AUSGEWÄHLTE ASPEKTE DER KRYPTOVERWAHRUNG

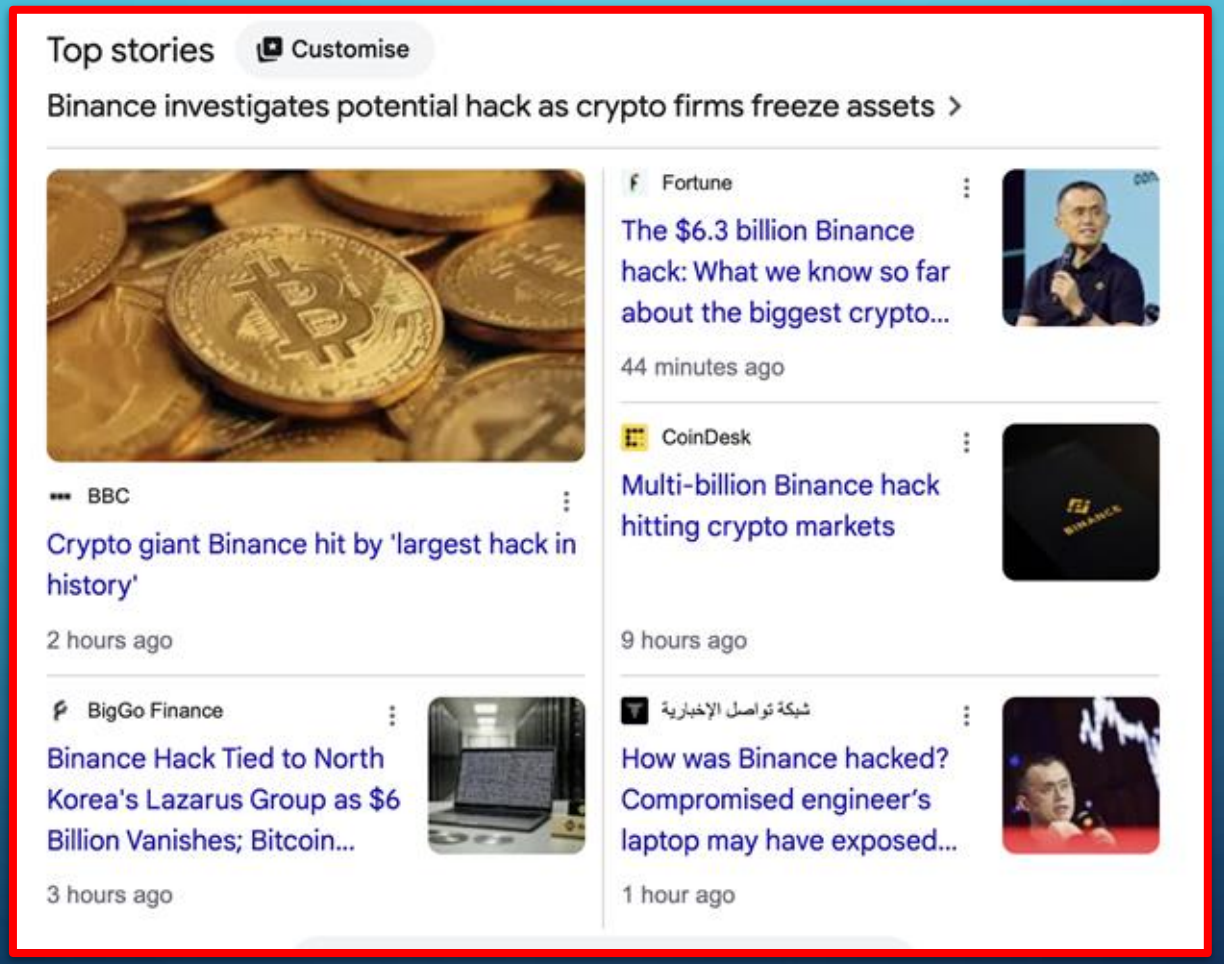
59. SWISS COMPLIANCE OFFICERS MEETING (SCOM)
5. NOVEMBER 2026, SIX CONVENTION POINT, ZÜRICH

FABIO ANDREOTTI, OBLIGATE AG

AGENDA

1. Kryptoverwahrung im Spannungsfeld von Recht und Technologie
2. Praktische Anwendungsbeispiele mit Compliance- und Risk-Bezug
3. Diskussion im Plenum

1. KRYPTOVERWAHRUNG IM SPANNUNGSFELD VON RECHT UND TECHNOLOGIE



Google News, 30. Oktober 2026

1. KRYPTOVERWAHRUNG IM SPANNUNGSFELD VON RECHT UND TECHNOLOGIE



https://www.bloomberg.com/news/articles/2026-08-03/hackers-target-bitcoin-s-safest-hiding-place-in-ongoing-attack



Tech

Ledger says unauthorized implant found in at least one device sold by CryptoBilis

Ledger confirmed an unauthorized hardware implant in a device linked to crypto losses at CryptoBilis, a Southeast Asian reseller. The company says confirmed cases are limited and its internal systems remain unaffected.

By Omkar Godbole, AI Boost | Edited by Jamie Crawley

Oct 12, 2026, 3:49 a.m. EDT

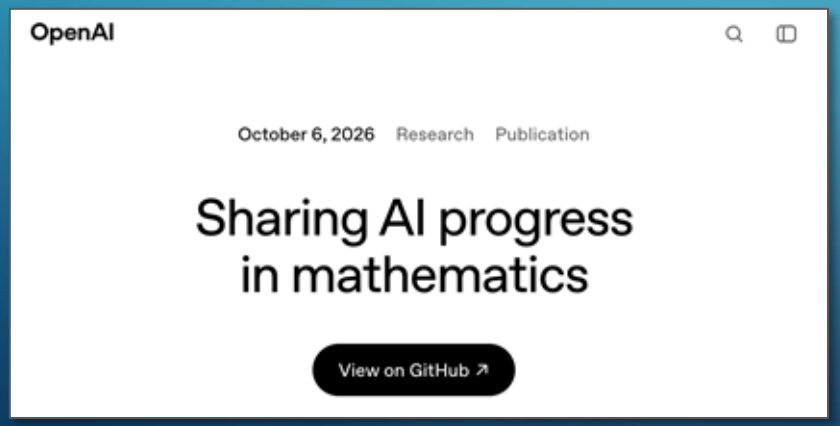
3 min read Share Make CoinDesk preferred on Google

https://www.coindesk.com/tech/2026/10/12/ledger-says-unauthorized-implant-found-in-at-least-one-device-sold-by-cryptobilis

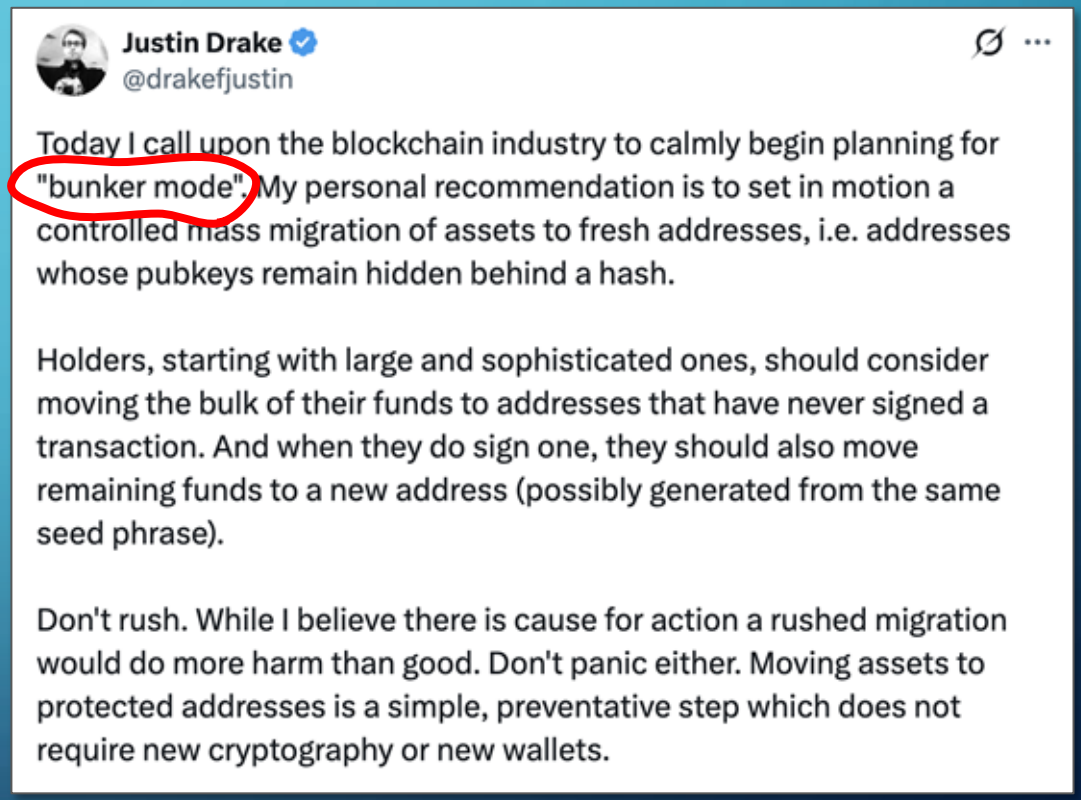
1. KRYPTOVERWAHRUNG IM SPANNUNGSFELD VON RECHT UND TECHNOLOGIE



https://arxiv.org/abs/2603.28846



https://openai.com/index/sharing-ai-progress-in-mathematics/



https://x.com/drakefjustin/status/2107837081313505768

1. KRYPTOVERWAHRUNG IM SPANNUNGSFELD VON RECHT UND TECHNOLOGIE

Quantum Computing
Post-Quanten-Signaturen



HSM und MPC als Markt-Standards
u.a. Policy-Kontrollen setzen Grenzen

Schlüsselerzeugung und Freigabeprozesse
Coldcard-Hack (Juli 2026),
Bitget-Hack (Sept. 2026)

Lieferketten-Risiken
Trust Software-Wallet (Jan. 2026),
Ledger Hardware-Wallet (Okt. 2026)

Hacking & Social Engineering
v.a. staatlich-gesponserte Aktivitäten

1. KRYPTOVERWAHRUNG IM SPANNUNGSFELD VON RECHT UND TECHNOLOGIE

Zivilrecht

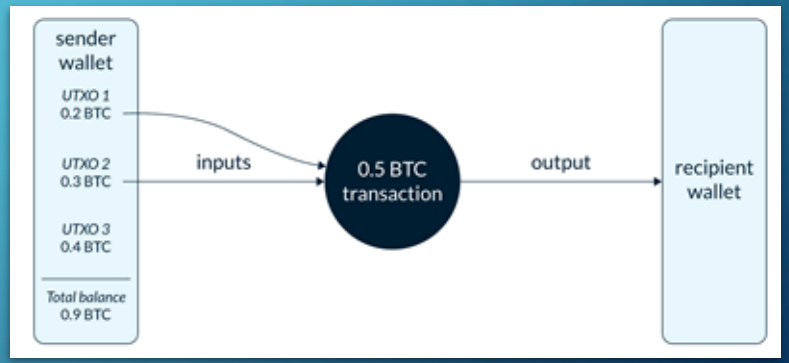
- Kryptowährungen: faktische Vermögenswerte, kein Eigentum möglich
- Verwahrvertrag: Auftrag (Art. 394 ff. OR) mit Hinterlegungselementen

Konkursrecht

- Aussonderung bei jederzeitiger Bereithaltung und Zuordnung zum Kunden
- Art. 37d BankG (von Amtes wegen) bzw. Art. 242a SchKG (auf Antrag)

Aufsichtsrecht

- GwG grundsätzlich stets anwendbar; Bewilligungspflicht nach BankG je nach Verwahrungsmodell
- FINMA-Praxis (insb. AM 08/2023, AM 01/2026, DARP)
- FINIG-Revision geplant



https://www.mtpelerin.com/blog/how-do-bitcoin-transactions-work

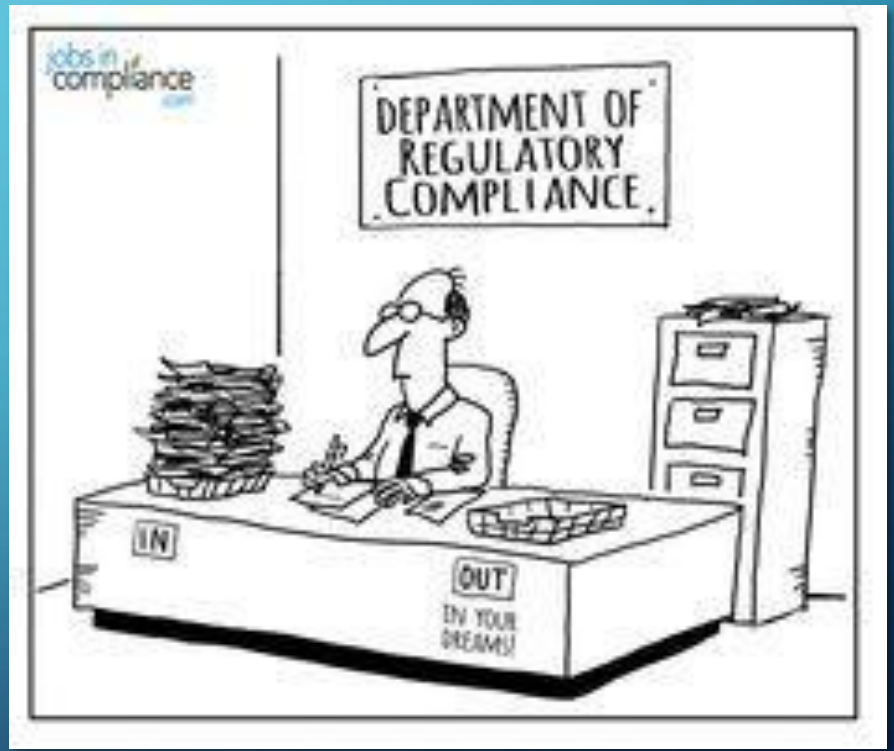
2. PRAKTISCHE ANWENDUNGSBEISPIELE MIT COMPLIANCE- UND RISK-BEZUG

2.1 Private Keys & Cyber-Risiken

2.2 Segregierung & Konkursschutz

2.3 Unterverwahrung & Auslagerung

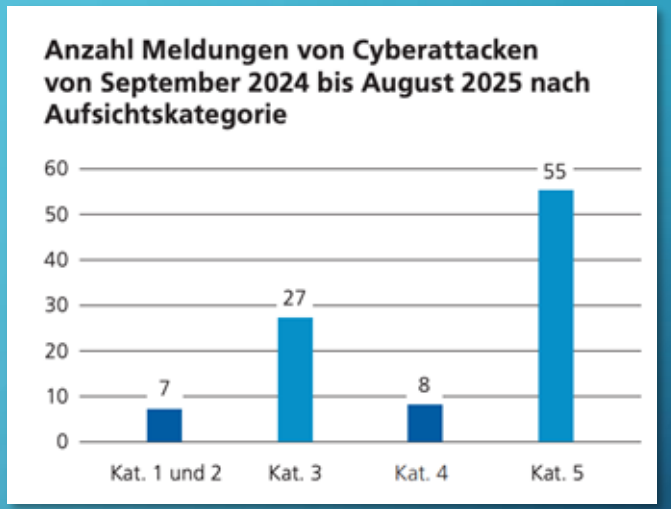
«Kryptoverwahrung ist viel & komplexe Arbeit – für alle Beteiligten»



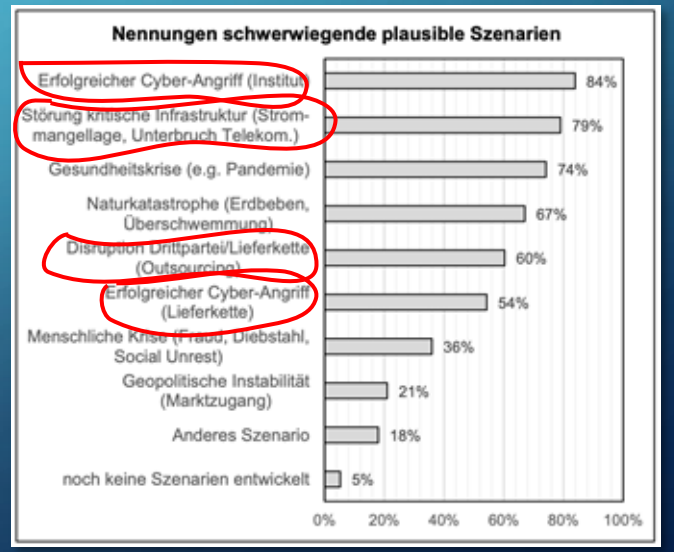
https://www.pinterest.com/mindim2/compliance-humor/

2.1 PRIVATE KEYS & CYBER-RISIKEN

- FINMA: «**Cyberrisiken** gehören zu den bedeutendsten operationellen Risiken von Finanzinstituten.»
- Besonders bedeutsam sind sie bei **Auslagerungen**, insb. aufgrund der hohen Anbieterkonzentration, operationellen Abhängigkeiten und Lieferkettenrisiken



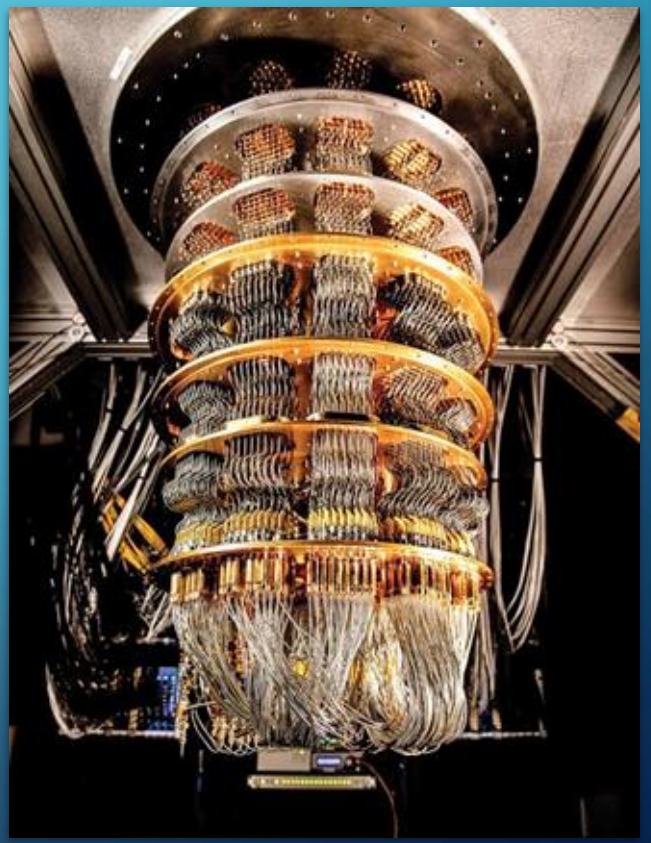
Quelle: FINMA-Risikomonitor 2025



Quelle: FINMA-AM 05/2025

2.1 PRIVATE KEYS & CYBER-RISIKEN

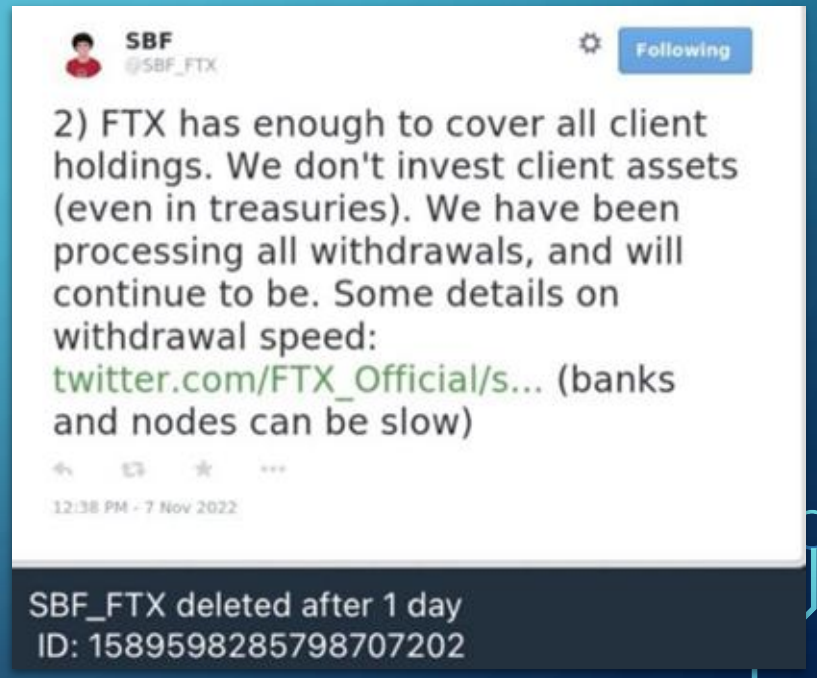
1. **Haftung bei Hacks**
   - Haftung für sorgfältige Verwahrung (Art. 398 OR; s. auch MiCAR)
   - Meldung von Cyber-Angriffen an FINMA (FINMA-AM 05/2020, AM 03/2024)
   - Konkursschutz erfasst jedoch nur noch vorhandene Werte(!)
2. **Fehlerhafte bzw. schwache Schlüsselerzeugung**
   - IKT-Risikomanagement inkl. Lieferanten (FINMA-RS 2023/1)
   - Kompromittierte Schlüssel: Migration und Abbildung im DARP
3. **Quantum Computing**
   - FINMA verlangt «Kryptoagilität» (FINMA-AM 05/2026)
   - Umstellung hängt von Blockchain ab; Risiken den Kunden offenlegen
   - Konsequentes Blockchain-Adressen-Management



https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors

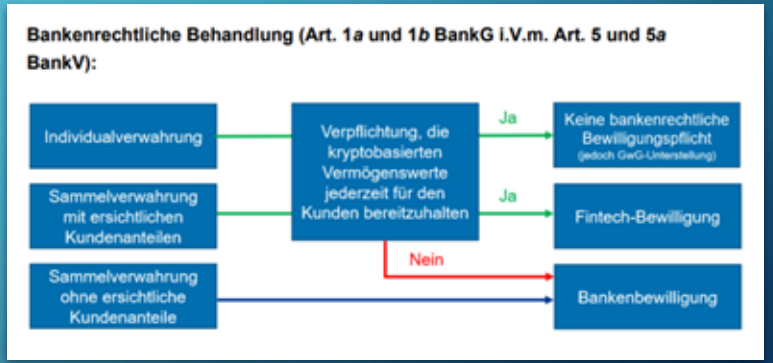
2.2 SEGREGIERUNG & KONKURSSCHUTZ

- **Segregierung** bzw. **Trennung** von Vermögenswerten ist ein operationelles Grundkonzept in der Fremdverwahrung (bisher Bucheffekten, nun auch Kryptowerte)
- Effektiver **Konkursschutz** hängt allerdings nicht alleine von der Frage der Segregierung ab



2.2 SEGREGIERUNG & KONKURSSCHUTZ

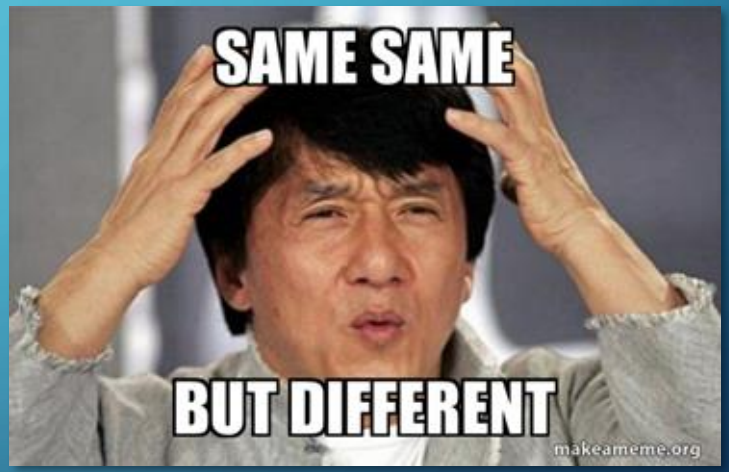
1. **FTX-Skandal von 2022 als Auslöser für internationale Regeln**
   - Aussonderung seit DLT-Vorlage 2021 (Art. 16/37d BankG, Art. 242a SchKG)
   - Keine Vermischung mit Eigenbeständen
   - Geplant: Segregierungspflicht für Krypto-Institute (Art. 51y VE-FINIG)
2. **Form der Verwahrung bestimmt die Regulierung**
   - Einzelverwahrung: grundsätzlich nur GwG, FINMA: eine Adresse pro Kunde
   - Sammelverwahrung mit Kundenanteilen: Bank- oder Fintech-Bewilligung
   - Ohne ersichtliche Anteile: Publikumseinlagen (Art. 1a BankG)
3. **Segregierung hat in der Blockchainwelt mehrere Ebenen**
   - Traditionell: Buchungen in der Kernbankensoftware bestimmt über die Segregierung
   - Blockchains und Smart Contracts sind weitere eigenständige (externe) Register (*Reconciliation*-Bedarf)



FINMA-AM 01/2026, Ziff. 3.1

2.3 UNTERVERWAHRUNG & AUSLAGERUNG

- Kryptoverwahrung beruht auf ganz **unterschiedlichen** Technologien in der Praxis, z.B. HSM, MPC oder hybride Systeme
- Die **Abgrenzung** der reinen IT-Auslagerung zur echten Unterverwahrung von Kryptowerten ist praktisch häufig schwierig



https://makeameme.org/meme/same-same-but-16ca377f76

2.3 UNTERVERWAHRUNG & AUSLAGERUNG

1. **Kryptoverwahrung ist in der Praxis oft ein Auslagerungsthema**
   - Auslagerung einer wesentlichen «kritischen» IT-Funktion (FINMA-RS 2018/3, RS 2023/1, s. auch DORA)
   - Finanzinstitut bleibt für Auswahl, Instruktion und Überwachung verantwortlich
   - Auslagerung ins Ausland: nur bei gleichwertiger Aufsicht und Konkursschutz (FINMA-AM 01/2026)

2. **Tech-Provider vs. Verwahrer**
   - Häufig unklar in der Praxis, wann die Grenze zur Unterverwahrung erreicht ist.
   - Massgeblich ist grundsätzlich die tatsächliche Verfügungsgewalt, nicht der SaaS-Vertrag oder das Marketing – welcher Grad relevanter Kontrolle ist jedoch massgeblich?
   - In beiden Fällen empfehlenswert, die Beziehung im Risikomanagement, BCP/DRP und DARP abzubilden.



https://cointelegraph.com/news/esma-crypto-custody-scrutiny-mica-transition

3. DISKUSSION IM PLENUM



Bangladesh Bank, 2016



Binance, 2026

Vielen Dank für Ihre Aufmerksamkeit.

GET IN TOUCH

Dr. iur. Fabio Andreotti

Head of Legal, Obligate AG

fabio@obligate.com

www.obligate.com