BITCOIN WETTERAU · BIBLIOTHEK

Bitcoin im Nachlass

Wie Deine Bitcoin geschützt bleiben und trotzdem bei Deinen Erben ankommen – die Ergänzung zum Guide „Mein digitaler Nachlass“

UNTERTHEMA
Digitale Vorsorge & Nachlass · Bitcoin

STAND
Oktober 2026 · Version 1.1

VERFASST VON
Frank M. inspiriert von Sven U.

LESEZEIT
ca. 25 Minuten · Einstieg
je nach Ausgangslage

HERZLICH WILLKOMMEN

Dein Guide auf einen Blick

Acht Abschnitte und ein Glossar – rund 25 Minuten Lesezeit. Am Ende steht ein Übergabekonzept, das Deine Bitcoin vor Dritten schützt und trotzdem sicher bei Deinen Erben ankommen lässt.

WO STEHST DU?

Dein Einstieg

Börse, eigene Hardware Wallet oder schon Passphrase – drei Ausgangslagen, drei nächste Schritte.

Seite 4

DER SONDERFALL

Kein Ansprechp., kein Zurücksetzen

Warum Erbschein und Gericht hier nicht helfen – und die wichtigsten Begriffe in einfachen Worten.

Seite 5

DAS GRUNDDILEMMA

Zugänglich für Erben, sicher vor Dritten

Fünf Risiken und die Vorsorge-Stufe, die zu Deinem Umfang passt.

Seite 6

BITCOIN AUF DER BÖRSE

Wenn eine Plattform verwahrt

Welche Nachweise Deine Erben brauchen – und warum Fremdverwahrung ein eigenes Risiko ist.

Seite 7

DER EMPFOHLENE WEG

Ein Schlüssel, mehrere Schlösser

Seedphrase in Metall, Passphrasen je Erbe und Köder-Wallet – Schritt für Schritt.

Seite 8

WEITERE MÖGLICHKEITEN

Andere Wege – kurz eingeordnet

Shamir, Multisig, Zeitschloss und gemeinsame Verwahrung im Überblick.

Seite 11

ERBEN HANDLUNGSFÄHIG MACHEN

Keine Experten nötig

Brief an die Erben, technische Vertrauensperson und die ersten Wochen nach dem Ernstfall.

Seite 12

RECHT, STEUERN UND PFLEGE

Was Du rechtlich beachten solltest

Testamentsbaustein, Erbschaft- und Einkommensteuer, Jahrescheck und Glossar.

Seite 14

EINFÜHRUNG

Keine zweite Chance

Warum Bitcoin eine eigene Vorsorge braucht – und wie dieser Guide mit „Mein digitaler Nachlass“ zusammenspielt.

Bitcoin ist der Sonderfall des digitalen Nachlasses. Bei Konten und Verträgen gibt es eine Bank oder einen Anbieter, der Erben nach Vorlage eines Erbnachweises Zugang verschafft. Bei selbst verwahrten Bitcoin gibt es niemanden: Ohne vorbereitete Übergabe sind sie im Ernstfall dauerhaft verloren.

Dieser Guide ergänzt den Guide „Mein digitaler Nachlass“ – im Folgenden kurz Hauptguide. Dort geht es um Geräte, Konten und Zugänge, um Vorsorgevollmacht und Testament und um den Praxistest mit Deiner Vertrauensperson. Hier geht es ausschließlich um Bitcoin: wie Du sie so verwahrst, dass sie vor Dritten sicher sind und trotzdem bei Deinen Erben ankommen.

Du kannst diesen Guide für sich allein lesen. Wo er auf die Bestandsaufnahme, den Notfallordner, die Vollmacht oder die Rollen Deiner Vertrauenspersonen verweist, findest Du die Details im Hauptguide. Am besten arbeitest Du beide durch – der Notfallordner und der Brief an Deine Erben verbinden sie.

> **WICHTIG · VERWAHRUNG, KEINE ANLAGEBERATUNG**
> Dieser Guide behandelt ausschließlich Verwahrung, Zugriff und Übergabe von Bitcoin. Es beantwortet nicht die Frage, ob oder wie viel Du investieren solltest. Rechtliche Hinweise und Muster ersetzen keine Beratung durch Notar, Fachanwalt oder Steuerberatung.

> **HINWEIS · ANDERE KRYPTOWERTE**
> Dieser Guide konzentriert sich auf Bitcoin. Das beschriebene Verfahren funktioniert grundsätzlich auch bei anderen Kryptowerten, deren Wallets mit einer Seedphrase nach dem verbreiteten Standard arbeiten. Prüfe dort aber genau, ob Passphrasen unterstützt werden und welche Software Deine Erben zur Wiederherstellung brauchen. Guthaben auf Plattformen und in Sonderformaten erfordern oft eigene Wege.

HINWEIS · LIGHTNING

Guthaben in Lightning-Kanälen lassen sich nicht allein mit der Seedphrase wiederherstellen. Die Seedphrase eines Lightning-Nodes sichert nur dessen On-Chain-Guthaben; für die Kanäle braucht es zusätzlich die aktuelle Kanal-Sicherung (Static Channel Backup) – und selbst damit werden die Kanäle nur geschlossen, nicht weitergeführt. Wer einen eigenen Node betreibt, hält im Notfallhandbuch (Hauptguide, Kapitel 03) fest, wo Node und Kanal-Sicherung liegen und wie die Kanäle geordnet geschlossen werden. Bei Lightning-Wallets auf dem Smartphone hängt es von der App ab, ob das Guthaben beim Anbieter liegt oder an einer eigenen Sicherung hängt. Für Lightning gilt deshalb: nur Beträge für den täglichen Gebrauch, keine Ersparnisse.

WO STEHST DU?

Dein Einstieg in diesen Guide

Nicht jeder muss alles lesen. Suche Dir die Zeile, die Deine Situation am besten beschreibt. Wenn Du unsicher bist, beginne bei A.

DEINE SITUATION	WAS DAS BEDEUTET	LIES VOR ALLEM	DEIN NÄCHSTER SCHRITT
A · Ich habe Bitcoin nur auf einer Börse oder in einer Trading-App	Die Börse verwahrt Deine Bitcoin. Deine Erben brauchen einen Erbnachweis – und müssen überhaupt davon wissen.	Sonderfall, Börse, Erben, Recht	Börse und Kundennummer in Deine Bestands-aufnahme eintragen (Hauptguide, Kapitel 01)
B · Ich habe eine eigene Hardware Wallet	Du verwahrst selbst. Ohne vorbereitete Übergabe sind Deine Bitcoin im Ernstfall verloren.	Den ganzen Guide, vor allem den empfohlenen Weg	Seedphrase sichern, Übergabe planen
C · Ich nutze bereits Passphrase oder Multisig	Die Technik steht. Offen ist meist, ob Deine Erben sie auch bedienen können.	Empfohlener Weg, weitere Möglichkeiten, Erben	Anleitung schreiben, Wiederherstellung testen

WARUM BITCOIN EIN SONDERFALL IST

Kein Ansprechpartner, kein Zurücksetzen

Bei einem Bankkonto gibt es eine Bank, die nach Vorlage von Sterbeurkunde und Erbschein auszahlt. Bei selbst verwahrtem Bitcoin gibt es niemanden. Wer den Schlüssel hat, verfügt über die Bitcoin. Wer ihn nicht hat, kommt nicht heran – auch nicht mit Erbschein und Gerichtsbeschluss.

1. **Keine zentrale Stelle.** Es gibt kein Unternehmen, bei dem Erben einen Antrag stellen könnten.
2. **Kein Zurücksetzen.** Ein verlorener Schlüssel lässt sich nicht wiederherstellen. Die Bitcoin bleiben für immer unerreichbar.
3. **Keine Spur auf Papier.** Es gibt keine Kontoauszüge. Erben erfahren oft gar nicht, dass Bitcoin existieren.
4. **Leicht zu stehlen.** Wer die Zugangsdaten findet, kann die Bitcoin in Minuten unwiderruflich übertragen.

Die Begriffe in einfachen Worten

- **Wallet:** die Software oder das Gerät, mit dem Du Deine Schlüssel verwaltest und Bitcoin sendest oder empfängst. Ein Wallet enthält nicht die Bitcoin selbst, sondern die Schlüssel, die über sie verfügen.
- **Seedphrase:** eine Folge von 12 oder 24 Wörtern, aus der sich alle Schlüssel Deines Wallets ableiten. Wer sie besitzt, besitzt die Bitcoin – es gibt keine Bank, die ein vergessenes Passwort zurücksetzt.
- **Passphrase:** ein zusätzliches, frei gewähltes Kennwort, oft „13. Wort“ (bei 12 Wörtern) oder „25. Wort“ (bei 24 Wörtern) genannt. Zusammen mit der Seedphrase öffnet sie ein völlig anderes Wallet. Jede Passphrase ergibt ein eigenes Wallet – mit derselben Seedphrase.
- **Hardware Wallet:** ein kleines Gerät, das die Schlüssel offline verwahrt und Zahlungen nur nach Bestätigung am Gerät freigibt.
- **XPUB:** der öffentliche Schlüssel eines Wallets. Er erlaubt, Guthaben und Bewegungen anzusehen, aber nicht, Bitcoin auszugeben.
- **Master-Fingerprint:** eine kurze Kennung aus acht Zeichen, die jedes Wallet eindeutig kennzeichnet. Stimmt sie bei der Wiederherstellung mit der notierten überein, war die Eingabe richtig.

Erst die Übersicht

Bevor Du über Verwahrung und Übergabe entscheidest, brauchst Du einen Überblick: Wo liegen Bitcoin, in welcher Form, und wer weiß davon? Die folgende Tabelle hält nur fest, **was** es gibt und **wo** die Zugangsteile liegen – niemals die Zugangsdaten selbst.

POSITION	ART	ZUGANGSTEILE LIEGEN (NUR ORT)	WER WEIß DAVON	LETZTE PRÜFUNG
Börsenkonto	Fremdverwahrung	Passwort-Manager, Notfallordner	Vertrauensperson	[Datum]
Wallet Erbe A	Hardware Wallet mit Passphrase	Ort A, versiegelter Umschlag beim Notar	Existenz bekannt (Brief), Inhalt niemand	[Datum]
Köder-Wallet	Hardware Wallet ohne Passphrase	Ort A	Nur Du	[Datum]

DAS GRUNDDILEMMA

Zugänglich für Erben, sicher vor Dritten

Je leichter Deine Erben an Deine Bitcoin herankommen, desto leichter gelingt das auch Dieben. Je besser Du sie schützt, desto größer ist die Gefahr, dass später niemand mehr herankommt. Gute Vorsorge findet die Balance – und die hängt von der davon ab, wie groß das Vermögen ist.

RISIKO	WAS PASSIEREN KANN	WAS SCHÜTZT
Verlust	Seedphrase oder Passphrase sind weg – die Bitcoin sind unerreichbar	Metallbackup, getestete Wiederherstellung, Anleitung
Diebstahl	Jemand findet die Seedphrase und leert das Wallet	Passphrase, Versiegelung, getrennte Aufbewahrung
Erpressung	Jemand zwingt Dich mit Gewalt zur Herausgabe	Köder-Wallet, Diskretion
Betrug an Erben	Falsche Helfer oder „Recovery-Dienste“ erschleichen die Zugangsdaten	Klare Anleitung, Warnhinweise, technische Vertrauensperson
Streit unter Erben	Unklare Aufteilung, Misstrauen	Testament, Transparenz über die XPUBs

Die passende Stufe

UMFANG	EMPFOHLENE VORSORGE
Kleine Beträge in einer Wallet-App auf dem Smartphone (Eigenverwahrung)	Seedphrase sichern, Anleitung für die Erben, Hinweis in der Übersicht
Ernsthaftes Sparen mit Hardware Wallet	Seedphrase in Metall, versiegelter Hinweis auf den Aufbewahrungsort, Anleitung für die Erben
Größere Beträge	Seedphrase und Passphrasen nach dem empfohlenen Weg dieses Guides
Sehr große Vermögen, Unternehmen	Multisig oder andere fortgeschrittene Verfahren, begleitet durch erfahrene Fachleute

BITCOIN AUF DER BÖRSE

Wenn eine Plattform verwahrt

Liegen Bitcoin bei einer Börse oder in einer Trading-App, verwahrt ein Unternehmen sie für Dich. Im Erbfall verhält es sich ähnlich wie eine Bank: Deine Erben müssen sich legitimieren und einen Antrag stellen.

- **Nachweise:** In der Regel verlangt die Börse Sterbeurkunde, Erbschein oder notarielles Testament samt Eröffnungsprotokoll sowie den Ausweis der Erben.
- **Dauer:** Die Bearbeitung dauert oft Wochen bis Monate. Bei Anbietern im Ausland kommen Übersetzungen und weitere Nachweise hinzu.
- **Auszahlung:** Meist in Euro auf ein Konto oder als Bitcoin auf ein Wallet der Erben.
- **Voraussetzung:** Deine Erben müssen wissen, bei welcher Börse Du ein Konto hast. Trage Börse, Kundennummer und registrierte Mailadresse in Deine Bestandsaufnahme (Hauptguide, Kapitel 01) und in die Übersicht dieses Guides ein; die Zugangsdaten gehören in den Passwort-Manager oder die Papierliste (Hauptguide, Kapitel 03).

> **HINWEIS · FREMDVERWAHRUNG IST EIN ZUSÄTZLICHES RISIKO**
> Gerät eine Börse in Schwierigkeiten oder stoppt den Handel, kann der Zugriff auf die Bitcoin verloren gehen – für Dich wie für Deine Erben. Wer größere Beträge hält, verwahrt sie deshalb meist selbst. Wie das mit Blick auf den Nachlass gelingt, beschreibt der folgende Abschnitt.

DER EMPFOHLENE WEG: SEEDPHRASE UND PASSPHRASE

Ein Schlüssel, mehrere Schlösser

Für die meisten Privatpersonen hat sich ein Verfahren bewährt, das ohne komplizierte Technik auskommt: eine Seedphrase, sicher in Metall verwahrt, kombiniert mit einer oder mehreren Passphrasen. Es trennt das, was man finden kann, von dem, was man wissen muss – und lässt sich sauber an mehrere Erben übergeben.

So funktioniert das Prinzip

Aus einer einzigen Seedphrase entstehen durch unterschiedliche Passphrasen mehrere voneinander unabhängige Wallets. Wer nur die Seedphrase findet, sieht ausschließlich das Wallet ohne Passphrase.

KOMBINATION	ERGEBNIS	ZWECK
Seedphrase ohne Passphrase	Köder-Wallet	Glaubwürdiger Betrag für den Fall einer Erpressung
Seedphrase + Passphrase 1	Wallet für Erbe A	Der Anteil, der Erbe A zugedacht ist
Seedphrase + Passphrase 2	Wallet für Erbe B	Der Anteil, der Erbe B zugedacht ist
Seedphrase + Passphrase 3	Wallet für einen Zweck	Zum Beispiel Rücklage, Unternehmen oder Bitcoin aus einer bestimmten Herkunft

FÜR FORTGESCHRITTENE · TECHNISCHER HINTERGRUND

Die optionale Passphrase nach dem verbreiteten Seed-Standard ist technisch kein weiteres Wort der Seedphrase, sondern fließt in die Berechnung des Master-Schlüssels ein. Jede Passphrase erzeugt deshalb einen eigenen Master-Fingerprint, einen eigenen XPUB und eigene Adressen. Eine falsche Passphrase erzeugt keine Fehlermeldung, sondern schlicht ein anderes, leeres Wallet. Groß- und Kleinschreibung sowie Leerzeichen zählen; auf Umlaute, ß und ungewöhnliche Sonderzeichen solltest Du verzichten, weil sie je nach Gerät unterschiedlich verarbeitet werden können. Notiere für jedes Wallet Master-Fingerprint, Adresstyp und Ableitungspfad – idealerweise als Wallet-Deskriptor –, damit die Wiederherstellung auch mit anderer Software gelingt.

Schritt für Schritt

I **Seedphrase selbst erzeugen.** Die größte Kontrolle hast Du, wenn Du den Zufall selbst erzeugst – etwa mit Casino-Würfeln – und daraus die Seedphrase bildest. Bei Hardware Wallets einzelner Hersteller wurden Fälle bekannt, in denen der erzeugte Zufall fehlerhaft und zu gering war. Wörter einfach selbst aus der Wortliste auszusuchen, genügt dagegen nicht: Menschen erzeugen keinen echten Zufall. Wer sich das nicht zutraut, lässt die Seedphrase vom Hardware Wallet erzeugen – das ist der übliche Weg; die Würfelmethode (Kasten) ist die Variante mit maximaler Kontrolle.

2 **12 oder 24 Wörter.** Beides ist sicher. 12 Wörter liefern bereits das Sicherheitsniveau, das Bitcoin selbst bietet, und halbieren den Aufwand und die Fehlergefahr beim Übertragen. Für dieses Verfahren empfehlen wir deshalb 12 Wörter.

3 **In Metall sichern und versiegeln.** Übertrage die Wörter mit Schlagbuchstaben oder Stanzwerkzeug auf eine Platte aus Edelstahl oder Titan – nummeriert und gut lesbar – und versiegle sie, damit ein unbefugter Zugriff auffällt. Teile die Wörter nicht auf mehrere Orte auf und verändere sie nicht durch eigene „Verschlüsselungen".

4 **Passphrasen festlegen.** Lege für jeden Erben und jeden Zweck eine eigene Passphrase fest. Sie muss lang, nicht erratbar und eindeutig schreibbar sein (siehe Kasten „Die Passphrase wählen").

5 **Wallets anlegen und dokumentieren.** Öffne jedes Wallet einmal mit seiner Passphrase am Hardware Wallet und notiere Master-Fingerprint und XPUB.

6 **Köder-Wallet einrichten.** Das Wallet ohne Passphrase erhält einen glaubwürdigen Betrag und wird gelegentlich genutzt, damit es echt wirkt.

7 **Aufbewahrung trennen.** Metallplatte an Ort A. Jede Passphrase in einem eigenen versiegelten Umschlag, der Hinweis auf Ort A in einem weiteren – jeweils an einem bekannten Ort oder beim Notar. Hinterlege den Hinweis auf Ort A und die Passphrasen dabei nicht an derselben Stelle: Wer beides in der Hand hat, braucht nur noch die Metallplatte. Die XPUBs aller Wallets ebenfalls versiegelt. Der Brief an die Erben (mit Anleitung) – ohne Geheimnisse – im Notfallordner, dem Ordner mit allen Vorsorgeunterlagen (Hauptguide, Kapitel 05).

8 **Wiederherstellung testen.** Stelle jedes Wallet einmal auf einem zweiten Gerät – oder auf demselben Gerät nach dem Zurücksetzen – aus Metallplatte und Passphrase wieder her und vergleiche den Master-Fingerprint. Erst dann ist das System belastbar.

FÜR FORTGESCHRITTENE · DIE WÜRFELMETHODE

Für 12 Wörter werden 128 Bit Zufall benötigt. Mit Münzwürfen wären dafür 128 Würfe nötig, mit einem sechsseitigen Würfel genügen rund 50 Würfe, weil jeder Wurf mehr Zufall liefert. Einige Hardware Wallets erlauben, Würfelergebnisse direkt als Zufallsquelle einzugeben. Alternativ wird der Zufall offline in die Wortfolge umgerechnet. Das letzte Wort enthält eine Prüfsumme und wird deshalb berechnet. Nutze für Casino-Würfel eine glatte Unterlage und würfle jedes Ergebnis einzeln.

HINWEIS · DIE PASSPHRASE WÄHLEN

Bewährt haben sich zwei Wege. **Zufallswörter:** mindestens sechs zufällig gewählte Wörter – schwer zu erraten, leicht zu notieren. **Ein persönlicher Satz:** ein eigener Glaubenssatz oder eine Nachricht an den jeweiligen Erben, etwa ein Wunsch für seine Zukunft – lang genug und ergänzt um Zahlen und Satzzeichen. Er ist leicht zu merken, und der Erbe liest ihn im Ernstfall als persönliche Botschaft. Wichtig: kein bekanntes Zitat, nichts, was Du öffentlich gesagt oder geschrieben hast, und nur Zeichen, die auf jeder Tastatur gleich sind – keine Umlaute, kein ß.

HINWEIS · DIE GOLDENE REGEL

Die Seedphrase wird nirgendwo eingegeben außer im Hardware Wallet selbst: nicht im Passwort-Manager, nicht im Browser, nicht in einer Notiz-App. Kein Foto, keine Cloud. Wer die Seedphrase hat, hat die Bitcoin.

Wer hat was – und wann?

TEIL	AUFBEWAHRUNG	WER WEIß DAVON	ZUGÄNGLICH
Seedphrase (Metallplatte)	Ort A: Tresor, Versteck oder vergraben	Du; bei vertrauter Beziehung auch die Erben	Nach dem Todesfall
Hinweis auf Ort A	Versiegelt an bekanntem Ort oder beim Notar	Existenz bekannt, Inhalt nicht	Nach dem Todesfall
Passphrase je Erbe	Je ein versiegelter Umschlag an bekanntem Ort oder beim Notar	Existenz bekannt, Inhalt nicht	Nach dem Todesfall, beim Notar gegen Nachweis
XPUBs aller Wallets	Versiegelt, eine Kopie je Erbe	Existenz bekannt, Inhalt nicht	Nach dem Todesfall – nur zum Ansehen
Brief an die Erben (mit Anleitung)	Notfallordner	Vertrauensperson	Sofort – enthält keine Geheimnisse
Köder-Wallet	Seedphrase ohne Passphrase	Nur Du	Jederzeit – bewusst

HINWEIS · WIE VIEL DÜRFEN DIE ERBEN ZU LEBZEITEN WISSEN?

Grundsätzlich bleibt der Hinweis auf das Versteck der Metallplatte versiegelt. Ist die Beziehung zu Deinen Erben eng und vertraut, kann es aber sinnvoll sein, ihnen schon zu Lebzeiten zu sagen, wo die Seedphrase liegt. Ohne Passphrase kommen sie damit nur an das Köder-Wallet – im Ernstfall müssen sie dann aber nicht erst suchen.

HINWEIS · BEI HANDLUNGSUNFÄHIGKEIT

Gute Vorsorge unterscheidet zwei Ernstfälle: Tod und Handlungsunfähigkeit. Das Übergabekonzept dieses Guides ist auf den Todesfall ausgelegt: Erst dann werden die Umschläge geöffnet. Bist Du vorübergehend oder dauerhaft nicht handlungsfähig, bleiben Deine Bitcoin in Eigenverwahrung unangetastet liegen – sie laufen nicht weg. Laufende Kosten bestreitet die bevollmächtigte Person aus Konten oder Börsenguthaben, für die Deine Vollmacht gilt (Hauptguide, Kapitel 04).

Ob und unter welchen Bedingungen sie versiegelte Umschläge öffnen darf, regelst Du ausdrücklich in der Vollmacht – im Zweifel: nicht. Wer Umschläge beim Notar hinterlegt, legt in der Verwahrungsanweisung fest, wer sie gegen welchen Nachweis erhält: nach dem Tod gegen Erbnachweis, bei Handlungsunfähigkeit gegen ärztliches Attest und Vollmacht.

HINWEIS · TRANSPARENZ UNTER ERBEN

Nach dem Ernstfall erhält jeder Erbe die XPUBs aller Wallets. So kann jeder sehen, welche Beträge in den anderen Wallets liegen, und nachvollziehen, dass die Aufteilung dem Testament entspricht – ohne auf fremde Wallets zugreifen zu können. Zu Lebzeiten bleiben die XPUBs versiegelt, denn wer sie kennt, kennt Dein Bitcoin-Vermögen und jede künftige Bewegung.

HINWEIS · DAS KÖDER-WALLET

Das Wallet ohne Passphrase ist für den Fall gedacht, dass Dich jemand mit Gewalt zur Herausgabe zwingt. Es muss sich für einen Angreifer lohnen und plausibel wirken: ein Betrag, der zu dem passt, was andere über Dich wissen könnten – als Orientierung oft ein umgerechnet fünfstelliger Eurobetrag –, dazu gelegentliche Bewegungen. Gleichzeitig muss sein Verlust für Dich verkraftbar sein.

Im Ernstfall gilt immer: Deine Sicherheit geht vor. Wer das Verfahren kennt, fragt womöglich nach einer Passphrase. Die beste Vorsorge bleibt deshalb, über Bitcoin-Bestände nicht öffentlich zu sprechen.

WICHTIG · DIE RISIKEN DIESES WEGES

Eine vergessene oder falsch notierte Passphrase bedeutet den Totalverlust dieses Wallets – eine Wiederherstellung gibt es nicht. Werden Metallplatte und Passphrase zusammen gefunden, ist das Wallet ungeschützt. Ein vergrabenes oder verstecktes Backup nützt nur, wenn Deine Erben es finden. Prüfe deshalb regelmäßig, ob alle Teile vorhanden, lesbar und die Siegel unversehrt sind.

FÜR FORTGESCHRITTENE · WARUM 12 WÖRTER REICHEN

12 Wörter entsprechen 128 Bit Zufall. Der beste bekannte Angriff auf die Schlüssel von Bitcoin selbst erfordert ebenfalls rund 2^{128} Rechenschritte – mehr Sicherheit, als Bitcoin selbst bietet, bringen 24 Wörter also nicht. Sie erhöhen aber den Aufwand beim Stanzen und die Gefahr von Übertragungsfehlern. Die zusätzliche Sicherheit liefert die Passphrase.

WEITERE MÖGLICHKEITEN IM ÜBERBLICK

Andere Wege – kurz eingeordnet

Neben dem hier empfohlenen Weg gibt es weitere Verfahren. Sie haben ihre Berechtigung, sind aber für die meisten Privatpersonen entweder zu einfach oder zu komplex. Die Übersicht hilft bei der Einordnung.

VERFAHREN	PRINZIP	GRENZEN	GEEIGNET FÜR
Seedphrase ohne Passphrase	Metallbackup und Anleitung, sonst nichts	Wer das Backup findet, hat alles	Kleinere Beträge

VERFAHREN	PRINZIP	GRENZEN	GEEIGNET FÜR
Shamir-Verfahren	Die Seedphrase wird mathematisch in Teile zerlegt, zum Beispiel „2 von 3“; ein einzelnes Teil verrät nichts – anders als das bloße Aufteilen der Wörter, das Schritt 3 ausschließt	Nicht jedes Gerät unterstützt es; mehrere Teile müssen verwaltet werden	Technisch Versierte
Multisig	Mehrere Schlüssel auf verschiedenen Geräten, zum Beispiel „2 von 3“ müssen unterschreiben	Deutlich komplexer; ohne vollständige Dokumentation keine Wiederherstellung	Sehr große Vermögen, Unternehmen
Wallets mit Zeitschloss (z. B. die quelloffene Software Liana)	Ein Wiederherstellungsschlüssel wird erst nach einer Frist ohne Bewegung gültig	Die Frist muss regelmäßig erneuert werden; Einrichtung anspruchsvoll	Technisch Versierte
Gemeinsame Verwahrung mit Dienstleister	Ein Dienstleister hält einen von mehreren Schlüsseln und unterstützt die Erben	Abhängigkeit, Kosten, Offenlegung Deiner Identität	Wer Begleitung wünscht

GRUNDSATZ · KOMPLEXITÄT IST DER FEIND DER SICHERHEIT

Die meisten verlorenen Bitcoin wurden nicht gestohlen, sondern von ihren Besitzern unerreichbar gemacht – durch zu komplizierte Verfahren, die nach Jahren niemand mehr versteht. Wähle das Verfahren, das Du und Deine Erben dauerhaft beherrschen, nicht das technisch anspruchsvollste.

ERBEN HANDLUNGSFÄHIG MACHEN

Keine Experten nötig – aber eine gute Anleitung

Deine Erben müssen keine Bitcoin-Fachleute werden. Sie brauchen eine klare Anleitung, einen Menschen, den sie fragen können, und die Gewissheit, dass sie sich Zeit lassen dürfen.

Der Brief an die Erben

Der Brief liegt im Notfallordner und enthält **keine** Seedphrase, **keine** Passphrase und **keinen** Hinweis auf das Versteck. Er erklärt, was zu tun ist, und verweist auf die versiegelten Umschläge. Bewährt hat sich diese Gliederung:

1. **Was es gibt:** dass Bitcoin vorhanden sind, in welcher Form (Wallets, Börse) und wie sie laut Testament aufgeteilt sind.
2. **Wo die Umschläge liegen:** welche versiegelten Umschläge es gibt, wo sie liegen und wie man an sie herankommt – nicht das Versteck der Metallplatte selbst.

3 **Wer hilft:** Name und Kontakt der technischen Vertrauensperson.

4 **Wie es geht:** Schritt für Schritt – welches Gerät, welche Art von Software, wie der Master-Fingerprint geprüft wird.

5 **Was nicht zu tun ist:** die Warnhinweise aus dem folgenden Kasten.

6 **Persönliche Worte:** was Dir wichtig ist – vielleicht auch, was die Bitcoin für Dich bedeutet haben.

Die technische Vertrauensperson

Eine technisch versierte Person Deines Vertrauens kann Deinen Erben bei der Wiederherstellung zur Seite stehen. Sie erhält zu Lebzeiten **keinen** Zugang: weder Seedphrase noch Passphrase. Ihre Rolle ist, zu erklären und zu begleiten – die Umschläge öffnen die Erben selbst.

> **WARNUNG · WAS DEINE ERBEN NICHT TUN SOLLTEN**
> Die Seedphrase niemals in einen Computer, ein Smartphone oder eine Website eingeben – nur in ein Hardware Wallet. Niemandem Seedphrase oder Passphrase verraten, auch keinem angeblichen Support, keiner Börse und keinem „Recovery-Dienst". Seriöse Anbieter fragen nie danach. Keine Eile: Die Bitcoin laufen nicht weg. Nicht öffentlich über das Erbe sprechen. Geräte nicht zurücksetzen, verkaufen oder entsorgen, bevor alles geprüft ist.

Die ersten Wochen – für Deine Erben

1 **Ruhe bewahren.** Nichts überstürzen, nichts bewegen, niemandem Zugangsdaten nennen.

2 **Anleitung lesen.** Den Brief im Notfallordner lesen und die technische Vertrauensperson informieren.

3 **Nachweise besorgen.** Sterbeurkunde und Erbnachweis beantragen; die versiegelten Umschläge holen bzw. beim Notar anfordern.

4 **Wiederherstellen.** Gemeinsam mit der Vertrauensperson das eigene Wallet auf einem neuen Hardware Wallet wiederherstellen und den Master-Fingerprint vergleichen.

5 **Abgleichen.** Mit den XPUBs prüfen, ob die Beträge in allen Wallets der Aufteilung im Testament entsprechen.

6 **Neu sichern.** Die Bitcoin auf ein eigenes, neu erzeugtes Wallet übertragen. Die alten Zugangsdaten gelten als bekannt, sobald Umschläge geöffnet wurden.

7 **Steuern klären.** Den Erwerb dem Finanzamt melden und die steuerlichen Folgen mit einer Steuerberatung klären.

RECHTLICH UND STEUERLICH KOMPAKT

Was Du rechtlich beachten solltest

Bitcoin werden vererbt wie jedes andere Vermögen. Die Technik entscheidet, wer herankommt – das Testament entscheidet, wem sie gehören. Beides muss zusammenpassen.

- **Aufteilung im Testament festhalten.** Wenn Du über Passphrasen einzelnen Erben eigene Wallets zuordnest, verteilst Du faktisch Vermögen. Halte diese Zuordnung im Testament fest, etwa als Vermächtnis, und prüfe, ob Pflichtteilsrechte berührt sind.
- **Keine Zugangsdaten ins Testament.** Das Testament wird nach dem Tod eröffnet und allen Beteiligten bekannt gegeben. Es darf die Wallets benennen – zum Beispiel über den Master-Fingerprint –, aber niemals Seedphrase oder Passphrase enthalten.
- **Vollmacht über den Tod hinaus.** Sie ermöglicht Deiner Vertrauensperson, schon vor Erteilung des Erbscheins zu handeln – auch bei einer Börse, sofern diese sie anerkennt.
- **Erbschaftsteuer.** Maßgeblich ist der Wert der Bitcoin am Todestag. Es gelten die üblichen Freibeträge. Der Erwerb muss dem Finanzamt innerhalb von drei Monaten angezeigt werden.
- **Einkommensteuer beim Verkauf.** Erben übernehmen den Anschaffungszeitpunkt der verstorbenen Person. Dokumentiere deshalb Kaufdaten und -preise – sie entscheiden später darüber, ob ein Verkauf steuerfrei ist. Liegt zwischen dem Kauf durch die verstorbene Person und dem Verkauf mehr als ein Jahr, ist der Gewinn nach heutiger Rechtslage einkommensteuerfrei.
- **Mehrere Wohnsitze.** Innerhalb der EU gilt grundsätzlich das Erbrecht des letzten gewöhnlichen Aufenthalts; im Testament kannst Du das Recht Deiner Staatsangehörigkeit wählen.

Baustein · Bitcoin im Testament

Im eigenhändigen Testament vollständig von Hand zu schreiben:

> Meine Bitcoin verteile ich wie folgt: [Vorname Nachname] erhält als Vermächtnis die Bitcoin, die dem Wallet mit dem Master-Fingerprint [Kennung] und dem XPUB [XPUB] zugeordnet sind. [Vorname Nachname] erhält als Vermächtnis die Bitcoin, die dem Wallet mit dem Master-Fingerprint [Kennung] und dem XPUB [XPUB] zugeordnet sind. Die Bitcoin im Wallet mit dem Master-Fingerprint [Kennung] und dem XPUB [XPUB] fallen in den übrigen Nachlass.
>
> Die Zugangsinformationen sind nicht Teil dieses Testaments. Eine Anleitung zur Wiederherstellung befindet sich [Ort].

HINWEIS · FINGERPRINT UND XPUB IM TESTAMENT

Master-Fingerprint und XPUB zusammen bezeichnen ein Wallet eindeutig und verraten keine Zugangsdaten. Der XPUB ist allerdings über hundert Zeichen lang – im handschriftlichen Testament ist das fehleranfällig. Schreibe ihn sehr sorgfältig ab oder nutze ein notarielles Testament, in das er sicher übernommen werden kann.

Bedenke: Nach der Eröffnung können alle Beteiligten mit dem XPUB die Guthaben einsehen – das ist im Erbfall gewollt.

MUSTER · KEINE RECHTSBERATUNG

Lass den Baustein zusammen mit Deinem übrigen Testament von einem Notar oder Fachanwalt für Erbrecht prüfen – insbesondere, wenn es Pflichtteilsberechtigte gibt, die Bitcoin einen großen Teil Deines Vermögens ausmachen oder Du Wohnsitze in mehreren Ländern hast.

TESTEN UND AKTUELL HALTEN

Ein System, das auch in zehn Jahren funktioniert

Bitcoin-Vorsorge ist kein einmaliges Projekt. Geräte ändern sich, Menschen ändern sich, und ein System, das niemand geprüft hat, versagt im entscheidenden Moment.

- **Einmal im Jahr:** Siegel prüfen, Lesbarkeit der Metallplatte kontrollieren, eine Wiederherstellung auf einem Zweitgerät testen.
- **Nach jedem Test:** Wurde ein Siegel geöffnet oder eine Passphrase sichtbar, neu versiegeln – im Zweifel die Bitcoin auf ein neues Wallet übertragen.
- **Bei Veränderungen:** neues Wallet, neue Passphrase, Geburt oder Tod eines Erben, Trennung, Umzug oder ein geändertes Testament – Umschläge, Brief und Testament gemeinsam anpassen.
- **Software im Blick:** Prüfe gelegentlich, ob sich Deine Wallets mit aktueller Software noch wiederherstellen lassen.

Checkliste: Bitcoin-Vorsorge

- ☐ Alle Bitcoin-Positionen in der Übersicht erfasst – ohne Zugangsdaten.
- ☐ Seedphrase selbst erzeugt, in Metall gesichert und versiegelt.
- ☐ Passphrasen je Erbe und Zweck festgelegt, Master-Fingerprints und XPUBs notiert.
- ☐ Köder-Wallet eingerichtet und plausibel befüllt.
- ☐ Umschläge für Passphrasen, XPUBs und den Hinweis auf das Versteck versiegelt und hinterlegt.
- ☐ Brief an die Erben im Notfallordner, technische Vertrauensperson informiert.

- ☐ Zuordnung der Wallets im Testament festgehalten und notariell geprüft.
- ☐ Kaufdaten und -preise dokumentiert.
- ☐ Wiederherstellung jedes Wallets erfolgreich getestet.
- ☐ Termin für den nächsten Jahrescheck eingetragen.

> *Der Schlüssel entscheidet, wer herankommt. Das Testament, wem es gehört. Beides muss zusammenpassen.*

Vera Vorsorge

KERNAUSSAGEN

Was Du mitnehmen solltest

- Bei Bitcoin in Eigenverwahrung gibt es keine Bank, die Erben hilft – ohne vorbereitete Übergabe sind sie verloren.
- Seedphrase in Metall plus Passphrasen trennt, was man finden kann, von dem, was man wissen muss – und erlaubt eine klare Aufteilung auf mehrere Erben.
- Passphrasen, XPUBs und der Hinweis auf das Versteck bleiben versiegelt, bis der Ernstfall eintritt.
- Das Testament benennt die Wallets, verrät aber keine Zugangsdaten. Technik und Testament müssen zusammenpassen.
- Das beste Verfahren ist das, das Du und Deine Erben dauerhaft beherrschen – und das Du regelmäßig testest.

ZUM WEITERLESEN · BITCOIN-ENTDECKEN.DE

Dieser Guide gehört zum Guide „Mein digitaler Nachlass“: Schnellstart, Bestandsaufnahme, Ordnung, Zugangsverwaltung, Vollmacht und Testament, Praxistest – dazu im Anhang Notfall-Deckblatt, Vorlagen zum Ausfüllen und Glossar. Erst beide zusammen ergeben eine vollständige Vorsorge.

GLOSSAR

Die wichtigsten Begriffe

BEGRIFF	ERKLÄRUNG
Adresse	Eine Art Kontonummer, an die Bitcoin gesendet werden. Ein Wallet hat viele Adressen.
Börse	Ein Unternehmen, bei dem man Bitcoin kauft und das sie auf Wunsch für einen verwahrt (Fremdverwahrung).
Eigenverwahrung	Du verwahrst die Schlüssel zu Deinen Bitcoin selbst, ohne Bank oder Börse.
Entropie	Der Zufall, aus dem eine Seedphrase entsteht. Je echter der Zufall, desto sicherer die Seedphrase.
Erbnachweis	Oberbegriff für Dokumente, mit denen Erben ihr Erbrecht belegen – meist Erbschein oder notarielles Testament mit Eröffnungsprotokoll.
Hardware Wallet	Ein kleines Gerät, das die Schlüssel zu Bitcoin offline verwahrt und Zahlungen nur nach Bestätigung am Gerät freigibt.
Kanal-Sicherung	Sicherungsdatei eines Lightning-Nodes (Static Channel Backup). Mit ihr lassen sich die Kanäle nach einem Verlust schließen, sodass das Guthaben zurück in die Bitcoin-Blockchain fließt. Sie muss nach jeder Änderung an den Kanälen aktuell sein.
Köder-Wallet	Ein Bitcoin-Wallet ohne Passphrase, das im Fall einer Erpressung herausgegeben werden kann.
Lightning	Ein Zahlungsnetz, das auf Bitcoin aufsetzt. Zahlungen laufen schnell und günstig über Kanäle zwischen den Teilnehmern – gedacht für kleinere Beträge im Alltag.
Master-Fingerprint	Eine kurze Kennung aus acht Zeichen, die ein Bitcoin-Wallet eindeutig kennzeichnet. Damit prüfst Du, ob eine Wiederherstellung gelungen ist.
Multisig	Ein Verfahren, bei dem mehrere Schlüssel gemeinsam eine Bitcoin-Zahlung freigeben müssen.
Node	Ein Programm auf einem eigenen Rechner, das am Bitcoin- oder Lightning-Netz teilnimmt. Ein Lightning-Node verwaltet Kanäle und das Guthaben darin.
Notfallordner	Der Ordner – auf Papier oder als verschlüsselte Datei – mit allen Vorsorgeunterlagen (Guide „Mein digitaler Nachlass“, Kapitel 05). Deine Vertrauensperson weiß, wo er liegt. Dort findet sich auch der Brief an die Erben.
On-Chain	Bitcoin, die direkt in der Bitcoin-Blockchain liegen – im Gegensatz zu Guthaben in Lightning-Kanälen.
Passphrase	Ein zusätzliches Kennwort, das zusammen mit der Seedphrase ein eigenes Bitcoin-Wallet öffnet („13.“ bzw. „25. Wort“).
Seedphrase	12 oder 24 Wörter, aus denen sich alle Schlüssel eines Bitcoin-Wallets ableiten. Wer sie hat, hat die Bitcoin.

BEGRIFF	ERKLÄRUNG
Shamir-Verfahren	Eine Methode, eine Seedphrase mathematisch in mehrere Teile zu zerlegen, von denen nur eine bestimmte Anzahl zur Wiederherstellung nötig ist.
Vermächtnis	Die Zuwendung eines bestimmten Gegenstands oder Werts an eine Person im Testament – etwa der Bitcoin eines bestimmten Wallets.
Wallet	Die Software oder das Gerät, mit dem Du Deine Bitcoin-Schlüssel verwaltest und Bitcoin sendest oder empfängst. Ein Wallet enthält nicht die Bitcoin selbst, sondern die Schlüssel, die über sie verfügen.
Wallet-Deskriptor	Eine technische Beschreibung eines Bitcoin-Wallets, mit der es sich in verschiedener Software wiederherstellen lässt.
XPUB	Der öffentliche Schlüssel eines Bitcoin-Wallets. Damit kann man Guthaben ansehen, aber keine Bitcoin ausgeben.
Zeitschloss	Eine Regel, nach der ein Schlüssel erst nach Ablauf einer bestimmten Frist gültig wird.