein „thing in action" und damit Eigentum (property) ist, das Gegenstand eines Trusts sein kann. Er begründete dies mit der Fähigkeit des Inhabers, andere durch die Kontrolle über den Schlüssel auszuschließen.[2] Die technische Tatsache ist in beiden Rechtsordnungen identisch. Verschieden ist die dogmatische Schublade, in die jede Rechtsordnung sie legt. Teil D, Kapitel I und Teil J, Kapitel I führen den Vergleich weiter.

Seed-Phrasen, Ableitung und die praktische Bedeutung von „einem Schlüssel"

Moderne Wallets speichern nicht einen privaten Schlüssel. Sie speichern einen Seed, dem Nutzer meist als zwölf oder vierundzwanzig englische Wörter angezeigt, aus dem nach den Standards BIP-32 und BIP-39 deterministisch beliebig viele Schlüsselpaare abgeleitet werden. Wer den Seed hält, hält jede daraus abgeleitete Adresse auf jeder unterstützten Chain. Für einen Willensvollstrecker, einen Liquidator oder eine Staatsanwaltschaft bedeutet das: Wer eine einzige Seed-Phrase sicherstellt, kann damit die Kontrolle über Hunderte von Adressen erlangen. Ein Inventar der Bestände eines Verstorbenen oder eines Konkursiten muss daher bei den Seeds ansetzen und nicht bei einzelnen Adressen.[3]

Beispiel

Ein in Zug ansässiger Gründer stirbt 2026. Er hinterlässt ein Hardware-Wallet und einen versiegelten Umschlag mit vierundzwanzig Wörtern. Sein Testament setzt einen Willensvollstrecker in Zürich ein und vermacht „meine Bitcoin" seiner Tochter. Ein Willensvollstrecker, der die Wörter als Passwort für ein einzelnes Konto behandelt, übersieht Ether, Stablecoins und tokenisierte Aktien, die unter anderen Ableitungspfaden desselben Seeds gehalten werden. Ein Willensvollstrecker, der die Ableitung versteht, durchsucht jeden gängigen Pfad in

© 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.

jedem wichtigen Netzwerk, bevor er das nach Art. 553 ZGB erforderliche Inventar erstellt. Teil D, Kapitel VIII und Teil P, Kapitel VIII kommen auf die Planungsseite dieses Problems zurück.

Anmerkungen

1. Bericht des Bundesrates vom 14. Dezember 2018, Abschnitt 5.1.1 (rechtliche Qualifikation von Token; kein Sachenrecht im Sinne des Zivilgesetzbuches; tatsächliche Verfügungsmacht als Anknüpfungspunkt). Die zivilrechtlichen Folgen werden in Teil D, Kapitel I entwickelt. ↩
2. ByBit Fintech Ltd v Ho Kai Xin [2023] SGHC 199 (Philip Jeyaretnam J), abrufbar auf eLitigation als 2023_SGHC_199; die eigentumsrechtliche Analyse findet sich im Abschnitt des Urteils zur Frage, ob USDT Gegenstand eines Trusts sein kann. ↩
3. Bitcoin Improvement Proposals BIP-32 (Hierarchical Deterministic Wallets, 2012) und 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.