BITCOIN SICHER AUFBEWAHREN

Multisig oder Seed + Passphrase?

Zwei Wege zur souveränen Eigenverwahrung – ein neutraler Vergleich

Stand: November 2026

Jedes Setup balanciert zwei Risiken



Verlust

Ich komme nicht mehr an meine Bitcoin

Backup verbrannt, Passphrase vergessen, Deskriptor verlegt, Gerät defekt – oder der Erbfall ist nicht geregelt.



Diebstahl

Jemand anderes kommt an meine Bitcoin

Backup gefunden, Gerät oder Firmware fehlerhaft, Schadsoftware – oder Erpressung unter Zwang.

Jedes Setup verschiebt das Gleichgewicht zwischen beiden Risiken – keines beseitigt sie ganz. Die Frage ist nicht „welches ist sicherer?“, sondern „welches passt zu mir?“

ZWEI SETUPS IM BILD

Was man bei welchem Setup aufbewahrt

Seed + Passphrase

Singlesig – ein Schlüssel, zwei Faktoren

Seed (Stahl)	Seed (Stahl)
Ort A	Ort B
Passphrase	**Passphrase**
Ort C, z. B. Notar	Ort D

Ausgeben: Seed + Passphrase in einem zustandslosen Signer
Prüfen: Fingerprint bestätigt die richtige Passphrase

Multisig 2-von-3

Drei Schlüssel, zwei davon nötig

Schlüssel 1	Schlüssel 2	Schlüssel 3
Ort A	Ort B	Ort C

+ Deskriptor bei jedem Schlüssel
alle xpubs, Schwellwert, Pfade – ohne ihn keine Wiederherstellung

Ausgeben: zwei beliebige Schlüssel + Deskriptor
Geräte: drei Signer, möglichst verschiedene Hersteller

DIE KERNBOTSCHAFT

Sicherheit entsteht durch Regeln – nicht durch die Anzahl der Schlüssel.

Ein sauber umgesetztes Singlesig mit Passphrase ist besser als ein Multisig, das man nicht vollständig versteht – und umgekehrt.

Wenn das Gerät schlechten Zufall liefert

Im Juli 2026 wurde bekannt: Die Seed-Erzeugung eines verbreiteten Hardware-Wallet-Herstellers nutzte seit einer Code-Umstellung 2021 nicht mehr den Hardware-Zufallsgenerator. Angreifer konnten schwache Seeds durchprobieren.

5 Jahre

blieb der Fehler unbemerkt (2021–2026)

40–72 Bit

Entropie statt der vorgesehenen 128 Bit

≈ 1.790 BTC

in vier Wellen gestohlen, davon 1.083 BTC in den ersten 41 Minuten (Galaxy Research)

Was geholfen hat

Starke Passphrase

lang, zufällig, nie an Smartphone oder PC eingegeben

Multisig mit Mischung

nur wenn die Schlüssel von verschiedenen Herstellern stammten

Selbst gewürfelter Seed

ca. 50 faire Würfe ≈ 128 Bit, ca. 99 Würfe ≈ 256 Bit

Die unterschätzte Bedrohung kommt an die Haustür

72

verifizierte Überfälle auf Bitcoin-Halter weltweit 2025 – ein Plus von 75 %

52

Fälle allein im ersten Halbjahr 2026 – Europa ist Schwerpunkt

37 %

der dokumentierten Fälle sind Überfälle in der eigenen Wohnung

Unsere Regel: Nichts zu Hause

Kein Seed, keine Passphrase, kein entsperrbares Gerät im Haus – und die Passphrase nicht auswendig kennen. Dann muss ein Täter mehrere Orte erreichen, egal ob Seed + Passphrase oder Multisig. Wer nichts herausgeben kann, ist kein lohnendes Ziel.

WEG 1

Seed + Passphrase

Ein Schlüssel, zwei Faktoren



- Ein Seed in Stahl, zweimal an getrennten Orten
- Eine Passphrase, ebenfalls zweimal getrennt verwahrt
- Ein zustandsloser Signer zum Ausgeben

Stärken

Einfach

Ein Standard (BIP-39), ein Signer – in etwa einer Stunde eingerichtet.

Robust beim Fund

Ein gefundener Seed ist ohne Passphrase wertlos – und umgekehrt.

Schutz bei Gerätefehlern

Eine lange, zufällige Passphrase schützte 2026 auch schwach erzeugte Seeds.

Erbfreundlich

Wenige Schritte, Kontrolle per Fingerprint, Übergabe z. B. über einen Notar.

Familientauglich

Ein Seed, eine eigene Passphrase je Person – transparent über xpubs.

Günstig und privat

Keine laufenden Kosten, keine Dritten, unauffällige Transaktionen.

Grenzen – und wie man sie auffängt

Grenze	So fangen wir sie auf
Passphrase vergessen oder verloren = Totalverlust	**Passphrase zweimal getrennt sichern, z. B. beim Notar**
Ein Tippfehler öffnet unbemerkt eine leere Wallet	**Fingerprint notieren und bei jeder Eingabe prüfen**
Seed und Passphrase treffen sich auf einem Gerät	**Zustandsloser Open-Source-Signer, Seed selbst würfeln**
Bei bekanntem Seed lässt sich eine schwache Passphrase erraten	**Passphrase lang und zufällig erzeugen**
Erpressung, wenn alles griffbereit ist	**Nichts zu Hause, Passphrase nicht auswendig kennen**
Kein Vier-Augen-Prinzip möglich	**Für gemeinsame Verfügung Multisig wählen**

WEG 2

Multisig 2-von-3

Drei Schlüssel, zwei davon nötig



- Drei Seeds auf drei Signern, möglichst verschiedene Hersteller
- Drei getrennte Orte, gegebenenfalls drei Personen
- Ein Deskriptor bei jedem Schlüssel-Backup

Stärken

Kein Schlüssel reicht allein

Fund oder Diebstahl eines einzelnen Schlüssels bleibt folgenlos.

Verlust verkraftbar

Ein Schlüssel darf ausfallen – die anderen zwei genügen.

Herstellerrisiko gestreut

Geräte verschiedener Hersteller fangen Firmware-Fehler ab.

Vier-Augen-Prinzip

Gemeinsame Verfügung – ideal für Firmen, Vereine, Gremien.

Schutz vor Zwang

Signieren ist nur an mehreren Orten möglich.

Personalwechsel

Ein Schlüsselhalter kann ausscheiden, ohne dass das Vermögen blockiert.

Grenzen – und wie man sie auffängt

Grenze	So fangen wir sie auf
Ohne Deskriptor keine Wiederherstellung – trotz zweier Seeds	**Deskriptor zu jedem Schlüssel-Backup legen**
Drei Geräte, drei Firmwares, Koordinator-Software	**Regelmäßig prüfen, Wiederherstellung üben**
Höherer Einrichtungs- und Lernaufwand	**Erst Singlesig beherrschen, dann erweitern**
Erben brauchen deutlich mehr Wissen	**Ausführliche Anleitung, Vertrauensperson benennen**
Alle Schlüssel am selben Ort = kaum Schutz	**Getrennte Orte, gegebenenfalls getrennte Personen**
Deskriptor verrät alle Guthaben, höhere Gebühren	**Deskriptor diskret verwahren, selten bewegen**

DIREKTER VERGLEICH

Beide Setups nach unseren Regeln umgesetzt

Kriterium	Seed + Passphrase	Multisig 2-von-3
Einrichtung	✓ einfach, ca. 1 Stunde	● aufwendig, bis ca. 2 Tage
Ein Backup geht verloren	✓ je eine Reservekopie	✓ ein Schlüssel darf fehlen
Ein Backup wird gefunden	✓ ohne Passphrase wertlos	✓ ohne zweiten Schlüssel wertlos
Fehler eines Herstellers	● klein mit SeedSigner + Würfeln	✓ gestreut bei Herstellermix
Überfall zu Hause	✓ wenn nichts zu Hause liegt	✓ wenn Schlüssel verteilt sind
Gemeinsame Verfügung	✗ nicht möglich	✓ Kernstärke
Erbfall	✓ wenige Schritte	● Software + Deskriptor nötig
Wiederherstellung testen	✓ einfach	● aufwendiger
Kompatibilität	✓ BIP-39, fast jede Wallet	● Multisig-fähige Software
Gebühren und Privatsphäre	✓ unauffällig, günstig	● größere Transaktionen

✓ Vorteil ● eingeschränkt ✗ Nachteil

Die entscheidende Frage: Wer soll verfügen dürfen?



Eine Person

Seed + Passphrase

- Sparer und Einsteiger
- Ältere Menschen
- Wer oft umzieht oder reist
- Student im Wohnheim – Backups bei Eltern oder Notar statt im Zimmer



Mehrere – jeder für seinen Teil

Ein Seed, eigene Passphrasen

- Ehepaare und Partner
- Erwachsene Kinder
- Erben und Familie
- Ausfall regeln per Notar oder Passwortmanager mit Nachlassfunktion

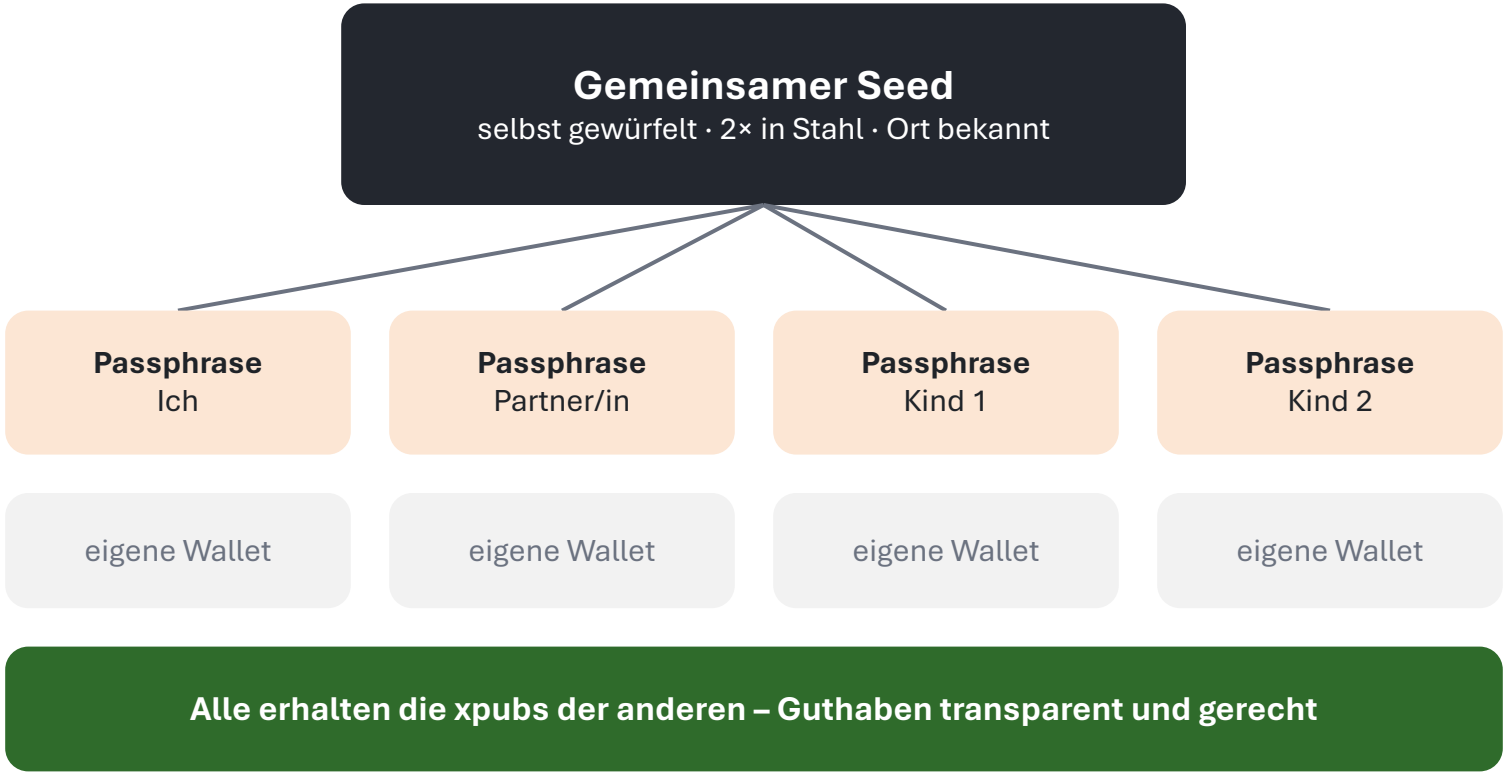


Mehrere – nur gemeinsam

Multisig

- Unternehmen mit mehreren Geschäftsführern
- Vereine, Stiftungen, Gremien
- Gemeinschaftskassen und Treuhand
- Wer das Herstellerrisiko bewusst streuen will

Ein Seed – eine eigene Passphrase je Person



Große Beträge lassen sich zusätzlich auf mehrere Passphrasen an verschiedenen Orten verteilen.

Übergabe im Erbfall

- Versiegelter Umschlag über den Notar oder Passwortmanager mit Nachlassfunktion
- Fingerprint je Wallet zur Kontrolle
- Eigene Erfahrung oder eine Vertrauensperson

Voraussetzungen

- Passphrasen lang und zufällig
- Aufteilung mit Testament abstimmen
- Seed-Orte so sicher wie bei jedem Setup

Was die Wege ungefähr kosten

Seed + Passphrase

selbst eingerichtet

ca. 100–300 €

einmalig: Signer (z. B. SeedSigner), zwei Stahlplatten, Würfel

Multisig

selbst eingerichtet

ca. 300–700 €

einmalig: drei Signer, drei Stahlplatten – Software kostenlos

Begleitung und Dienste

Multisig mit Unterstützung

ab ca. 250 € / Jahr

von pauschalen Jahresgebühren bis zu prozentualen Gebühren auf das Vermögen

Begleitung kann sinnvoll sein. Entscheidend ist, dass man das eigene Setup danach selbst versteht und unabhängig wiederherstellen kann. Richtwerte, ohne Notarkosten.

UNSERE EMPFEHLUNG

Sieben Regeln für Seed + Passphrase

1 

Seed selbst würfeln

z. B. mit dem SeedSigner

2 

Zustandsloser Signer

keine entsperrbaren Geräte zu Hause

3 

2 + 2 Backups

Seed 2× in Stahl, Passphrase 2× getrennt

4 

Nichts zu Hause

Passphrase nicht auswendig kennen

5 

Fingerprint notieren

lange, zufällige Passphrase prüfbar machen

6 

Familie: eigene Passphrasen

ein Seed, xpubs für Transparenz

7 

Erbfall regeln

Übergabe über Notar oder Nachlassfunktion

Multisig, wenn mehrere gemeinsam verfügen sollen – oder bei sehr großen Beträgen zur Herstellerstreuung.

ENTSCHEIDUNGSHILFE

In drei Fragen zum passenden Setup

1	Sollen mehrere Personen nur gemeinsam verfügen können?	Ja →	Multisig
2	Sollen mehrere Personen je über ihren eigenen Teil verfügen?	Ja →	Ein Seed, eigene Passphrasen
3	Sehr großer Betrag und drei Geräte plus Deskriptor sicher im Griff?	Ja →	Multisig möglich – oder Betrag auf mehrere Passphrasen verteilen

In allen anderen Fällen: Seed + Passphrase nach unseren sieben Regeln.

Faustregel: Die beste Lösung ist die, die man selbst sicher beherrscht – und mit der auch die Erben zurechtkommen.

Quellen

- Coinkite / Coldcard: Sicherheitshinweis zur Seed-Erzeugung, 30.07.2026 – Zusammenfassungen u. a. bei Casa Blog, Forklog, WuBlockchain, Coin360
- Galaxy Research: Analyse der Abflüsse ab 30.07.2026 – 1.789,28 BTC von 8.865 Adressen in vier Wellen
- CertiK: Skynet Wrench Attacks Report (Februar 2026) und 2026 Wrench Attacks Overview
- Chainalysis: Bericht zu physischen Angriffen auf Krypto-Halter, 1. Halbjahr 2026
- Coldcard Learn: „Bitcoin Multisig“ – Deskriptor-Backup, Vergleich mit Singlesig + Passphrase
- Delving Bitcoin: Diskussion zu Deskriptor-Backups bei Multisig (2025)
- BitBox Blog: „The pitfalls of multisig when using hardware wallets“
- Eigene Workshop-Unterlagen: „Level der Bitcoin-Verwahrung“ und Handout „Singlesig oder Multisig?“

HINWEIS ZUR WEITERGABE

Zum Weitergeben gedacht

- **Ehrenamtlich erstellt**

  ohne kommerzielles Interesse und ohne Bezug zu Anbietern oder Dienstleistern

- **Keine Beratung**

  keine Anlage-, Rechts- oder Steuerberatung – Erbfragen mit Notar oder Anwalt klären

- **Ohne Gewähr**

  Stand November 2026; Technik und Angebote ändern sich laufend

- **Weitergabe erwünscht**

  gern unverändert, mit Quelle: bitcoin-entdecken.de