BAND 2 · REIHE KRYPTO VERSTEHEN

KRYPTO
SICHER AUFBEWAHREN & VERERBEN

Dein Notfallplan für Coins, Wallets und Zugänge



Sicher verwahren. Klar regeln. Gut übergeben.

Krypto sicher aufbewahren & vererben

Dein Notfallplan für Coins, Wallets und Zugänge

Olaf Fleischer

Sicher verwahren. Klar regeln. Gut übergeben.

Leseprobe · Stand: November 2026

Inhalt

Vorwort 4

1 Das vergessene Vermögen 6

9 Was Erben wissen müssen, und was nicht zu früh 14

Ende der Leseprobe 24

Vorwort

01 Warum dieses Buch

Als ich „Krypto verstehen“ geschrieben habe, kam beim Kapitel über die Seed Phrase immer wieder dieselbe Frage auf: *Und was passiert damit, wenn mir etwas zustößt?* In Band 1 steht dazu ein Absatz. Die ehrliche Antwort braucht aber ein ganzes Buch.

Denn Krypto hat eine Eigenschaft, die im Alltag eine Stärke ist und im Ernstfall zur Falle wird: Niemand außer dir kommt an deine Coins heran. Keine Bank, kein Amt, kein Gericht, und ohne Vorbereitung auch nicht deine Familie.

02 Für wen das Buch gedacht ist

Für alle, die Kryptowerte besitzen, ob als Sparplan bei einer Börse oder auf einer eigenen Hardware-Wallet, und die sicherstellen wollen, dass diese Werte im Notfall bei den richtigen Menschen ankommen. Du brauchst kein Technikwissen. Wenn du Band 1 gelesen hast oder schon eine Wallet benutzt, bringst du alles mit. Wo es nötig ist, verweise ich auf die Grundlagen in Band 1.

Ein Kapitel richtet sich direkt an deine Erben: **Kapitel 12** ist so geschrieben, dass du es ausdrucken und deiner Notfallmappe beilegen kannst.

03 Was dieses Buch leisten kann

- Dir zeigen, **was du besitzt** und wo es liegt.
- Dir helfen, deine Werte **dauerhaft sicher** aufzubewahren, passend zur Höhe deines Bestands.
- Dir erklären, was gilt, wenn du **lebst, aber nicht handeln kannst**.

- Dir einen Weg zeigen, deine Werte **zu vererben**, ohne dass jemand zu früh Zugriff bekommt.
- Dir mit der **Notfallmappe** ein Werkzeug geben, das alles zusammenführt.

04 Was dieses Buch nicht leisten kann

- Es ist **keine Rechts- und keine Steuerberatung**. Wo es um Testament, Vollmacht oder Erbschaftsteuer geht, nenne ich die Grundregeln mit Quellen und sage dir, wann du einen Notar, Anwalt oder Steuerberater fragen solltest.
- Es gibt **keine Anlageempfehlung**. Ob und wie viel Krypto zu dir passt, ist eine andere Frage (Band 1, Kapitel 13).
- Es empfiehlt **keine bestimmten Produkte oder Anbieter**. Geräte, Börsen und Passwort-Manager werden bewusst nicht genannt.
- Es kann **Gesetze und Anbieterregeln nicht einfrieren**. Alle Angaben sind mit Prüfdatum versehen. Prüfe den aktuellen Stand, bevor du handelst.

05 Wie du das Buch liest

Du kannst es von vorn nach hinten lesen. Wenn du schnell anfangen willst: Lies Kapitel 1 und 2, fülle die ersten drei Seiten der Notfallmappe aus (Kapitel 14), und arbeite dich von dort aus weiter. Eine halbe Mappe heute ist mehr wert als eine perfekte irgendwann.

Durch das Buch begleitet dich **Familie Berger**: Thomas, Anja und ihre Kinder. Sie sind erfunden, ihre Fragen sind es nicht.

TEIL I · WARUM DAS THEMA DRÄNGT

01

Das vergessene Vermögen

DIE FRAGE ZUM EINSTIEG

„Ich habe ein paar hundert Euro in Bitcoin, die liegen auf meiner Wallet. Das ist doch nicht so viel, dass ich mir über Erben und Notfälle Gedanken machen muss, oder?“

Doch, und zwar gerade dann. Kleine Beträge wachsen mit einem Sparplan über die Jahre. Sie sind außerdem die, über die niemand spricht. Und Coins, von denen keiner weiß, sind im Ernstfall verloren.

DAS LERNST DU

- Du verstehst, warum Krypto im Notfall anders funktioniert als ein Bankkonto.
- Du kennst die fünf häufigsten Wege, auf denen Coins für immer verloren gehen.
- Du weißt, was zwei bekannte Fälle über das Thema lehren und was nicht.
- Du weißt, wie dieses Buch dich Schritt für Schritt zu deiner eigenen Notfallmappe führt.

01 Die Bank findet die Erben, die Blockchain findet niemanden

Stell dir zwei Nachbarn vor. Beide sterben unerwartet, beide hinterlassen 20.000 €.

Bei Frau Krüger liegt das Geld auf dem Girokonto. Die Bank erfährt vom Todesfall, sperrt das Konto und wartet auf die Erben. Die Erben müssen nachweisen, wer sie sind. Das kostet Zeit und Nerven, aber am Ende bekommen sie das Geld. Selbst ein vergessenes Sparbuch ist nicht verloren, denn die Bank kennt ihren Kunden.

Bei Herrn Yilmaz liegen die 20.000 € als Bitcoin auf einer Hardware-Wallet in der Schreibtischschublade. Niemand sperrt etwas, und niemand wartet auf die Erben. Die Blockchain weiß nicht, dass Herr Yilmaz gestorben ist, und es ist ihr gleichgültig. Sie kennt nur eine Regel: **Wer die Schlüssel hat, hat die Werte.**

Findet die Familie die Seed Phrase, ist alles gut. Findet sie sie nicht, bleiben die Bitcoin für immer auf ihrer Adresse liegen, für jeden sichtbar und für niemanden erreichbar. Es gibt keinen Kundendienst, kein Amt und kein Gericht, das daran etwas ändern kann.

Das ist kein Fehler im System, sondern die Kehrseite seiner größten Stärke. Dass niemand deine Coins sperren oder beschlagnahmen kann, bedeutet auch: Niemand kann sie für deine Erben retten.



Abbildung 1.1 Zwei Nachbarn, zwei Wege: Beim Girokonto führt der Weg über Bank, Sperre und Nachweis zu den Erben, bei der Wallet entscheidet allein, ob die Seed Phrase gefunden wird. Schematische Darstellung.

02 Fünf Wege, auf denen Coins verloren gehen

1. Tod ohne Plan

Der Klassiker und der Grund für dieses Buch. Die Familie weiß nicht, dass es Coins gibt, oder sie weiß es, findet aber den Zugang nicht. Oft liegt die Hardware-Wallet sogar im Haus, aber ohne Seed Phrase und PIN ist sie nur ein kleines Stück Plastik.

2. Krankheit, Unfall, Demenz

Weniger bekannt, aber genauso gefährlich: Du lebst, kannst aber nicht mehr handeln. Nach einem Schlaganfall, einem schweren Unfall oder bei beginnender Demenz kann niemand für dich auf die Coins zugreifen, nicht einmal, um Rechnungen zu bezahlen. Teil 3 dieses Buchs (Kapitel 7) widmet sich genau diesem Fall.

3. Die verlorene Seed Phrase

Der Zettel ist beim Umzug weggekommen, verblasst, beim Aufräumen weggeworfen oder bei einem Wasserschaden zerstört worden. Solange das Gerät funktioniert, merkst du nichts. Erst wenn es kaputtgeht, wird aus dem kleinen Versäumnis ein Totalverlust. Kapitel 4 zeigt, wie du die Wörter dauerhaft schützt.

4. Feuer, Wasser, Einbruch

Gerät und Seed Phrase liegen im selben Schrank, und der Schrank brennt. Oder ein Einbrecher nimmt beides mit. Wer alles an einem Ort aufbewahrt, hat am Ende im besten Fall gar nichts mehr und im schlimmsten Fall einen Dieb mit vollem Zugang.

5. Betrug, gerade im Ernstfall

Betrüger suchen sich Menschen in Ausnahmesituationen. Eine trauernde Witwe, die „nur kurz Hilfe bei der Wallet“ braucht, ist ein ideales Ziel. Wie du deine Familie davor schützt, zeigt Kapitel 12.

03 Zwei Fälle, die man kennen sollte

Der Mann mit der Festplatte

Der Brite James Howells hat nach eigenen Angaben im Sommer 2013 eine Festplatte weggeworfen, auf der die Schlüssel zu rund **8.000 Bitcoin** lagen. Die Festplatte landete auf einer Deponie in Newport (Wales). Über Jahre versuchte er, die Stadt zu einer Grabung zu bewegen. Im Januar 2025 wies ein Gericht seine Klage ab, und auch die Berufung scheiterte.

Die Lehre: Es gab keine Sicherung. Ein einziger Datenträger war der einzige Zugang. Mit einer Seed Phrase auf Papier, sicher an einem zweiten Ort aufbewahrt, wäre die Festplatte ersetzbar gewesen.

Die Börse, deren Chef starb

Im Dezember 2018 starb Gerald Cotten, Chef der kanadischen Kryptobörse QuadrigaCX, auf einer Reise in Indien. Kurz darauf hieß es, nur er habe die Passwörter zu den Offline-Wallets der Börse gekannt. Rund 115.000 Kunden konnten nicht mehr an ihr Geld. Es ging um bis zu 250 Mio. kanadische Dollar.

Die Geschichte schien der perfekte Beleg für „Schlüssel nur bei einem Menschen“. Doch die Wertpapieraufsicht von Ontario kam 2020 zu einem anderen Ergebnis: Ein großer Teil des Geldes war gar nicht in verlorenen Wallets, sondern durch **Betrug** des Chefs verschwunden, durch fiktive Konten und riskanten Handel mit Kundengeld.

Die Lehre ist eine doppelte:

- Wenn nur ein Mensch den Zugang hat, ist der Zugang mit ihm verloren, egal ob durch Tod oder durch Betrug.
- Wer Coins bei einer Börse lässt, vertraut darauf, dass die Börse ehrlich und gut organisiert ist. Das kann man nicht selbst prüfen. Band 1 (Kapitel 5 und 6) erklärt, worauf du bei der Wahl einer Börse und bei der Selbstverwahrung achtest.

04 Wie viel Krypto ist schon verloren?

Das weiß niemand genau. Man sieht auf der Blockchain zwar Adressen, die sich seit vielen Jahren nicht bewegt haben. Man sieht aber nicht, ob der Besitzer tot ist, den Zugang verloren hat oder einfach sehr geduldig ist. Schätzungen, die durch die Medien gehen, sind deshalb mit Vorsicht zu genießen. Sicher ist nur: Es sind keine Einzelfälle, und jeder einzelne verlorene Coin ist endgültig verloren.

05 Was dieses Buch mit dir macht

Am Ende dieses Buchs hast du:

1. eine **Übersicht**, was du wo besitzt (Kapitel 2),
2. eine **Aufbewahrung**, die zu deinem Betrag passt und Feuer, Einbruch und Vergesslichkeit übersteht (Teil 2),
3. eine **Regelung für den Notfall zu Lebzeiten** (Teil 3),
4. einen **Plan für deine Erben**, mit dem sie die Werte bekommen, ohne vorher Zugriff zu haben (Teil 4),
5. eine **ausgefüllte Notfallmappe** (Teil 5 und Anhang).

Du musst dafür kein Technikprofi sein. Wenn du „Krypto verstehen“ (Band 1) gelesen hast oder schon eine Wallet benutzt, bringst du alles mit.

HÄUFIGER ANFÄNGERFEHLER

„Das lohnt sich bei meinem Betrag noch nicht.“ Ein Sparplan von 50 € im Monat ergibt nach zehn Jahren 6.000 € Einzahlungen. Ihr Wert kann darüber oder darunter liegen, aber er ist kein Kleingeld mehr. Die Notfallregelung kostet heute einen Nachmittag. Später ist sie nicht schwieriger, aber du verschiebst sie leichter.

WAS DU DIR MERKEN SOLLTEST

- Bei der Bank ist Geld im Todesfall blockiert, bei Krypto ohne Zugang verloren.
- Coins gehen meist nicht durch Hacker verloren, sondern durch fehlende Vorbereitung.
- Nur ein Mensch mit Zugang bedeutet: Der Zugang hängt an diesem einen Menschen.
- Auch kleine Beträge brauchen einen Plan, denn sie wachsen und werden vergessen.

Verständnisfragen

1. Warum kann eine Bank vergessenes Geld an Erben auszahlen, die Blockchain aber nicht?
2. Welche fünf Wege zum Totalverlust kennst du jetzt? Welcher davon betrifft dich am ehesten?
3. Was lehrt der Fall QuadrigaCX über Börsen, und was über einzelne Schlüsselinhaber?
4. Weiß heute schon jemand in deiner Familie, dass du Krypto besitzt?

Quellen

- Bitcoin buried in Newport landfill (Wikipedia, Weiterleitung von „James Howells“): 8.000 BTC, Entsorgung 2013, Klage abgewiesen 09.01.2025, Berufung abgewiesen März 2025 – geprüft am 22.11.2026. Bestätigt durch:
  - 11KBW, 09.01.2025: Klage abgewiesen, [2025] EWHC 22 (Ch)
  - Local Government Lawyer, 19.03.2025: Berufung am 13.03.2025 nicht zugelassen
  - Cointelegraph, 17.03.2025 und heise online, 13.01.2025: 8.000 BTC, Entsorgung 2013

  Alle geprüft am 22.11.2026.
- Quadriga (cryptocurrency exchange) (Wikipedia): Tod im Dezember 2018, bis zu 250 Mio. CAD, rund 115.000 Kunden – geprüft am 22.11.2026

- Ontario Securities Commission: QuadrigaCX – A Review by Staff of the OSC, 2020: Zusammenbruch durch Betrug des Chefs, keine bloß verlorenen Schlüssel; Einschätzung der Behördenmitarbeiter, kein Urteil – geprüft am 22.11.2026
- Schätzungen zu verlorenen Bitcoin: bewusst ohne Zahl, weil keine belastbare Primärquelle gefunden wurde (geprüft am 22.11.2026).

TEIL IV · VERERBEN

09

Was Erben wissen müssen, und was nicht zu früh

DIE FRAGE ZUM EINSTIEG

„Meine Frau weiß, dass ich Bitcoin habe. Aber wo, wie viel und wie sie rankommt, weiß sie nicht. Soll ich ihr einfach die Wörter geben?“

Nein, jedenfalls nicht so. Aber du hast recht, dass etwas passieren muss. Dieses Kapitel zeigt, wie du beides schaffst: Deine Erben kommen im Ernstfall an die Werte, und vorher kommt niemand heran.

DAS LERNST DU

- Du verstehst das Grundproblem, das Krypto vom Bankkonto unterscheidet.
- Du kennst die drei Dinge, die Erben wissen müssen, und das eine, das sie nicht zu früh haben dürfen.
- Du kennst drei Modelle für die Übergabe, mit ihren Stärken und Schwächen.
- Du weißt, warum du die Seed Phrase nie in zwei Hälften teilen solltest.
- Du kannst für dich ein Modell auswählen und mit der Notfallmappe (Kapitel 14) umsetzen.

01 Das Grundproblem

Stirbt jemand mit einem Girokonto, ist die Lage vergleichsweise einfach. Die Bank erfährt vom Tod, sperrt das Konto und gibt es nach Vorlage der nötigen Nachweise an die Erben frei. Das Geld ist nicht weg, nur vorübergehend blockiert.

Bei Coins in der **Selbstverwahrung** (du hältst die Schlüssel selbst, siehe Band 1, Kapitel 6) gibt es niemanden, der das übernimmt. Die Blockchain kennt keinen Erbschein. Sie kennt nur eine Regel: **Wer die**

Schlüssel hat, hat die Werte. Findet niemand die Seed Phrase, bleiben die Coins für immer auf ihrer Adresse liegen, sichtbar für alle, aber für niemanden erreichbar.

Rechtlich gehören die Coins trotzdem den Erben. Im deutschen Recht geht das Vermögen eines Verstorbenen als Ganzes auf die Erben über (**Gesamtrechtsnachfolge**, § 1922 BGB). Der Bundesgerichtshof hat 2018 am Beispiel des Kontos in einem sozialen Netzwerk entschieden, dass der Nutzungsvertrag grundsätzlich auf die Erben übergeht und sie Anspruch auf Zugang zum Konto haben. Das Recht nützt aber nichts, wenn der Zugang fehlt. Kein Gericht kann eine verlorene Seed Phrase herbeizaubern.

Daraus folgt der Zielkonflikt dieses Kapitels:

- **Zu wenig Information:** Im Erbfall ist alles verloren.
- **Zu viel Information zu früh:** Zu Lebzeiten kann jemand die Werte wegbewegen, aus Absicht, aus Neugier oder weil er selbst betrogen wurde.

02 Was Erben wissen müssen

Deine Erben müssen zunächst nur **drei Dinge** wissen, und das darf ruhig früh geschehen:

1. **Dass es Krypto gibt.** Klingt banal, ist aber der häufigste Fehler. Erben, die nichts von Coins ahnen, suchen nicht danach. Eine Hardware-Wallet sieht aus wie ein USB-Stick, und eine Metallplatte mit Wörtern landet schnell im Altmetall.
2. **Wo die Anleitung liegt.** Nicht die Wörter selbst, sondern die Notfallmappe: welche Börsen, welche Wallets, wen man anrufen soll und was man auf keinen Fall tun darf.
3. **Wem sie vertrauen können, und wem nicht.** Ein Name für Rückfragen, etwa ein technisch versierter Freund oder der Notar, und die Warnung: Wer sich nach deinem Tod meldet und „bei der Wiederherstellung helfen“ will, ist verdächtig (Kapitel 12).

Was sie **nicht zu früh** haben dürfen, ist genau eines: **den vollständigen Zugang.** Das sind die Seed Phrase und, falls vorhanden, die Passphrase zusammen. Alles in diesem Kapitel dreht sich darum, diesen einen Punkt erst im Ernstfall freizugeben.

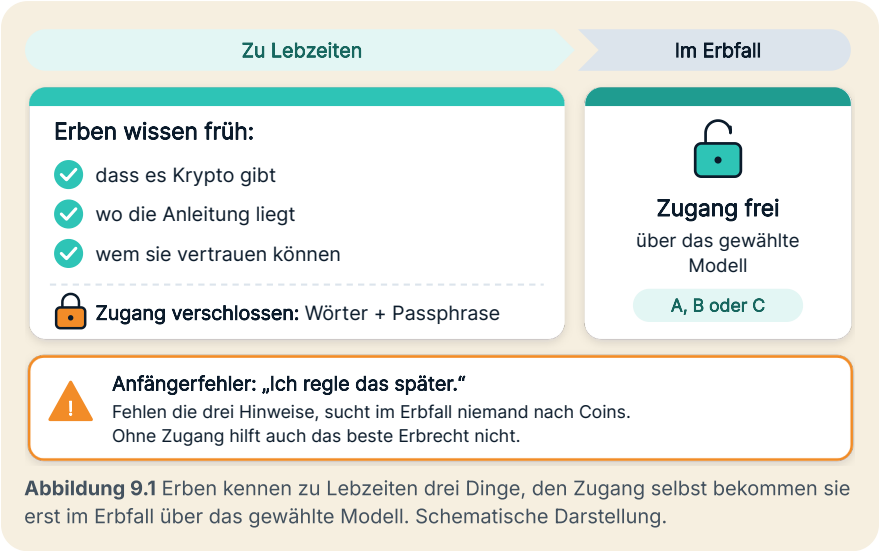

Abbildung 9.1 Erben kennen zu Lebzeiten drei Dinge, den Zugang selbst bekommen sie erst im Erbfall über das gewählte Modell. Schematische Darstellung.

03 Drei Modelle für die Übergabe

Es gibt keine perfekte Lösung, nur Abwägungen. Die folgenden drei Modelle decken die meisten Fälle ab. Du kannst sie auch kombinieren.

Modell A: die Vertrauensperson

Du übergibst die Seed Phrase in einem **versiegelten Umschlag** an eine Person, der du vollkommen vertraust, zum Beispiel an deinen Partner oder ein erwachsenes Kind. Die Anleitung liegt getrennt davon in der Notfallmappe.

- **Stärken:** einfach, kostet nichts, im Ernstfall schnell.
- **Schwächen:** Die Person *könnte* den Umschlag öffnen. Wichtiger noch: Sie könnte bestohlen werden, umziehen, den Umschlag

verlegen oder vor dir sterben. Trennungen kommen vor; dann liegt dein Zugang bei der falschen Person.

- **Passt zu:** kleinen bis mittleren Beträgen und sehr stabilen Verhältnissen.

Ein versiegelter Umschlag schützt nicht vor dem Öffnen, er macht es nur **sichtbar**. Unterschreibe quer über die Klebelasche und kontrolliere den Umschlag bei deinem jährlichen Sicherheits-Check (Kapitel 6).

Modell B: Schließfach oder amtliche Verwahrung

Die Seed Phrase liegt im **Bankschließfach**. Im Testament steht, *dass* es Krypto gibt und *wo* der Zugang liegt, aber nicht die Wörter selbst. Das Testament kann beim Amtsgericht in **amtliche Verwahrung** gegeben werden. Dann wird es im Erbfall sicher gefunden und eröffnet.

- **Stärken:** Zu Lebzeiten kommt niemand außer dir heran. Die Übergabe folgt einem geordneten Verfahren.
- **Schwächen:** Es dauert. Erben kommen meist erst nach Vorlage von Nachweisen an das Schließfach, und das kann Wochen bis Monate dauern. In dieser Zeit können die Kurse stark schwanken, ohne dass jemand handeln kann. Außerdem kostet das Schließfach jedes Jahr Geld.
- **Passt zu:** größeren Beträgen, Familien mit mehreren Erben und allen, die eine geordnete Übergabe wünschen.

Wichtig: Schreibe die Wörter **nie ins Testament selbst.** Ein Testament lesen im Erbfall viele Menschen: Nachlassgericht, Miterben, manchmal Anwälte. Ins Testament gehören die Existenz und der Fundort, nicht der Schlüssel.

Modell C: Schlüssel und Passphrase getrennt

Du nutzt zusätzlich zur Seed Phrase eine **Passphrase** (das „25. Wort“, siehe Band 1, Kapitel 7). Die Wörter liegen an einem Ort, zum Beispiel zu Hause im Tresor, die Passphrase an einem anderen, etwa bei der

Vertrauensperson oder im Schließfach.

- **Stärken:** Ein einzelner Fund reicht nicht. Wer nur die Wörter findet, sieht eine leere oder fast leere Wallet. Wer nur die Passphrase hat, kann damit nichts anfangen.
- **Schwächen:** Das ist die anspruchsvollste Lösung. Geht einer der beiden Teile verloren, ist alles verloren. Die Erben müssen zudem verstehen, dass beides zusammengehört. Ein Tippfehler bei der Passphrase erzeugt keine Fehlermeldung, sondern öffnet eine andere, leere Wallet.
- **Passt zu:** größeren Beträgen und Erben, denen du eine genaue Schritt-für-Schritt-Anleitung hinterlässt.

Die Modelle im Vergleich

	Modell A: Vertrauensperson	Modell B: Schließfach/Testament	Modell C: getrennte Teile
Schutz zu Lebzeiten	gering bis mittel	hoch	hoch
Tempo im Erbfall	schnell	langsam	mittel
Aufwand für dich	gering	mittel	hoch
Risiko „alles weg“	mittel	gering	mittel (zwei Teile)
Laufende Kosten	keine	Schließfach, Gebühren	je nach Ort

Grobe Einordnung, keine Messwerte. Deine Lage kann anders sein.

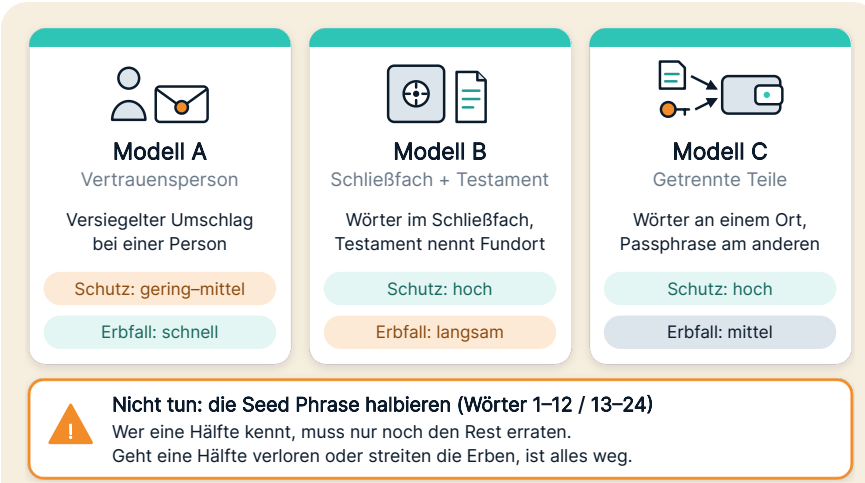

Abbildung 9.2 Die drei Übergabe-Modelle unterscheiden sich im Schutz zu Lebzeiten und im Tempo im Erbfall. Schematische Darstellung.

04 Was du nicht tun solltest: die Seed Phrase halbieren

Eine naheliegende Idee lautet: Wörter 1 bis 12 bekommt die Tochter, Wörter 13 bis 24 der Sohn. Nur beide zusammen kommen an die Coins. Klingt clever, ist aber **gefährlich**:

- **Weniger Schutz als gedacht.** Wer die Hälfte der Wörter kennt, muss nur noch die andere Hälfte erraten. Das ist zwar immer noch sehr schwer, aber deutlich leichter als bei 24 unbekannten Wörtern. Die Sicherheit einer Seed Phrase ist nicht dafür gemacht, in Teilen verteilt zu werden.
- **Doppeltes Verlustrisiko.** Geht eine Hälfte verloren, ist alles verloren.
- **Streit wird zum Totalverlust.** Zerstreiten sich die beiden Erben, blockiert einer den anderen dauerhaft.

Wenn du einen Zugang wirklich auf mehrere Personen verteilen willst, gibt es dafür eigens gebaute Verfahren: **Multisig** und **aufgeteilte Sicherungen nach Shamir**. Beide stellt Kapitel 5 vor, ehrlich mit ihren Tücken für Erben.

PRAXISBEISPIEL: FAMILIE BERGER ENTSCHEIDET SICH

Beispiel, erfundene Personen und Zahlen.

Thomas (58) hat seit 2021 einen Krypto-Sparplan. Ein Teil liegt bei einer Börse, der größere Teil auf einer Hardware-Wallet. Seine Frau Anja weiß davon, hat sich aber nie damit beschäftigt. Die beiden Kinder sind erwachsen und wohnen in anderen Städten.

Thomas überlegt:

- Modell A allein ist ihm zu unsicher. Anja würde den Umschlag nie öffnen, aber bei einem Einbruch wären Wallet *und* Umschlag im selben Haus.
- Modell B allein ist ihm zu langsam. Anja soll im Ernstfall nicht monatelang warten müssen.

Seine Lösung, eine Kombination:

1. Die **Wörter** liegen versiegelt im Bankschließfach, auf das Anja eine Vollmacht hat.
2. Die **Passphrase** liegt versiegelt bei seinem Bruder.
3. Die **Notfallmappe** liegt bei Anja im Aktenordner. Sie enthält: welche Börse, wo die Hardware-Wallet liegt, dass Schließfach *und* Bruder nötig sind, und dass sie sich Zeit lassen und niemandem mit „Hilfsangeboten“ trauen soll.
4. Im **Testament** steht ein Satz, dass Krypto vorhanden ist und die Notfallmappe bei Anja liegt.

So kommt zu Lebzeiten niemand allein an die Werte, auch nicht der Bruder. Im Ernstfall reichen aber zwei Wege, die Anja kennt.

HÄUFIGER ANFÄNGERFEHLER

„Ich regle das später." Die meisten verlorenen Coins gehen nicht durch Hacker verloren, sondern durch fehlende Vorbereitung. Unfall und Krankheit kündigen sich nicht an. Ein einfaches Modell A, heute umgesetzt, ist besser als ein perfektes Modell C, das nie fertig wird.

WAS DU DIR MERKEN SOLLTEST

- Ohne Zugang hilft auch das beste Erbrecht nicht. Die Blockchain kennt keinen Erbschein.
- Erben müssen früh wissen, *dass* es Krypto gibt und *wo* die Anleitung liegt. Den Zugang selbst bekommen sie erst im Ernstfall.
- Die Wörter gehören nie ins Testament, nur der Hinweis darauf.
- Teile die Seed Phrase nie in Hälften auf.
- Ein einfaches Modell heute ist besser als ein perfektes irgendwann.

Verständnisfragen

1. Warum gehen Coins in der Selbstverwahrung im Erbfall leichter verloren als Geld auf einem Girokonto?
2. Welche drei Dinge sollten deine Erben schon zu Lebzeiten wissen?
3. Warum gehören die Seed-Wörter nicht ins Testament?
4. Was spricht dagegen, die 24 Wörter auf zwei Personen aufzuteilen?
5. Welches der drei Modelle passt zu deiner Lage, und warum?

Quellen

- § 1922 BGB (Gesamtrechtsnachfolge) – Deutschland, geprüft am 22.11.2026
- BGH, Urteil vom 12.07.2018, III ZR 183/17, Pressemitteilung Nr. 115/2018 (Nutzungsvertrag eines sozialen Netzwerks geht grundsätzlich auf die Erben über) – Deutschland, geprüft am 22.11.2026
- § 2247 BGB (eigenhändiges Testament) und § 2248 BGB (besondere amtliche Verwahrung auf Verlangen) – Deutschland, geprüft am 22.11.2026
- BIP-39, Abschnitt „From mnemonic to seed“ (Passphrase) – github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, geprüft am 20.11.2026 (Band 1)
- Zugang zum Schließfach im Erbfall: Bedingungen der jeweiligen Bank – *allgemein formuliert lassen, keine Bank nennen*

Ende der Leseprobe

Das war ein Auszug aus **Krypto sicher aufbewahren & vererben**. Das vollständige Buch hat 15 Kapitel in fünf Teilen, Checklisten und eine ausfüllbare Notfallmappe als PDF.