

The Custody Illusion

Die Regeln der professionellen Lagerung & Begriffserklärung

Teil 1: Die Regeln der professionellen Lagerung

01 | Die Hot-Wallet- & Börsen-Illusion: Börsen und internetverbundene Wallets (Hot Wallets) sind Marktplätze und Geldbörsen für den Alltag – keine Tresore. Wer Summen, deren Verlust schmerzt, online lagert, delegiert die Sicherheit an Dritte und riskiert den Totalverlust.

02 | Der analoge Ursprung (Keine digitale Speicherung): Eine Seed-Phrase darf niemals abfotografiert, in einer Cloud, einer E-Mail oder einem Passwortmanager gespeichert werden. Echte Sicherheit ist zwingend analog und offline (Air-Gapped).

03 | Die absolute rote Linie (Niemand fragt nach dem Seed): Kein legitimer Dienstleister, keine Wallet-Software und auch wir bei Montfort Key Vault werden jemals Ihre Seed-Phrase abfragen. Jede Aufforderung zur Eingabe auf einer Website oder am Telefon ist ein Betrugsversuch.

04 | Physische Resilienz (Stahl statt Papier): Papier verbrennt, verblasst oder wird durch Wasser zerstört. Wahre Sicherheit auf Generationen-Ebene erfordert die Stanzung oder Gravur des Seeds in säure- und feuerfesten Edelstahl (Steel-Backup).

05 | Geografische Redundanz: Ein Tresor im eigenen Haus schützt nicht vor Bränden, Naturkatastrophen oder Home-Invasion. Backups müssen zwingend an mindestens zwei geografisch voneinander getrennten, hochsicheren Standorten (z. B. VdS-zertifizierte Anlagen) gelagert werden.

06 | Die Passphrase-Architektur (Das 25. Wort): Ein zusätzliches, selbst gewähltes Passwort, das den eigentlichen Seed nochmals verschlüsselt. Fällt das Steel-Backup in falsche Hände, bleibt das Vermögen ohne die Passphrase sicher. Wichtig: Seed und Passphrase dürfen niemals am selben Ort gelagert werden.

07 | Fortgeschrittene Seed-Verteilung (Multisig & Shamir): Den physischen Seed mit der Schere in zwei Hälften zu schneiden, stellt ein mathematisches Risiko dar. Professionelle Setups nutzen kryptografische Aufteilungen (Shamir's Secret Sharing) oder verteilte Signaturen (Multi-Signature), um 'Single Points of Failure' restlos auszuschließen.

Teil 2: Die Montfort Begriffserklärung (Glossar)

Hot Wallet vs. Cold Wallet: Eine 'Hot Wallet' ist ein internetverbundenes System (z.B. App auf dem Smartphone) und damit permanent potenziellen Angriffen ausgesetzt. Eine 'Cold Wallet' (Hardware-Wallet) generiert und lagert die Schlüssel komplett offline (kalt) und ist somit manipulationssicher.

Seed-Phrase (Recovery Seed): Die 12 oder 24 englischen Wörter, die den ultimativen Master-Schlüssel zu Ihrem Vermögen darstellen. Wer diese Wörter besitzt, hat die absolute Kontrolle über die Wallet.

Passphrase (Das 25. Wort): Ein optionales, zusätzliches und völlig frei wählbares Passwort. Es wird an die Seed-Phrase angehängt und generiert eine komplett neue Wallet. Es dient als ultimativer Schutzmechanismus, falls der physische Seed gestohlen wird.

Multi-Signature (Multisig): Ein kryptografisches Schließfach-System, bei dem mehrere Schlüssel generiert werden. Um eine Transaktion auszulösen, wird ein Quorum (z. B. 2 von 3 Schlüsseln) benötigt. Der Standard für Corporate Treasuries und Family Offices.

Redundanz: Die bewusste, geografisch getrennte Mehrfachauslegung von Backups (Sicherungs-Fragmenten). Sie stellt sicher, dass beim Ausfall oder der Zerstörung eines Standorts (z.B. durch Brand) der Zugriff auf das Vermögen weiterhin garantiert ist.