SWISSRATION

Bitcoin Einsteigerleitfaden

Grundlagen verstehen
Möglichkeiten und Risiken einordnen
Bitcoin sicher verwahren

Für Menschen ohne technische Vorkenntnisse
Mit Beispielen und Hinweisen für die Schweiz

Kostenlose Ausgabe 2.1
21. Oktober 2026

Wissen für eine selbstbestimmte Entscheidung.
Ohne Kaufdruck und ohne Renditeversprechen.

Sicherheitshinweis: Dieser Leitfaden dient der allgemeinen Information. Er ersetzt keine individuelle Finanz-, Steuer- oder Rechtsberatung. Bei Bitcoin sind erhebliche Verluste bis zum Totalverlust möglich, insbesondere durch Kursverfall, Betrug, Verlust der Schlüssel oder Probleme eines Verwahrers.

Inhaltsverzeichnis

Willkommen und Orientierung....3
1 Einleitung und Entstehung von Bitcoin....4
2 Blockchain einfach erklärt....6
3 Warum Bitcoin schwer manipulierbar ist....9
4 Dezentralität und Zugriffskontrolle....11
5 Anwendungsmöglichkeiten von Bitcoin....13
6 Bitcoin als möglicher Wertspeicher....15
7 Bitcoin als Zahlungsmittel in der Schweiz....19
8 Hartes und weiches Geld....22
9 Eigenverwahrung von Bitcoin....24
10 Bitcoin kaufen und verkaufen in der Schweiz....31
11 Ist Bitcoin ein Betrug oder Schneeballsystem....34
12 Häufige Fehler im Umgang mit Bitcoin....36
Die wichtigsten Erkenntnisse....39
Glossar....41
Quellen und weiterführende Informationen....44

Willkommen zum Bitcoin Einsteigerleitfaden

Bitcoin lässt sich verstehen, ohne dass du programmieren kannst oder dich mit Börsen auskennst. Dieser Leitfaden erklärt dir, wie das Netzwerk funktioniert, welche Möglichkeiten es bietet und wo seine Grenzen liegen. Du erfährst auch, weshalb die sichere Verwahrung mindestens so wichtig ist wie das Verständnis der Technik.

Dabei unterscheiden wir zwischen dem Bitcoin-Netzwerk, der Einheit Bitcoin und den Unternehmen, die Dienstleistungen dazu anbieten. Ein Fehler bei einem Anbieter ist etwas anderes als ein Fehler im Netzwerk. Ein steigender Preis sagt wiederum wenig darüber aus, wie sicher du deine eigenen Bitcoin aufbewahrst.

Du musst keine Bitcoin kaufen, um von diesem Wissen zu profitieren. Auch die Entscheidung, Bitcoin vorerst oder dauerhaft nicht zu nutzen, kann gut begründet sein. Dieser Leitfaden enthält keine persönliche Kaufempfehlung und keine Prognose für den künftigen Preis.

So kannst du den Leitfaden nutzen

Lies die Kapitel möglichst in ihrer Reihenfolge. Die ersten vier Kapitel erklären die Grundlagen. Die Kapitel 5 bis 8 ordnen Anwendung, Werterhalt und Geldsysteme ein. Ab Kapitel 9 geht es um Verwahrung, Kauf, Verkauf und Fehlervermeidung. Unbekannte Begriffe kannst du im Glossar nachschlagen.

Nimm dir besonders für Kapitel 9 Zeit. Wenn du später selbst Bitcoin verwahren möchtest, solltest du in eigenen Worten erklären können, was ein privater Schlüssel und eine Wiederherstellungssicherung sind. Du brauchst dafür keine mathematischen Einzelheiten zu kennen.

Alle Rechenbeispiele sind erfunden und ausdrücklich keine aktuellen Kursangaben. Quellenverweise in eckigen Klammern führen zum Quellenverzeichnis. Angaben zu Schweizer Angeboten und Behörden wurden für diese Ausgabe am 21. Oktober 2026 geprüft. Sie können sich ändern.

Bitcoin im Swissration Vorsorgekonzept

Bitcoin ist bei Swissration ein eigenständiger Themenbereich innerhalb der Hauptsäule Vermögensschutz. Dieser Bereich umfasst vier Schwerpunkte: die physische Eigenverwahrung von Gold und Silber, die Fremdverwahrung von Edelmetallen, Bitcoin und digitale Vermögenswerte sowie die Nachlassregelung. Der vorliegende Leitfaden behandelt ausschliesslich Bitcoin und erklärt seine Grundlagen, Möglichkeiten, Grenzen und Risiken.

Bitcoin kann eine digitale Ergänzung sein. Er liefert aber weder Trinkwasser noch Lebensmittel, ersetzt keine Notfallreserve in verfügbaren Zahlungsmitteln und garantiert keinen Werterhalt. Auch Edelmetalle schwanken im Preis. Eine zweckmässige Vorsorge orientiert sich zuerst daran, welche Bedürfnisse und Verpflichtungen du tatsächlich hast.

Die unterschiedlichen Vorsorgebereiche werden bei Swissration eigenständig behandelt und durch entsprechende Informations- und Beratungsangebote ergänzt.

1 Einleitung und Entstehung von Bitcoin

Was Geld im Alltag leistet

Wenn du im Laden Brot kaufst, musst du dem Bäcker keine Gegenleistung anbieten, die er gerade selbst braucht. Du bezahlst mit Geld. Geld erleichtert damit den Austausch von Gütern und Dienstleistungen. Diese Aufgabe nennt man die Funktion als Tauschmittel.

Geld ist ausserdem eine Recheneinheit: Ein Brot kostet beispielsweise CHF 5, ein anderes CHF 7. Du kannst die Preise vergleichen, ohne jedes Produkt gegen jedes andere tauschen zu müssen. Als Wertspeicher soll Geld schliesslich ermöglichen, heutige Einnahmen erst später auszugeben. Wie gut das gelingt, hängt von der Entwicklung seiner Kaufkraft ab.

Diese Funktionen müssen nicht gleich gut erfüllt sein. Ein Vermögenswert kann sich leicht übertragen lassen und trotzdem stark im Preis schwanken. Ein Zahlungsmittel kann sehr verbreitet sein, obwohl seine Kaufkraft über Jahre etwas abnimmt. Deshalb genügt die Bezeichnung «Geld» allein noch nicht, um seine Eignung zu beurteilen.

Bargeld und Bankguthaben

Schweizer Franken begegnen dir als Banknoten, Münzen und Kontoguthaben. Ein Bankguthaben ist eine Forderung gegenüber deiner Bank. Die Bank führt Buch darüber, welchen Betrag sie dir schuldet, und wickelt Zahlungen nach ihren Verfahren und den geltenden Regeln ab.

Die Schweizerische Nationalbank, kurz SNB, betreibt die Geldpolitik. Geschäftsbanken schaffen bei der Kreditvergabe unter bestimmten Bedingungen zusätzliches Buchgeld, indem sie Guthaben auf Konten gutschreiben. Sie können das nicht grenzenlos tun: Finanzierung, Eigenmittel, Regulierung, Risiken und Kreditnachfrage setzen Grenzen. Geldschöpfung bedeutet daher mehr als das Drucken von Banknoten. [Q19]

Das heutige Geldsystem ermöglicht unter anderem Kredite und eine Reaktion auf wirtschaftliche Veränderungen. Zugleich verlangt es Vertrauen in Banken, Zentralbanken und staatliche Institutionen. Die SNB soll Preisstabilität gewährleisten und dabei die konjunkturelle Entwicklung berücksichtigen. Preisstabilität ist ein geldpolitisches Ziel, keine Zusage unveränderlicher Preise für jedes einzelne Produkt. [Q10]

Welche Frage Bitcoin beantworten wollte

Digitale Dateien lassen sich leicht kopieren. Eine kopierte Fotografie ist weiterhin eine brauchbare Fotografie. Bei digitalem Geld wäre beliebiges Kopieren ein Problem: Du könntest denselben Betrag mehrfach ausgeben.

Banken verhindern dies in ihren eigenen Kontobüchern. Die zentrale Frage hinter Bitcoin lautet: Wie können sich Menschen über gültige Zahlungen einigen, wenn keine einzelne Stelle das verbindliche Kontobuch führt?

Unter dem Namen Satoshi Nakamoto erschien im Oktober 2008 ein Whitepaper, also ein technisches Konzeptpapier. Es beschrieb ein elektronisches Zahlungssystem, in dem Teilnehmer direkt miteinander kommunizieren können. Der englische Ausdruck dafür ist «Peer-to-Peer». Vorgesehen war ein Verfahren gegen doppelte Ausgaben ohne zentrale Abrechnungsstelle. [Q1]

Finanzkrise und Netzwerkstart

Die Veröffentlichung fiel in die Finanzkrise von 2008. Bankenrettungen und die Stabilität des Finanzsystems wurden damals intensiv diskutiert. Im ersten Bitcoin-Block ist eine Zeitungszeile vom 3. Januar 2009 über eine mögliche weitere britische Bankenrettung hinterlegt. Das belegt den historischen Bezug. Es beweist jedoch nicht, dass die Krise der einzige Entstehungsgrund war. [Q8]

Am 3. Januar 2009 entstand dieser erste Block, auch Genesisblock genannt. Im Januar folgten die Veröffentlichung der Software und der weitere Netzwerkbetrieb. Wer hinter dem Namen Satoshi Nakamoto steht, ist nicht verlässlich geklärt. Bitcoin baut zudem auf älteren Arbeiten zu digitalen Signaturen und digitalen Zahlungssystemen auf.

In der frühen Phase experimentierten vor allem technisch interessierte Menschen mit Bitcoin. Später kamen Handelsplätze, Zahlungsdienste und spezialisierte Geräte hinzu. Aus dieser Entwicklung lässt sich keine sichere Aussage über die Zukunft ableiten: Frühere Verbreitung und frühere Kursanstiege garantieren keine weitere Nachfrage.

Merksatz: Bitcoin verbindet eine digitale Werteinheit mit einem offenen Verfahren zur Prüfung von Zahlungen. Seine Entstehung ist eine historische Tatsache; seine zukünftige wirtschaftliche Bedeutung bleibt offen.

2 Blockchain einfach erklärt

Ein gemeinsames öffentliches Kassenbuch

Stell dir einen Verein vor, dessen Mitglieder Kopien eines Kassenbuchs führen. Neue Einträge sollen nur gelten, wenn sie den gemeinsam vereinbarten Regeln entsprechen. Niemand darf nachträglich unbemerkt eine Einnahme erfinden oder denselben vorhandenen Betrag zweimal ausgeben.

Bei Bitcoin übernimmt die Blockchain eine vergleichbare Aufgabe. «Block» bezeichnet ein Paket von Transaktionen, «Chain» die Kette dieser Pakete. Viele Computer prüfen die Daten unabhängig voneinander. Einen solchen vollständig prüfenden Netzwerkteilnehmer nennt man Full Node, auf Deutsch etwa vollständiger Prüfknoten.

Der Vergleich hat eine Grenze: Bitcoin führt keine Namensliste mit persönlichen Bankkonten. Das Netzwerk erfasst übertragene Beträge und die Bedingungen, unter denen diese weiter ausgegeben werden dürfen. Deine Wallet, also deine Verwaltungssoftware, berechnet daraus den für dich verfügbaren Bestand. Die öffentlich sichtbaren Angaben sind normalerweise Adressen und technische Daten, keine im Protokoll hinterlegten Kundennamen. [Q2, Q3]

Von einer Zahlung zum Block

Angenommen, Anna möchte Beat einen Bitcoin-Betrag senden. Ihre Wallet erstellt dafür eine Transaktion. Darin steht vereinfacht, welcher bisher verfügbare Betrag verwendet wird und wohin die neuen Beträge gehen sollen. Anna gibt die Zahlung mit ihren geheimen Schlüsseln frei, ohne diese Schlüssel selbst zu veröffentlichen.

Die Transaktion wird an das Netzwerk übermittelt. Prüfknoten kontrollieren unter anderem, ob die Freigabe gültig ist und die verwendeten Beträge verfügbar sind. Gültige, noch nicht bestätigte Transaktionen können sie in ihrem vorläufigen Speicher behalten. Dieser heisst Mempool. Es gibt keine einzige weltweite Warteschlange: Die Speicher einzelner Knoten können sich unterscheiden.

Miner stellen aus geeigneten Transaktionen einen möglichen Block zusammen. Sie betreiben dafür spezialisierte Computer. Erst wenn ein Miner den erforderlichen Arbeitsnachweis gefunden hat, kann sein Block von anderen Teilnehmern als gültige Erweiterung akzeptiert werden. Die Prüfknoten kontrollieren auch diesen Block selbstständig.

Eine Bitcoin-Zahlung im Überblick

Vereinfachter Ablauf bei Eigenverwahrung. Eine Bestätigung entsteht mit der Aufnahme in einen akzeptierten Block. Weitere Blöcke erhöhen die Zahl der Bestätigungen; eine feste Wartezeit ist nicht garantiert.

Warum die Blöcke zusammenhängen

Jeder neue Block enthält einen Verweis auf den vorherigen Block. Dafür wird ein Hash verwendet: eine durch Berechnung erzeugte Zeichenfolge, die wie ein digitaler Fingerabdruck bestimmter Daten wirkt. Werden die Daten verändert, ergibt sich praktisch ein anderer Fingerabdruck.

Eine nachträgliche Änderung betrifft deshalb auch die Verknüpfung zu den folgenden Blöcken. Ein Angreifer kann nicht einfach eine einzelne Zeile austauschen und die übrige Kette unverändert weiterverwenden. Er müsste eine konkurrierende gültige Geschichte mit genügend Arbeitsnachweisen aufbauen. Wie dieser Schutz funktioniert, erklärt Kapitel 3. [Q1, Q2]

Die Verknüpfung der Blöcke

Jeder Verweis zeigt rückwärts zum vorherigen Block.

Wird ein alter Block verändert, ändern sich Fingerabdrücke.
Die betroffene Folge braucht neue gültige Arbeitsnachweise.

Die Pfeile zeigen die Verweise auf Vorgängerblöcke. Wer die Vergangenheit ändern will, muss gültige Arbeitsnachweise neu aufbauen und gegenüber der weiterlaufenden Kette aufholen. Zusätzliche Bestätigungen erschweren dies; absolute Unveränderlichkeit ist damit nicht garantiert.

Was Bestätigungen bedeuten

Wird Annas Transaktion in einen akzeptierten Block aufgenommen, hat sie eine Bestätigung. Folgt ein weiterer Block, sind es zwei Bestätigungen. Jeder zusätzliche Block baut auf der bereits akzeptierten Geschichte auf.

Das Netzwerk zielt langfristig auf durchschnittlich etwa zehn Minuten pro Block. Daraus folgt keine garantierte Wartezeit. Ein Block kann deutlich früher oder später entstehen. Ausserdem wird deine Transaktion möglicherweise erst in einen späteren Block aufgenommen, etwa wegen einer niedrigen Gebühr oder hoher Nachfrage.

Ein Anbieter kann mehrere Bestätigungen verlangen, bevor er eine Einzahlung gutschreibt. Welche Anzahl angemessen ist, hängt unter anderem vom Betrag und vom Risiko ab. Die verbreitete Zahl von sechs Bestätigungen ist keine allgemeingültige Sicherheitsgarantie und bedeutet auch nicht zuverlässig eine Stunde Wartezeit.

Warum eine Anzeige noch keine endgültige Zahlung ist

Eine Wallet kann eine eingehende Transaktion bereits anzeigen, bevor sie bestätigt ist. Das ist zunächst die Information, dass eine Zahlung im Netzwerk gesehen wurde. Es ist noch kein belastbarer Nachweis, dass sie dauerhaft in der akzeptierten Geschichte bleibt.

Auch bestätigte Blöcke können bei einer sogenannten Reorganisation ersetzt werden, wenn sich eine konkurrierende gültige Kette mit mehr kumulierter Rechenarbeit durchsetzt. Bei wenigen Bestätigungen ist dieses Risiko höher. Für Einsteiger genügt deshalb die praktische Regel, den Bestätigungsstatus zu beachten und die Vorgaben des Empfängers einzuhalten.

Merksatz: Eine Bestätigung ist ein Schritt zu höherer Sicherheit. Bitcoin hat weder eine feste Zehn-Minuten-Lieferfrist noch eine zentrale Stelle, die jede Zahlung endgültig garantiert.

3 Warum Bitcoin schwer manipulierbar ist

Digitale Signaturen schützen die Freigabe

Wenn du eine Überweisung unterschreibst, soll die Bank erkennen, dass du den Auftrag erteilt hast. Bitcoin nutzt dafür eine digitale Signatur. Sie wird mit einem privaten Schlüssel erzeugt. Das ist eine geheime Zahl, die deine Wallet verwaltet.

Andere Teilnehmer können die Signatur prüfen, ohne den privaten Schlüssel zu kennen. Die Freigabe ist an die betreffende Transaktion gebunden. Eine gültige Signatur für eine Zahlung lässt sich daher nicht einfach als allgemeine Vollmacht für beliebige weitere Zahlungen verwenden.

Der Vergleich mit einer Unterschrift erklärt die Freigabe, aber nicht die Identität. Bitcoin prüft, ob die technischen Ausgabebedingungen erfüllt sind. Das Netzwerk weiss nicht, ob der Schlüssel rechtmässig verwendet oder vorher gestohlen wurde. Eine Zahlung eines Diebes kann technisch gültig sein. [Q3, Q4]

Dieselben Bitcoin zweimal ausgeben

Stell dir vor, Anna versucht, denselben verfügbaren Betrag gleichzeitig an Beat und an Carla zu senden. Beide Aufträge könnten zunächst an unterschiedlichen Stellen des Netzwerks auftauchen. Sie dürfen aber nicht beide in derselben gültigen Transaktionsgeschichte ausgeführt werden.

Die Prüfknoten erkennen, dass beide Zahlungen denselben früheren Betrag verwenden. Wird eine davon Teil der akzeptierten Geschichte, ist dieser Betrag verbraucht. Die konkurrierende Zahlung kann dann nicht zusätzlich gültig ausgeführt werden. Genau deshalb ist es riskant, eine unbestätigte Zahlung bereits wie endgültig erhaltenes Geld zu behandeln.

Wie setzt deine Wallet einen Zahlungsbetrag zusammen? Sie verwendet einzelne noch verfügbare Beträge aus früheren Transaktionen. Reichen diese zusammen über den Zahlungsbetrag und die Gebühr hinaus, entsteht normalerweise ein Restbetrag für dich selbst. Diese noch nicht ausgegebenen Transaktionsausgänge heissen UTXO. Es handelt sich nicht um physische Münzen auf deinem Gerät.

Proof of Work als Arbeitsnachweis

Wie wird es aufwendig, eine konkurrierende Transaktionsgeschichte aufzubauen? Miner müssen mit spezialisierten Computern sehr viele Rechenversuche durchführen, bis ein Ergebnis die Vorgaben des Netzwerks erfüllt. Dieses Verfahren heisst Proof of Work, also Arbeitsnachweis. Das Finden ist aufwendig; das Überprüfen des gefundenen Ergebnisses ist vergleichsweise einfach.

Ein Alltagsvergleich ist ein Zahlenschloss, bei dem sehr viele Kombinationen ausprobiert werden müssen. Der Vergleich erklärt den Aufwand, aber nicht alle mathematischen Einzelheiten. Die Rechenarbeit erzeugt keine beliebigen Bitcoin: Auch ein erfolgreich gefundener Block muss sämtliche Regeln einhalten.

Die Schwierigkeit wird im Bitcoin-Hauptnetz nach jeweils 2’016 Blöcken angepasst. Damit soll die durchschnittliche Zeit pro Block langfristig ungefähr zehn Minuten betragen. Fällt plötzlich viel Rechenleistung aus, können Blöcke bis zur Anpassung langsamer eintreffen. [Q8]

Die Kette mit der meisten Arbeit

Bei konkurrierenden gültigen Ketten orientieren sich Prüfknoten an der insgesamt nachgewiesenen Rechenarbeit. Entscheidend ist nicht eine Abstimmung nach Anzahl Computer und auch nicht bloss die grösste Anzahl Blöcke.

Wer ältere Transaktionen umordnen möchte, muss die Arbeit für eine konkurrierende Geschichte aufbringen und gegenüber der weiterlaufenden Kette aufholen. Mit zusätzlichen Bestätigungen wird dies unter den üblichen Sicherheitsannahmen schwieriger. Die Schutzwirkung hängt unter anderem davon ab, wie viel Rechenleistung ein Angreifer kontrolliert. [Q1, Q2]

Was ein mächtiger Angreifer könnte

Ein Angreifer mit einem grossen Anteil der Rechenleistung könnte versuchen, eigene Zahlungen rückgängig erscheinen zu lassen und denselben Betrag anders auszugeben. Er könnte auch die Aufnahme bestimmter Transaktionen behindern. Bei dauerhafter Kontrolle über die Mehrheit der Rechenleistung spricht man häufig von einem 51-Prozent-Angriff.

Diese Bezeichnung ist eine Vereinfachung, keine scharfe Grenze zwischen «sicher» und «unsicher». Angriffe können auch unterhalb einer Mehrheit mit einer gewissen Wahrscheinlichkeit gelingen. Eine Mehrheit der Rechenleistung verleiht dagegen keine Fähigkeit, beliebige fremde Signaturen zu fälschen oder für unveränderte Prüfknoten die Mengenregeln ausser Kraft zu setzen.

Netzwerksicherheit und persönliche Sicherheit

Das Netzwerk kann eine gefälschte Signatur zurückweisen. Es kann dich aber nicht daran hindern, freiwillig eine Zahlung an einen Betrüger zu bestätigen. Ebenso wenig kann es verlorene Schlüssel neu ausstellen.

Neben Angriffen bestehen Risiken durch Softwarefehler, Konzentration bei Mining-Dienstleistern und langfristige Veränderungen der Technik. Öffentliche Prüfung und verteilte Kontrolle reduzieren Risiken, beseitigen sie aber nicht. Auch der Energieverbrauch des Arbeitsnachweises ist ein realer Aufwand, dessen Umweltwirkung vom Strommix und weiteren Umständen abhängt. Langfristig soll mit sinkender Neuausgabe ein grösserer Teil der Miner-Einnahmen aus Gebühren stammen. Wie sich daraus das künftige Sicherheitsniveau entwickelt, ist eine offene wirtschaftliche Frage.

Merksatz: Bitcoin macht Regelverstösse und nachträgliche Eingriffe schwer. Für dich bleibt zusätzlich entscheidend, wer deine Schlüssel kontrolliert und welche Zahlung du tatsächlich freigibst.

4 Dezentralität und Zugriffskontrolle

Was zentral und dezentral bedeutet

Bei einem zentral geführten Kontosystem entscheidet eine zuständige Organisation, welche Einträge gültig sind. Sie kann berechtigte Korrekturen vornehmen, Zugänge sperren und Kunden bei Problemen unterstützen. Technisch kann sie trotzdem über viele Rechenzentren verfügen. «Zentral» bedeutet daher nicht zwingend, dass alles auf einem einzigen Computer liegt.

Bei Bitcoin gibt es keine einzelne Organisation mit einer allgemeinen Änderungsbefugnis über das Kontobuch. Viele Teilnehmer prüfen selbst. Dezentralität beschreibt diese Verteilung von Kontrolle. Sie bedeutet nicht, dass alle Teilnehmer gleich viel Einfluss besitzen oder dass jede Dienstleistung rund um Bitcoin dezentral organisiert ist.

Verschiedene Aufgaben im Netzwerk

Entwickler schreiben Software und schlagen Verbesserungen vor. Betreiber von Prüfknoten entscheiden, welche Software und Regeln sie verwenden. Miner liefern Arbeitsnachweise und schlagen neue Blöcke vor. Nutzer entscheiden, welche Wallets und Dienste sie einsetzen und welche Transaktionen sie freigeben.

Diese Rollen können sich überschneiden. Ein Unternehmen kann beispielsweise selbst einen Prüfknoten betreiben und gleichzeitig Kundenbestände verwahren. Trotzdem sind die Aufgaben zu unterscheiden: Ein Miner allein kann einen regelwidrigen Block nicht für alle anderen verbindlich machen. Ein Entwickler kann eine veröffentlichte Änderung nicht automatisch auf sämtlichen Computern installieren.

Nicht jeder Wallet-Nutzer prüft die gesamte Blockchain selbst. Viele Wallets beziehen Informationen von fremden Servern. Das spart Aufwand, schafft aber zusätzliche Abhängigkeiten, beispielsweise bei Datenschutz oder Verfügbarkeit. Eine eigene Node kann diese Abhängigkeit reduzieren, ist für das erste Verständnis von Bitcoin jedoch keine Voraussetzung. [Q4, Q9]

Was sich bei Regeländerungen abspielt

Bitcoin-Regeln sind in Software umgesetzt. Menschen können andere Software schreiben. Damit daraus das allgemein verwendete Bitcoin-System wird, müssen relevante Teilnehmer diese Regeln tatsächlich übernehmen.

Wenn Gruppen dauerhaft unterschiedliche, unvereinbare Regeln verwenden, kann eine Aufspaltung entstehen. Diese wird Fork genannt. Eine alternative Software erzeugt deshalb nicht automatisch zusätzliche Einheiten, die vom bisherigen Netzwerk als dieselben Bitcoin anerkannt werden. Die ökonomische Anerkennung einer solchen Abspaltung ist eine weitere, getrennte Frage.

Die Mengenbegrenzung ist somit eine durch das Netzwerk durchgesetzte Regel. Sie ist nicht ein Naturgesetz, das unabhängig von Menschen und

Software existiert. Ihre Stärke liegt gerade darin, dass eine Änderung nicht einseitig gegenüber unverändert prüfenden Teilnehmern erzwungen werden kann.

Zugriff bei einer Bank und bei Eigenverwahrung

Bei deiner Bank benötigst du einen funktionierenden Zugang und die Mitwirkung des Instituts. Eine Sperre kann beispielsweise aus gesetzlichen Gründen oder wegen eines Sicherheitsverdachts erfolgen. Dafür gibt es auch Ansprechpartner und Verfahren zur Wiederherstellung des Kontozugangs.

Bei Bitcoin-Eigenverwahrung gibt es keine vergleichbare zentrale Kontosperrstelle. Wenn du die notwendigen Schlüssel kontrollierst und eine Transaktion ins Netzwerk gelangt, kann sie nach den Netzwerkregeln verarbeitet werden. Daraus folgt aber kein grenzenloser Schutz vor Zugriffen oder Beschränkungen.

Behörden können Anbieter regulieren, Auszahlungen sperren lassen, Geräte oder Sicherungen beschlagnahmen und rechtliche Pflichten durchsetzen. Internet- oder Stromprobleme können deine Nutzung verhindern. Wer deine Schlüssel erlangt, kann unter Umständen selbst verfügen. Die tatsächliche Kontrolle hängt deshalb auch von deinem Umfeld ab.

Wo Konzentration entsteht

Viele Miner arbeiten über Mining-Pools zusammen, um Einnahmen gleichmässiger zu verteilen. Grosse Pools können Einfluss auf die Blockzusammenstellung erhalten. Auch wenige grosse Handelsplätze oder Wallet-Dienstleister können für viele Menschen wichtige Zugangspunkte sein.

Solche Konzentration verschwindet nicht dadurch, dass das Grundprotokoll offen ist. Die richtige Frage lautet deshalb: Welche Teile prüfst oder kontrollierst du selbst, und an welchen Stellen verlässt du dich auf andere?

Merksatz: Bitcoin verteilt die Kontrolle über sein Regelwerk. Deine konkrete Nutzung kann trotzdem von Unternehmen, Geräten, Infrastruktur und rechtlichen Rahmenbedingungen abhängen.

5 Anwendungsmöglichkeiten von Bitcoin

Zahlungen und digitale Übertragungen

Bitcoin ermöglicht die Übertragung eines digitalen Vermögenswerts zwischen Menschen, die sich nicht am selben Ort befinden. Der Empfänger braucht dafür keinen Zugang zu deiner Bank. Beide Seiten müssen aber passende technische Möglichkeiten haben und sich darüber einig sein, was übertragen werden soll.

Das kann für grenzüberschreitende Zahlungen interessant sein. Ein Bitcoin-Betrag lässt sich unabhängig von den Öffnungszeiten einzelner Banken an das Netzwerk übermitteln. Ob der gesamte Vorgang schneller oder günstiger ist als eine Banküberweisung, hängt vom konkreten Fall ab.

Wenn du zuerst Franken gegen Bitcoin tauschst und der Empfänger anschliessend Bitcoin gegen eine andere Währung verkauft, fallen möglicherweise mehrere Gebühren und Kursaufschläge an. Dazu kommen Wartezeiten für Identitätsprüfung, Bestätigungen und Auszahlung. Die reine Netzwerkübertragung ist nur ein Teil des Ablaufs.

Ein Beispiel über eine Landesgrenze

Du möchtest einer Bekannten den Gegenwert von CHF 200 zukommen lassen. Ihr klärt zuerst, ob sie Bitcoin behalten oder in ihre Landeswährung wechseln möchte. Danach prüft ihr die Kosten auf beiden Seiten.

Angenommen, zwischen Kauf und Verkauf sinkt der Bitcoin-Kurs. Dann kann die Bekannte weniger Gegenwert erhalten, obwohl genau die vereinbarte Bitcoin-Menge angekommen ist. Wenn die Zahlung einen festen Frankenbetrag erfüllen soll, müsst ihr auch den massgeblichen Wechselkurs und den Zeitpunkt der Umrechnung klären.

Dieses Beispiel zeigt den Unterschied zwischen Menge und Kaufkraft. Das Netzwerk kann eine bestimmte Menge übertragen. Es garantiert keinen bestimmten Wechselkurs für den späteren Verkauf.

Verwahrung ohne laufendes Kundenkonto

Du kannst Bitcoin selbst verwahren, ohne dass ein Unternehmen für jede Ausgabe zustimmen muss. Dazu verwaltest du die nötigen Schlüssel. Eine ausgeschaltete Hardware-Wallet verhindert nicht, dass Bitcoin an eine bereits korrekt geprüfte Empfangsadresse gesendet werden.

Zum späteren Kontrollieren der Zahlung und zum Übermitteln neuer Transaktionen brauchst du wieder Zugang zu geeigneter Infrastruktur. Eine Hardware-Wallet ist dabei kein physischer Behälter für Bitcoin. Sie dient der geschützten Freigabe. Kapitel 9 erklärt diesen Unterschied ausführlich.

Was bei Stromausfall passiert

Wenn in deiner Wohnung der Strom ausfällt, verschwinden dadurch nicht die Einträge der weltweiten Blockchain. Andere Teile des Netzwerks können weiterarbeiten. Deine eigene Möglichkeit, eine Zahlung vorzunehmen, kann trotzdem eingeschränkt sein.

Ein geladenes Mobiltelefon allein genügt nicht in jeder Situation. Du brauchst gewöhnlich eine nutzbare Datenverbindung; auch der Empfänger und beteiligte Dienste müssen erreichbar sein. Alternative Übertragungswege sind technisch möglich, aber kein verlässlicher Ersatzplan für Menschen ohne entsprechende Vorbereitung.

Bei einer grösseren regionalen Störung können deshalb Bargeld, Vorräte und andere unmittelbare Hilfsmittel praktischer sein. Bitcoin ist kein universelles Zahlungsmittel für einen Stromausfall und keine Lösung für fehlende Lebensmittel oder Trinkwasser.

Grenzen im täglichen Gebrauch

Ein Händler muss Bitcoin überhaupt annehmen. Die Wallets müssen den angebotenen Zahlungsweg unterstützen. Bei einer Rückerstattung braucht es die Mitwirkung des Empfängers; es gibt keine zentrale Stelle, die eine falsch ausgeführte Bitcoin-Zahlung einfach zurückbucht.

Auch der Datenschutz verlangt Aufmerksamkeit. Bitcoin-Zahlungen auf der Blockchain sind öffentlich nachvollziehbar. Adressen enthalten zwar nicht automatisch deinen Namen, können aber über Zahlungen oder Daten von Handelsplattformen mit dir verbunden werden. Bitcoin ist deshalb nicht einfach anonym. [Q13]

Merksatz: Der praktische Nutzen hängt von der gesamten Situation ab: Empfänger, Kosten, Kursrisiko, Verwahrung und Infrastruktur. Die technische Übertragbarkeit allein entscheidet noch nicht über die Eignung.

6 Bitcoin als möglicher Wertspeicher

Kaufkraft über die Zeit erhalten

Ein Wertspeicher soll ermöglichen, mit heute zurückgelegtem Vermögen später noch etwas kaufen zu können. Entscheidend ist die Kaufkraft. Wenn ein Betrag zahlenmässig unverändert bleibt, während deine Lebenshaltung teurer wird, ist seine Kaufkraft gesunken.

Für die Beurteilung sind mehrere Fragen wichtig: Wie stark schwankt der Preis? Wie rasch kommst du an den Wert heran? Welche Kosten entstehen? Kann der Vermögenswert verloren gehen? Und wie sicher ist es, dass später noch Nachfrage besteht?

Kein einzelnes Merkmal beantwortet alle diese Fragen. Ein seltener Gegenstand kann knapp und trotzdem kaum verkäuflich sein. Eine liquide Anlage kann gut handelbar sein und dennoch deutlich fallen. «Knapp» und «wertstabil» bedeuten etwas Unterschiedliches.

Die Grenze von knapp 21 Millionen

Nach den geltenden Bitcoin-Regeln werden insgesamt weniger als 21 Millionen Bitcoin durch die vorgesehene Ausgabe neu geschaffen. Die oft verwendete Angabe «21 Millionen» ist die gerundete Obergrenze. Neue Einheiten entstehen nach einem festgelegten Plan als Teil der Vergütung für gültige Blöcke.

Der neue Bitcoin-Anteil dieser Vergütung wird nach jeweils 210’000 Blöcken halbiert. Das nennt man Halving. Bei ungefähr zehn Minuten je Block entspricht das etwa vier Jahren. Die Ausgabe endet nach dem derzeitigen Plan ungefähr im Jahr 2140; das ist keine minutengenau feststehende Terminangabe. Transaktionsgebühren kommen als weiterer Bestandteil der Miner-Vergütung hinzu. [Q7, Q8]

Bereits verlorene Schlüssel verringern möglicherweise die praktisch verfügbare Menge, schaffen aber keinen Ersatzanspruch. Verlorene Bitcoin werden nicht automatisch neu ausgegeben. Auch feinere Teilbarkeit erzeugt keine zusätzliche Gesamtmenge, ähnlich wie das Wechseln einer Banknote in kleinere Einheiten ihren Gesamtwert nicht erhöht.

Drei Mengen sind zu unterscheiden: Die maximal mögliche Ausgabe liegt nach den geltenden Regeln knapp unter 21 Millionen Bitcoin. Die tatsächlich bisher erzeugte Menge lässt sich aus der öffentlich überprüfbaren Ausgabehistorie nachvollziehen. Wie viele dieser Bitcoin heute noch zugänglich sind, ist dagegen nicht exakt bekannt, weil sich verlorene private Schlüssel nicht vollständig feststellen lassen.

Die Regeln legen fest, wie viel pro Block höchstens neu ausgegeben werden darf. Nimmt ein Miner weniger in Anspruch, wird die ausgelassene Neuausgabe später nicht nachgeholt. Die geplante maximale Ausgabe ist deshalb nicht mit einer Garantie für die tatsächlich erzeugte Menge gleichzusetzen. [Q2, Q7]

Weshalb Knappheit den Preis nicht garantiert

Der Marktpreis entsteht aus Kauf- und Verkaufsbereitschaft. Die Mengenregeln begrenzen das Angebot neuer Bitcoin. Sie zwingen jedoch niemanden, Bitcoin zu kaufen oder zu behalten.

Wenn die Nachfrage fällt, kann auch der Preis eines knappen Vermögenswerts sinken. Eine Halbierung der Neuausgabe führt deshalb nicht automatisch zu einer Kursverdoppelung. Erwartungen über künftige Ereignisse können zudem bereits im Preis enthalten sein.

Wer Bitcoin als langfristigen Wertspeicher betrachtet, verbindet überprüfbare technische Eigenschaften mit einer wirtschaftlichen Erwartung: dass andere Menschen diese Eigenschaften auch künftig schätzen. Diese Erwartung kann sich erfüllen, teilweise erfüllen oder enttäuscht werden.

Bitcoin und Gold im Vergleich

Eigenschaft	Bitcoin	Physisches Gold
Existenz	Digitaler Vermögenswert.	Physisches Edelmetall.
Angebot	Nach den geltenden Regeln auf knapp 21 Millionen Bitcoin begrenzt.	Keine festgelegte Ausgabegrenze wie bei Bitcoin. Zusätzliches Gold kann gefördert werden; die natürlichen Vorkommen sind endlich.
Bereits vorhandene Menge	Die bisher erzeugte Menge lässt sich anhand der Blockchain unabhängig überprüfen.	Die historisch geförderte Menge ist nicht exakt bekannt. Wissenschaft und Branche liefern Schätzungen.
Künftig verfügbare Menge	Die künftig maximal erzeugbare Menge lässt sich nach den geltenden Regeln berechnen.	Noch vorhandene und wirtschaftlich förderbare Vorkommen sind nicht vollständig bekannt. Neue Lagerstätten können entdeckt werden.
Übertragung	Weltweit digital möglich. Transaktionen werden nach Netzwerkregeln geprüft. Technische Infrastruktur ist erforderlich.	Physische Übergabe oder Transport. Gegebenenfalls sind Echtheit, Gewicht und Feingehalt zu prüfen.

Eigenschaft	Bitcoin	Physisches Gold
Verwahrung	Private Schlüssel und Wiederherstellungswörter vor Verlust und fremdem Zugriff schützen.	Das Metall vor Verlust und Diebstahl schützen.
Preis	Erhebliche Preisschwankungen möglich.	Ebenfalls schwankender Marktpreis.
Erfahrung	Netzwerk seit 2009 in Betrieb.	Seit Jahrtausenden als Wertgegenstand verwendet.

Ein wichtiger Unterschied: Überprüfbarkeit und Echtheit

Bitcoin und Gold unterscheiden sich nicht nur durch ihre digitale beziehungsweise physische Form, sondern auch darin, wie sich Menge und Echtheit überprüfen lassen. Bei Bitcoin kann die bisher erzeugte Menge anhand der öffentlich zugänglichen Blockchain und der geltenden Regeln unabhängig nachvollzogen werden. Auch die künftig maximal mögliche Ausgabe ist durch diese Regeln festgelegt. [Q2, Q7]

Bei Gold ist die historisch geförderte Menge nur näherungsweise bekannt. Bekannte wirtschaftlich förderbare Reserven sind nicht mit sämtlichem geologisch vorhandenem Gold gleichzusetzen. Neue Lagerstätten, technische Fortschritte, Marktpreise und Förderkosten können verändern, welche Vorkommen wirtschaftlich abgebaut werden können. [Q20, Q21]

Bei der Übertragung prüfen Bitcoin-Netzwerkteilnehmer die technischen Regeln. Bei physischem Gold sind beim Kauf oder bei der Übergabe gegebenenfalls Echtheit, Gewicht und Feingehalt zu prüfen. Das betrifft Barren und Münzen, besonders auch Privatkäufe, Wiederverkäufe und andere Eigentümerwechsel. Herstellerprägungen, Zertifikate und Herkunft geben Hinweise, ersetzen aber nicht in jedem Fall eine unabhängige Prüfung. [Q22]

Eine technisch gültige Bitcoin-Transaktion beweist weder die rechtliche Eigentümerschaft noch eine sichere Zahlung. Du musst weiterhin Empfangsadresse, Betrag und Schlüsselverwaltung beachten. Beide Vermögenswerte haben unterschiedliche Vorteile und Risiken.

Merksatz: Bei Bitcoin lassen sich Ausgabe und Transaktionsregeln unabhängig prüfen. Goldmengen werden geschätzt; die Echtheit des Metalls ist gegebenenfalls gesondert zu prüfen.

Auch der Begriff «digitales Gold» ist nur ein Vergleich. Er hebt vor allem die Knappheit hervor. Er darf nicht verdecken, dass Gold weitere Verwendungen hat und Bitcoin andere technische, marktbezogene und betriebliche Risiken aufweist.

Warum der Preis stark schwanken kann

Die Nachfrage reagiert unter anderem auf Erwartungen, Nachrichten, Regulierung und die allgemeine Bereitschaft, Risiken einzugehen. Kreditfinanzierte Positionen können bei fallenden Kursen zwangsweise verkauft werden und Bewegungen verstärken. Nicht zu jedem Zeitpunkt stehen gleich viele Käufer und Verkäufer zur Verfügung.

Mehr Verbreitung könnte den Handel erleichtern und bestimmte Schwankungen verringern. Sie garantiert das aber nicht. Neue Risiken, konzentrierte Bestände oder veränderte Marktbedingungen können weiterhin grosse Ausschläge verursachen. Aussagen über künftig automatisch sinkende Schwankungen sind deshalb Prognosen.

Ein einfaches Rechenbeispiel: Ein Bestand im Wert von CHF 1’000 verliert 50 Prozent und ist danach CHF 500 wert. Um wieder CHF 1’000 zu erreichen, muss er vom niedrigeren Ausgangswert um 100 Prozent steigen. Das Beispiel zeigt, weshalb grosse Verluste nicht durch einen gleich hohen prozentualen Anstieg ausgeglichen werden.

Welche Rolle der Zeithorizont spielt

Wer Geld in drei Monaten für Miete, Steuern oder eine Reparatur benötigt, kann einen starken Kursrückgang nicht beliebig aussitzen. Ein langer Zeithorizont gibt mehr Zeit, garantiert aber ebenfalls keine Erholung. «Langfristig halten» beseitigt weder das Marktrisiko noch ein Verwahrungsproblem.

Diversifikation bedeutet, Vermögen auf unterschiedliche Risiken zu verteilen. Ein zusätzlicher Bitcoin-Bestand kann eine weitere Risikoquelle hinzufügen. Ob dadurch das gesamte Vermögen robuster wird, hängt von Anteil, übrigen Anlagen, Verpflichtungen und dem Verhalten der Preise zueinander ab. Eine feste Aufteilung lässt sich aus diesem Leitfaden nicht ableiten.

Merksatz: Die begrenzte Menge ist eine technische Eigenschaft. Langfristiger Werterhalt ist eine wirtschaftliche Möglichkeit, keine zugesicherte Folge dieser Begrenzung.

7 Bitcoin als Zahlungsmittel in der Schweiz

Kleine Einheiten statt ganzer Bitcoin

Du musst keinen ganzen Bitcoin kaufen oder ausgeben. Ein Bitcoin, abgekürzt BTC, lässt sich auf der Blockchain in 100’000’000 Satoshi teilen. Ein Satoshi entspricht damit 0,00000001 BTC. Die Abkürzung «sat» oder die Mehrzahl «sats» begegnet dir häufig in Wallets.

Rechenbeispiel mit einem frei gewählten Kurs: Wenn 1 BTC genau CHF 100’000 kosten würde, entspräche ein Kaffee für CHF 4 einem Betrag von 0,00004 BTC oder 4’000 Satoshi. Allfällige Gebühren kämen dazu. Bei einem anderen Kurs verändert sich die benötigte Bitcoin-Menge.

Die Teilbarkeit erleichtert kleine Zahlungen. Sie bedeutet weder, dass Bitcoin günstig bewertet ist, noch dass jede noch so kleine Zahlung auf jedem Zahlungsweg wirtschaftlich sinnvoll ist.

Die Aufgabe deiner Wallet

Eine Wallet zeigt dir einen Bestand an, erstellt Empfangsinformationen und hilft dir beim Senden. Bei Eigenverwahrung organisiert sie auch die benötigten Schlüssel beziehungsweise die Verbindung zu einem separaten Signiergerät. Ein Signiergerät gibt Zahlungen mit dem privaten Schlüssel frei.

Bei einer fremdverwahrenden Wallet kontrolliert der Anbieter die Schlüssel. Deine App ist dann vor allem ein Zugang zu seinem Dienst. Die Oberfläche kann bei beiden Varianten ähnlich aussehen. Ob eine App «Wallet» heisst, sagt deshalb noch nicht, wer die Bitcoin tatsächlich kontrolliert.

Eine gewöhnliche Bitcoin Zahlung

Eine Zahlung auf der Bitcoin-Blockchain wird als On-Chain-Zahlung bezeichnet. Der Empfänger gibt dir eine passende Empfangsadresse, oft als QR-Code. Ein QR-Code ist ein maschinenlesbares Bild, das beispielsweise Adresse und Betrag enthält.

Du scannst die Zahlungsanforderung, prüfst die Angaben und gibst die Transaktion frei. Das Scannen verhindert viele Tippfehler. Es beweist aber nicht, dass der angezeigte Code zum richtigen Empfänger gehört. Ein ausgetauschter oder gefälschter Code kann dich zu einem falschen Ziel führen.

Bei On-Chain-Zahlungen hängt die Netzwerkgebühr vor allem vom beanspruchten Datenplatz und der Nachfrage nach Blockplatz ab. Sie richtet sich nicht einfach nach einem festen Prozentsatz des Frankenbetrags. Eine kleine Zahlung kann deshalb im Verhältnis teuer werden. Die Wallet zeigt gewöhnlich einen Gebührenvorschlag an.

Was Lightning anders macht

Lightning ist ein zusätzliches Zahlungsnetz auf der Grundlage von Bitcoin. Beteiligte können Bitcoin in Zahlungskanälen binden und den verfügbaren Anteil zwischen sich verschieben, ohne jede einzelne Zahlung in die Blockchain zu schreiben. Zahlungen können über mehrere miteinander verbundene Kanäle weitergeleitet werden. Die Blockchain bleibt für die Absicherung und Abrechnung der Kanäle wichtig. [Q11]

Ein vereinfachter Vergleich ist eine laufende Abrechnung zwischen Geschäftspartnern: Nicht jede kleine Änderung wird einzeln im Hauptbuch abgeschlossen. Der Vergleich hat Grenzen, denn Lightning nutzt besondere technische Regeln, mit denen Ansprüche durchgesetzt werden können.

Lightning-Zahlungen sind häufig innerhalb von Sekunden möglich und können geringe Gebühren haben. Sie benötigen aber einen geeigneten Zahlungsweg mit ausreichend verfügbarer Kapazität. Zahlungen können scheitern. Selbstverwahrende Lightning-Lösungen benötigen ausserdem walletabhängige Verfahren zur Überwachung und Wiederherstellung der Kanäle. Kanalöffnung, Schliessung oder zusätzliche Dienste können weitere Kosten verursachen. «Lightning» bedeutet daher nicht automatisch kostenlos.

Zwei Zahlungswege im Überblick

Frage	On Chain	Lightning
Wo wird die Zahlung verarbeitet	Direkt auf der Bitcoin-Blockchain	In einem Netz von Zahlungskanälen
Wartezeit	Abhängig von Blockaufnahme und Bestätigungen	Häufig Sekunden, wenn ein Zahlungsweg verfügbar ist
Kosten	Datenumfang und Nachfrage sind wesentlich	Weiterleitung und mögliche Dienst- oder Kanalkosten
Empfang	Bitcoin-Empfangsadresse	Passende Lightning-Zahlungsanforderung
Sicherung	Wallet-Schlüssel und nötige Wiederherstellungsdaten	Zusätzlich walletabhängige Kanal- und Wiederherstellungs-verfahren

Nicht jede Wallet unterstützt beide Wege. Sende deshalb nur über den vom Empfänger ausdrücklich angebotenen Zahlungsweg. Bei Lightning genügt eine gewöhnliche Wörterliste je nach Wallet nicht zur vollständigen Wiederherstellung aller Kanalzustände. Beachte die spezifische Sicherungsanleitung.

Wo Zahlungen in der Schweiz möglich sind

Ein konkretes Beispiel ist Lugano. Die Stadt und ihre Initiative Plan ₿ dokumentieren die Nutzung von Bitcoin bei teilnehmenden Geschäften und Dienstleistungen. Die offizielle Händlerübersicht nennt Bitcoin-Lightning als unterstützten Zahlungsweg. Die jeweils aktuelle Teilnahme solltest du vor einem Besuch prüfen. [Q14]

Daraus folgt keine allgemeine Annahmepflicht für sämtliche Geschäfte in der Schweiz. Für deinen Alltag ist entscheidend, ob der konkrete Empfänger die Zahlung akzeptiert und welches Verfahren er anbietet. Eine Karte oder ein Aufkleber kann veraltet sein. Frage vor einer Bestellung nach, wenn du darauf angewiesen bist, mit Bitcoin zu bezahlen.

Der Händler kann einen Zahlungsdienst einsetzen, der Bitcoin annimmt und ihm Franken auszahlt. Die Zahlung mit Bitcoin bedeutet also nicht zwingend, dass das Geschäft selbst Bitcoin verwahrt. Ebenso ist der Kauf von Bitcoin an einem Automaten etwas anderes als das Bezahlen eines Produkts mit Bitcoin.

Eine Zahlung ruhig prüfen

Kläre zuerst den Preis in Franken und die angebotene Zahlungsart. Prüfe anschliessend Betrag, Empfängerinformationen und Gebühren in deiner Wallet. Bei einer Hardware-Wallet ist die Anzeige auf dem Gerät entscheidend. Warte nach dem Senden auf die Bestätigung des Empfängers.

Wenn die App eine unklare oder ausstehende Zahlung zeigt, sende nicht sofort erneut. Sonst riskierst du eine Doppelzahlung. Prüfe zuerst den Status und kontaktiere den Empfänger über einen bekannten Kontaktweg. Für die erste praktische Übung eignet sich ein kleiner, bewusst gewählter Testbetrag besser als eine dringende Rechnung.

Merksatz: Vor jeder Zahlung müssen Betrag, Empfänger und Zahlungsweg zusammenpassen. Bequemes Scannen ersetzt die Prüfung nicht.

8 Hartes und weiches Geld

Was mit diesen Begriffen gemeint ist

«Hartes Geld» bezeichnet in dieser Diskussion Geld oder Vermögenswerte, deren Angebot nur schwer ausgeweitet werden kann. Gold wird häufig so eingeordnet, weil zusätzliche Förderung Zeit, Arbeit und Kapital braucht. Bitcoin wird wegen seines festgelegten Ausgabeplans ebenfalls in diesem Zusammenhang genannt.

«Weiches Geld» bezeichnet hier eine vergleichsweise flexibel ausweitbare Geldmenge. Moderne staatliche Währungen werden deshalb häufig dieser Gruppe zugeordnet. Die Begriffe sind vereinfachend und teilweise weltanschaulich geprägt. Sie sind keine neutralen Gütesiegel und keine vollständige Beschreibung eines Geldsystems.

Insbesondere bedeutet «hart» nicht automatisch sicher, wertstabil oder für deinen Alltag geeignet. Bitcoin kann ein unelastisches Angebot und gleichzeitig einen stark schwankenden Preis haben. Umgekehrt kann eine flexibel gesteuerte Währung über längere Zeit relativ stabile Verbraucherpreise ermöglichen.

Geldmenge und Inflation

Inflation bezeichnet einen Anstieg des allgemeinen Preisniveaus über eine gewisse Zeit. Dass eine bestimmte Kaffeesorte teurer wird, reicht allein noch nicht, um eine allgemeine Inflation festzustellen. Dafür betrachtet man einen breiteren Warenkorb.

Wenn Geld und Ausgaben schneller wachsen als das verfügbare Angebot an Gütern und Dienstleistungen, kann das die Preise erhöhen. Der Zusammenhang ist aber nicht mechanisch. Wichtig ist auch, ob zusätzliches Geld ausgegeben oder gehalten wird, wie sich Kredite entwickeln und ob die Produktion zunimmt.

Energieknappheit, Lieferprobleme, Wechselkurse oder veränderte Nachfrage können ebenfalls zur Preisentwicklung beitragen. Eine Ausweitung der Zentralbankbilanz bedeutet daher nicht automatisch, dass sämtliche Konsumentenpreise im gleichen Verhältnis steigen. Umgekehrt kann eine Angebotsstörung Preise erhöhen, ohne dass sie einfach durch «mehr gedrucktes Geld» erklärt wird.

Was Preisstabilität für einen Haushalt bedeutet

Angenommen, dein gewöhnlicher Einkauf kostet heute CHF 100 und später CHF 103. Wenn dein verfügbares Einkommen unverändert bleibt, kannst du dir weniger leisten. Steigen Einkommen oder Zinsen ebenfalls, verändert sich das Ergebnis. Entscheidend ist deine konkrete Einnahmen- und Ausgabensituation.

Ein sinkendes allgemeines Preisniveau nennt man Deflation. Einzelne günstigere Produkte sind häufig erfreulich. Eine anhaltende breite Deflation kann aber mit schwacher Nachfrage und einer steigenden realen Schuldenlast verbunden sein. Auch sie ist daher nicht automatisch vorteilhaft.

Die SNB definiert Preisstabilität als einen jährlichen Anstieg der Konsumentenpreise von weniger als zwei Prozent; anhaltende Deflation verletzt ihr Ziel ebenfalls. Das ist die Beschreibung ihrer Strategie, keine Garantie, dass die Teuerung jederzeit in diesem Bereich liegt. [Q10]

Mögliche Vorteile einer begrenzten Menge

Befürworter harten Geldes schätzen, dass sich das Angebot nicht leicht durch kurzfristige politische Entscheidungen erhöhen lässt. Sie verbinden damit die Erwartung, dass Sparen und langfristige Planung begünstigt werden.

Das ist eine wirtschaftliche Argumentation. Die tatsächliche Wirkung hängt davon ab, wie sich Preise, Löhne, Kredite und Nachfrage entwickeln. Eine begrenzte Menge allein schützt einen Haushalt nicht davor, zum falschen Preis zu kaufen oder bei einer dringenden Ausgabe mit Verlust verkaufen zu müssen.

Auch bei einem begrenzten Grundgeld können Finanzdienstleister zusätzliche Forderungen und Kredite schaffen. Das Angebot des Basisvermögenswerts und die Menge darauf aufgebauter Ansprüche sind nicht dasselbe. Die Eigenschaften des gesamten Finanzsystems lassen sich deshalb nicht allein aus einer Obergrenze ableiten.

Mögliche Vorteile einer flexiblen Geldpolitik

Eine Zentralbank kann auf wirtschaftliche Veränderungen reagieren und unter bestimmten Voraussetzungen Liquidität bereitstellen. Liquidität bedeutet hier, dass Zahlungen und kurzfristige Finanzierungen möglich bleiben. Eine solche Reaktion kann in einer Krise zur Stabilisierung beitragen.

Gleichzeitig können Fehlentscheidungen, unangemessene Anreize oder anhaltend hohe Inflation erhebliche Kosten verursachen. Wer neue Finanzierung erhält und wer erst später höhere Preise spürt, kann unterschiedlich betroffen sein. Daraus folgt aber nicht, dass jeder frühe Empfänger automatisch gewinnt oder jeder Sparer zwangsläufig verliert.

Weshalb einfache Gesellschaftsversprechen nicht tragen

Mitunter wird behauptet, hartes Geld führe automatisch zu langlebigen Produkten und weiches Geld automatisch zu einer Wegwerfgesellschaft. Dafür reicht die Unterscheidung der Geldsysteme nicht aus. Produktqualität hängt unter anderem von Wettbewerb, Technik, Regulierung, Reparierbarkeit und Kundenwünschen ab.

Ebenso lässt sich aus einer bestimmten Geldordnung nicht zuverlässig ableiten, ob Menschen geduldiger, gerechter oder verantwortungsvoller handeln. Solche Aussagen sind Theorien oder politische Wertungen. Sie sollten nicht wie überprüfte technische Eigenschaften von Bitcoin dargestellt werden.

Merksatz: Angebotsbegrenzung und flexible Geldpolitik haben unterschiedliche Stärken und Risiken. Die Begriffe «hart» und «weich» ersetzen keine sorgfältige Betrachtung der Folgen.

9 Eigenverwahrung von Bitcoin

Was du tatsächlich verwahrst

Eine Wallet ist ein Werkzeug zur Verwaltung deiner Bitcoin-Zugänge. Die Bitcoin liegen nicht als Dateien auf dem Mobiltelefon oder auf einem USB-ähnlichen Gerät. Das Netzwerk hält fest, welche Beträge unter welchen Bedingungen ausgegeben werden dürfen.

Bei Eigenverwahrung kontrollierst du die geheimen Schlüssel, mit denen du diese Bedingungen erfüllen kannst. Ein anschaulicher Vergleich ist ein Schlüsselbund zu einem Schliessfach. Der Schlüssel ist nicht der Inhalt des Schliessfachs. Ebenso ist das Wallet-Gerät nicht der Bitcoin-Bestand selbst.

Der Vergleich endet dort, wo die digitale Kopierbarkeit beginnt. Ein geheimer Schlüssel kann unbemerkt kopiert werden. Dann besitzen zwei Personen dieselbe Möglichkeit zur Freigabe. Es gibt keine zentrale Schliessfachverwaltung, die für dich nachträglich das Schloss austauscht. Du musst den Bestand nötigenfalls an eine neue, sicher eingerichtete Wallet übertragen.

Private Schlüssel und öffentliche Informationen

Wer eine Zahlung freigeben möchte, braucht die passende geheime Information. Dieser private Schlüssel, auf Englisch Private Key, ist eine geheime Zahl. Aus ihm lassen sich mithilfe mathematischer Verfahren öffentliche Informationen ableiten. Für den normalen Gebrauch musst du diese Rechnungen nicht durchführen; die Wallet übernimmt sie.

Ein öffentlicher Schlüssel dient unter anderem dazu, digitale Signaturen zu überprüfen. Eine Empfangsadresse bezeichnet die Ausgabebedingungen für einen neu empfangenen Betrag in einer für Wallets nutzbaren Form. Öffentlicher Schlüssel und Adresse sind miteinander verbunden, aber nicht einfach zwei Namen für dieselbe Zeichenfolge. Je nach Adresstyp werden unterschiedliche technische Konstruktionen verwendet. [Q3, Q4]

Eine Empfangsadresse darfst du jemandem geben, der dir Bitcoin senden soll. Zum Empfangen braucht diese Person deinen privaten Schlüssel nicht. Für Zahlungen empfiehlt sich gewöhnlich eine neue, von derselben Wallet erzeugte Adresse. Das kann die unnötige öffentliche Verknüpfung von Zahlungen reduzieren, macht dich aber nicht automatisch anonym.

Sicherheitshinweis: Private Schlüssel und Wiederherstellungswörter gehören niemals in ein Kontaktformular, eine E-Mail, einen Chat oder eine Anfrage an einen Berater. Auch Swissration benötigt sie nicht.

Was Wiederherstellungswörter sind

Was geschieht, wenn dein Wallet-Gerät kaputtgeht? Eine vorher erstellte Sicherung kann den Zugriff auf einem geeigneten Ersatzgerät ermöglichen. Viele Wallets zeigen dafür bei der Einrichtung eine geordnete Liste von Wörtern an. Sie wird häufig Seed-Phrase, Recovery Phrase oder Wallet-

Backup genannt. «Seed» bedeutet Samen: Aus einem gemeinsamen Ausgangswert lassen sich viele verschiedene Schlüssel ableiten.

Die Wörter sind deshalb normalerweise nicht einfach ein ausgeschriebener einzelner privater Schlüssel. Sie sichern die Grundlage, aus der eine ganze Wallet mit vielen Adressen und Schlüsseln wiederhergestellt werden kann. Weit verbreitet sind zwölf oder 24 Wörter; je nach Verfahren sind andere Wortzahlen und Sicherungsformen möglich. [Q5]

Die Reihenfolge gehört zur Sicherung. Du solltest die Wörter genau in der angezeigten Schreibweise festhalten und nicht ins Deutsche übersetzen. Eine englische Wortliste bleibt beispielsweise eine englische Wortliste. Auch ein einzelner Fehler kann die Wiederherstellung erschweren oder verhindern.

Verwende nur Wörter, die eine vertrauenswürdig eingerichtete Wallet selbst erzeugt. Erfinde keine eigene Wortfolge. Übernimm keine bereits ausgefüllte Sicherungskarte aus einer Geräteverpackung und keine Wörter, die ein angeblicher Mitarbeiter für dich vorbereitet hat. Wer die Sicherung kennt, könnte den Zugang bereits kontrollieren.

PIN und zusätzliche Passphrase unterscheiden

Eine Geräte-PIN schützt gewöhnlich den Zugang zum Gerät. Sie ist nicht identisch mit den Wiederherstellungswörtern. Wer das vollständige ungeschützte Wörter-Backup kennt, kann je nach Wallet die Schlüssel auf einem anderen geeigneten Gerät wiederherstellen, ohne deine Geräte-PIN zu benötigen.

Manche Wallets ermöglichen zusätzlich eine Passphrase. Diese zusätzliche Zeichenfolge verändert die daraus abgeleitete Wallet. Die Wörter allein reichen dann nicht aus, um genau diesen Bestand wiederherzustellen. Eine verlorene Passphrase kann deshalb den Zugriff dauerhaft verhindern.

Eine Passphrase ist kein gewöhnliches Passwort mit einer Funktion «Passwort vergessen». Unterschiedliche Eingaben können unterschiedliche, gültige Wallets öffnen. Ein Tippfehler kann darum wie eine leere Wallet aussehen. Für Einsteiger ist zusätzliche Komplexität nicht automatisch zusätzliche Sicherheit. Nutze eine solche Funktion erst, wenn du ihre Folgen und die Sicherung vollständig verstehst. [Q5]

So arbeitet eine Hardware Wallet

Eine Hardware-Wallet ist ein spezialisiertes Gerät, das die geheimen Schlüssel geschützt hält und Transaktionen signiert. Eine Anwendung auf dem Computer oder Mobiltelefon bereitet den Auftrag vor. Das Gerät zeigt die wesentlichen Zahlungsdaten an und verlangt deine Bestätigung.

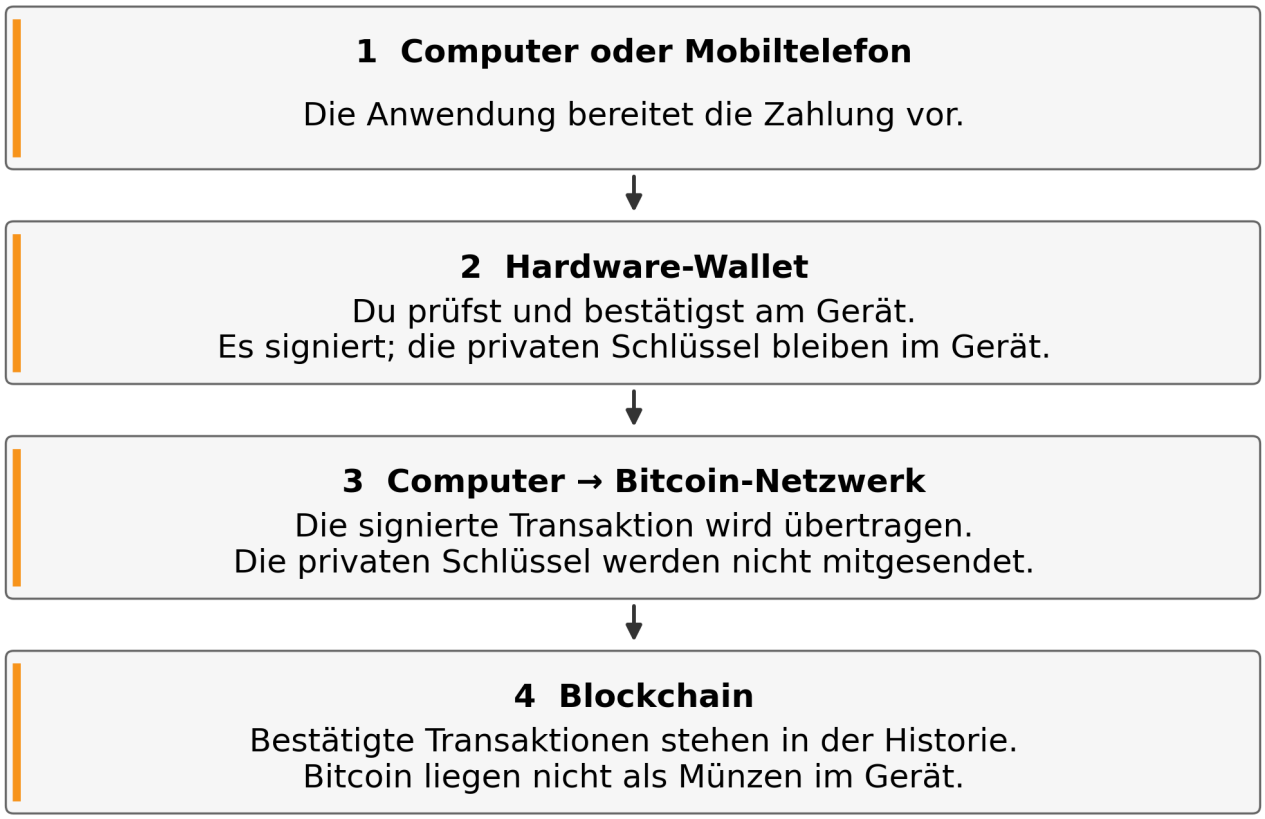
Beziehe ein neues Gerät direkt vom Hersteller oder von einem überprüften autorisierten Händler. Prüfe die Echtheit nach der offiziellen Anleitung und richte es selbst neu ein. Eine bereits vorbereitete PIN oder Wortliste ist kein vertrauenswürdiger Start.

Bei korrekter Funktionsweise verlassen die privaten Schlüssel das Gerät für die Signierung nicht. Anschliessend kann die signierte Transaktion über den Computer ins Netzwerk gelangen. Der angeschlossene Computer muss deshalb nicht dieselbe Vertrauensrolle erhalten wie das Signiergerät.

Du musst trotzdem die Anzeige auf dem Gerät kontrollieren. Eine Schadsoftware auf dem Computer könnte versuchen, eine andere Zieladresse vorzubereiten. Bestätigst du sie ungeprüft, kann auch eine Hardware-Wallet die falsche Zahlung nicht verhindern.

Prüfe die vollständige Adresse, soweit das Gerät dies ermöglicht, sowie Betrag und Gebühr. Der Vergleich nur weniger Anfangs- und Endzeichen ist schwächer, weil Betrüger ähnlich aussehende Adressen verwenden können. Bei ungewohnten Anzeigen oder einer unverständlichen Aufforderung brichst du den Vorgang ab und klärst ihn über die offizielle Anleitung.

Freigeben, ohne Schlüssel weiterzugeben



Das gilt bei korrekter Funktionsweise und sicherer Einrichtung. Kontrolliere Adresse, Betrag und Gebühr auf dem Gerät, bevor du die Zahlung bestätigst.

Hot Wallet und Cold Storage

Bei einer Hot Wallet befinden sich die Schlüssel in einer Umgebung, die mit dem Internet verbunden ist, etwa auf einem Mobiltelefon. Das ist praktisch für kleine Alltagszahlungen, vergrössert aber die Angriffsfläche durch Schadsoftware oder kompromittierte Geräte.

Cold Storage bezeichnet die Verwahrung der Schlüssel ausserhalb einer gewöhnlichen internetverbundenen Umgebung. Eine Hardware-Wallet kann

dazu beitragen. Ein «air-gapped» Gerät arbeitet ohne direkte Datenverbindung und tauscht Informationen beispielsweise über QR-Codes aus. Auch solche Verfahren sind nur so sicher wie Gerät, Software und Bedienung.

Offline-Verwahrung bedeutet nicht, dass du Bitcoin nur empfangen kannst, wenn das Gerät eingeschaltet ist. Sie beschreibt den Schutz der Schlüssel. Die Aufzeichnung der Zahlung erfolgt weiterhin im Netzwerk.

Eigenverwahrung und Fremdverwahrung vergleichen

Frage	Eigenverwahrung	Fremdverwahrung
Wer gibt technisch frei	Du mit deinen Schlüsseln	Der Anbieter nach seinen Verfahren
Bei Geräteverlust	Du brauchst eine geeignete Sicherung	Ein Kontowiederherstellungs-verfahren kann helfen
Zentrales Risiko	Schlüsselverlust, Diebstahl, Bedienfehler	Anbieterprobleme, Sperren, Auszahlungs-beschränkungen
Unterstützung	Hilfe beim Verfahren, kein zentraler Schlüsselersatz	Kundendienst und vertragliche Prozesse
Nachlass	Technischen Zugang und Berechtigung planen	Zusätzlich Verfahren und Unterlagen des Anbieters beachten

Fremdverwahrung bedeutet nicht automatisch, dass du rechtlich keinerlei Ansprüche besitzt. Eigentumszuordnung, Herausgabe und Behandlung bei einer Insolvenz hängen von Vertrag, Struktur und geltendem Recht ab. Die technische Kontrolle über die Schlüssel liegt jedoch beim Anbieter.

Eigenverwahrung reduziert diese besondere Abhängigkeit. Sie beseitigt keine Kursrisiken und macht Gerätehersteller oder Software nicht bedeutungslos. Eine überfordernde Eigenverwahrung kann für dich gefährlicher sein als eine bewusst geprüfte andere Lösung. Entscheidend ist, welche Risiken du verstehst und beherrschen kannst.

Eine sichere Sicherung vorbereiten

Notiere die Wiederherstellungswörter in einer privaten Umgebung ohne mitlaufende Kamera oder Bildschirmübertragung. Kontrolliere Schreibweise und Reihenfolge. Verwende für das grundlegende Offline-Backup kein Foto, keine Cloud, keine E-Mail und keine gewöhnliche Notiz-App. Jede digitale Kopie kann weitere Zugriffswege schaffen.

Papier ist einfach zu beschriften, kann aber durch Feuer, Wasser oder Alterung beschädigt werden. Eine geeignete Metallsicherung kann bestimmte physische Risiken verringern. Sie verhindert keinen Diebstahl. Wähle die Aufbewahrung nach den tatsächlichen Gefahren und deinen Möglichkeiten.

Eine zweite Sicherung an einem getrennten, geschützten Ort kann gegen den Verlust eines Standorts helfen. Jede zusätzliche vollständige Kopie ist gleichzeitig ein weiterer möglicher Zugang. Mehr Kopien sind deshalb nicht automatisch besser. Gerät und einzige Sicherung am selben Ort können bei einem Brand gemeinsam verloren gehen.

Bewahre ergänzende, nicht geheime Angaben zum Wallet-Typ und zum verwendeten Sicherungsverfahren nachvollziehbar auf. Bei besonderen Konstruktionen können weitere Wiederherstellungsdaten nötig sein. Ein Backup hilft nur, wenn du oder eine berechtigte Person später weiss, wie es korrekt verwendet wird. [Q6]

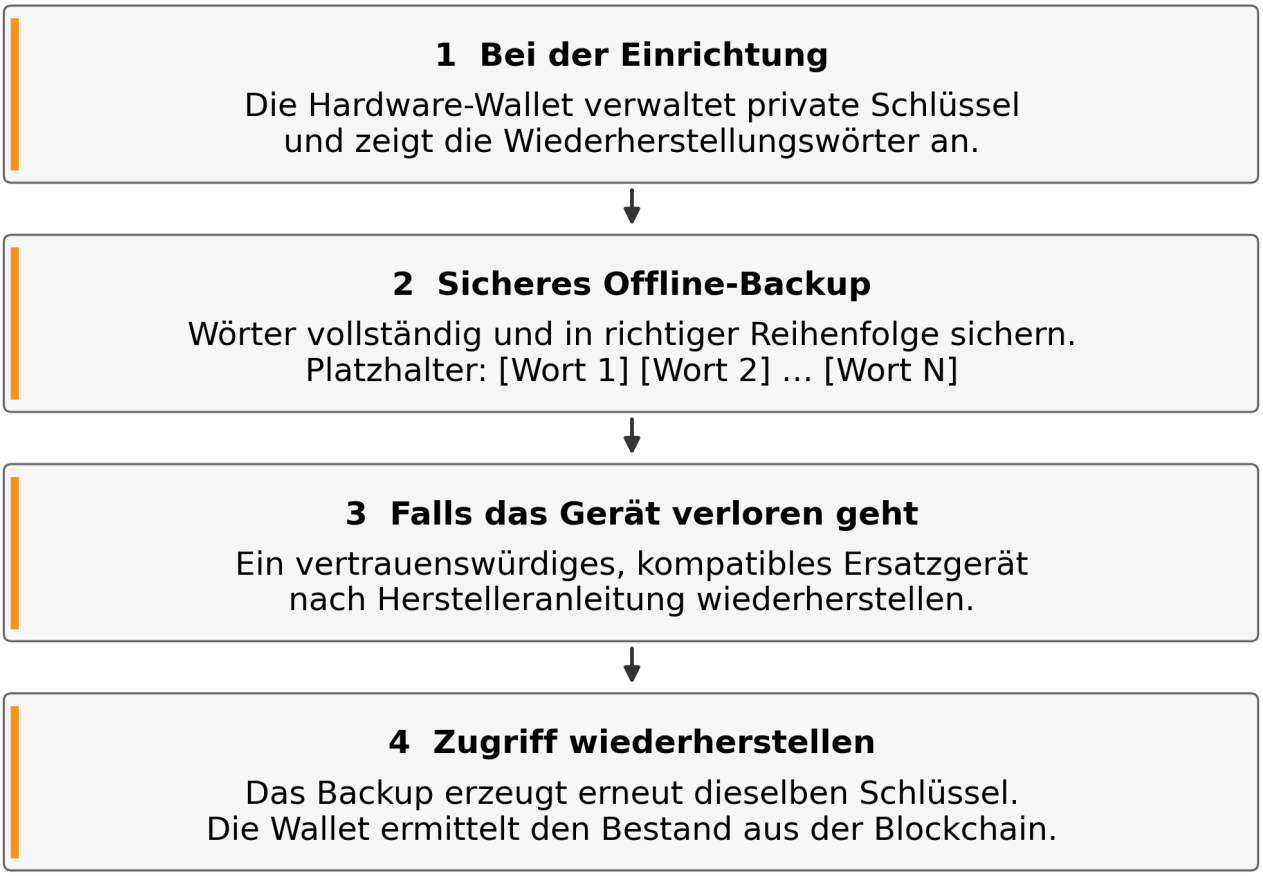
Das Backup prüfen ohne den Zugang zu gefährden

Verwende, sofern vorhanden, die offizielle Backup-Prüffunktion deines Geräts. Sie kann kontrollieren, ob die notierte Sicherung zur eingerichteten Wallet passt. Der genaue Ablauf hängt vom Modell ab. Folge der aktuellen Herstelleranleitung, die du selbst über die bekannte offizielle Adresse aufrufst. [Q15]

Setze eine bereits mit bedeutenden Werten belegte Wallet nicht bloss zu Übungszwecken zurück. Wenn sich die Sicherung als unvollständig erweist, könntest du deinen letzten funktionierenden Zugang vernichten. Eine vollständige Wiederherstellungsübung ist zunächst mit einer gesonderten Test-Wallet und einem kleinen Betrag sinnvoll.

Gib das Backup einer Hardware-Wallet nicht zur «Kontrolle» in eine beliebige Smartphone-App oder Webseite ein. Dadurch würdest du den bisherigen Offline-Schutz aufheben. Eine echte Wiederherstellung erfolgt nur bewusst, mit geeigneter vertrauenswürdiger Software oder Hardware und nach dem zum Gerät passenden Verfahren.

Zugriff nach Geräteverlust wiederherstellen



Die abgebildeten Wörter sind ausschliesslich Platzhalter, kein verwendbares Backup. Je nach Einrichtung brauchst du zusätzlich die Passphrase und weitere Wallet-Daten. Die Wiederherstellung überträgt keine Bitcoin und macht alte Geräte oder kopierte Schlüssel nicht ungültig. Gib die Wörter nur nach der geprüften Herstelleranleitung ein, niemals auf einer Webseite oder auf Aufforderung eines angeblichen Kundendienstes.

Drei Verlustfälle richtig einordnen

Das Gerät geht verloren, die Sicherung ist vorhanden. Bei einem vollständigen, passenden Backup lässt sich der Zugriff gewöhnlich auf einer kompatiblen Wallet wiederherstellen. Je nach Schutz des verlorenen Geräts kann zusätzlich eine Übertragung auf neue Schlüssel nötig sein. Die Wiederherstellung allein entzieht dem verlorenen Gerät seine bisherigen Schlüssel nicht.

Die Wörter gehen verloren, das Gerät funktioniert noch. Die Bitcoin sind nicht allein deshalb bereits verloren. Du kannst unter Umständen noch Zahlungen freigeben. Richte kontrolliert eine neue Wallet mit einer sicher geprüften Sicherung ein und übertrage den Bestand. Lösche oder setze den verbliebenen Zugang vorher nicht zurück.

Jemand könnte die Wörter kopiert haben. Behandle den Zugang als möglicherweise kompromittiert. Eine neue Geräte-PIN genügt nicht. Nötig kann die Übertragung an eine neu und sicher erzeugte Wallet sein. Nutze dafür keine Links oder Fernwartung des mutmasslichen Angreifers. Bei

Unsicherheit hole unabhängige fachliche Hilfe, ohne die Geheimnisse offenzulegen.

Wenn weder ein verwendbarer Schlüsselzugang noch eine vollständige Wiederherstellungsmöglichkeit vorhanden ist, kann der Bestand dauerhaft unzugänglich sein. Es gibt keine zentrale Stelle, die neue Schlüssel für dieselben Bitcoin ausstellt.

Nachlass und Handlungsunfähigkeit

Eine sichere Verwahrung muss auch dann verständlich bleiben, wenn du krank wirst oder stirbst. Berechtigte Angehörige sollten wissen, dass ein Bestand existiert, wo verlässliche Anweisungen zu finden sind und welche Unterstützung sie nutzen können.

Die rechtliche Berechtigung und der technische Zugriff sind zwei unterschiedliche Fragen. Ein Erbnachweis erzeugt keine verlorenen Schlüssel. Umgekehrt berechtigt der blosse Besitz einer Sicherung nicht automatisch dazu, das Vermögen für sich zu verwenden.

Lege nicht ohne fachliche Prüfung sämtliche Geheimnisse in Unterlagen, auf die zu viele Personen Zugriff erhalten könnten. Plane Auffindbarkeit und Vertraulichkeit gemeinsam. Dokumentiere den Ablauf so, dass er für deine Angehörigen tatsächlich verständlich ist, und prüfe ihn nach grösseren Änderungen erneut.

Mehrere Schlüssel für eine Freigabe

Soll eine einzelne Person oder ein einzelner verlorener Schlüssel nicht allein über den Zugang entscheiden? Eine Wallet kann so eingerichtet werden, dass eine Zahlung beispielsweise zwei von drei vorgesehenen Signaturen benötigt. Dieses Verfahren heisst Multisignatur, kurz Multisig. Es kann den Verlust eines einzelnen Schlüssels auffangen und verhindern, dass eine einzelne Person allein verfügt.

Es erhöht jedoch den Aufwand. Neben den Schlüsselsicherungen können zusätzliche Angaben zur gemeinsamen Wallet erforderlich sein. Eine unvollständige Dokumentation kann die Wiederherstellung erschweren. Multisig ist deshalb eine vertiefende Lösung für ein durchdachtes Sicherheitskonzept und kein notwendiger erster Schritt. [Q16]

Merksatz: Eine gute Verwahrung schützt vor fremdem Zugriff und erhält zugleich deinen eigenen Zugriff. Beides muss auch bei Geräteverlust, Krankheit und Nachlass funktionieren.

10 Bitcoin kaufen und verkaufen in der Schweiz

Zuerst klären was du erwerben möchtest

Nicht jedes Produkt mit «Bitcoin» im Namen ist ein direkt auszahlbarer Bitcoin-Bestand. Ein Wertpapier kann den Kurs abbilden, ohne dir eine Auszahlung an deine eigene Wallet zu ermöglichen. Ein Dienstleister kann wiederum echte Bitcoin für dich verwahren, während du nur über sein Kundenkonto darüber verfügen kannst.

Frage deshalb vor der Einzahlung: Kaufe ich Bitcoin, ein vertragliches Guthaben oder ein Wertpapier? Kann ich Bitcoin an eine eigene Adresse auszahlen? Wer verwahrt währenddessen die Schlüssel? Welche Bedingungen gelten, wenn ich verkaufen oder kündigen möchte?

Dieser Leitfaden vergleicht keine konkreten Anbieter und empfiehlt keine Handelsplattform. Angebote, Gebühren, Identitätsanforderungen und Auszahlungsverfahren ändern sich. Prüfe die für deinen Wohnsitz und dein Produkt geltenden Bedingungen jeweils direkt beim Anbieter.

Börsen Broker und Banken

Eine Börse bringt Kauf- und Verkaufsaufträge zusammen. Ein Broker wickelt den Kauf für dich ab oder nennt dir einen Preis, zu dem du handeln kannst. Eine Bank kann solche Leistungen ebenfalls anbieten oder dafür mit anderen Unternehmen zusammenarbeiten.

Die Bezeichnungen allein sagen wenig über die Sicherheit aus. Wichtig sind die tatsächlich verantwortliche Gesellschaft, die angebotene Leistung, der Verwahrungsprozess und die rechtliche Stellung deines Bestands. Ein vertraut klingender Markenname kann zudem von einer gefälschten Webseite nachgeahmt werden.

Automaten und Gutscheine können weitere Zugangswege sein. Prüfe dort ebenfalls Gebühren, Limits, Identifikation und den genauen Auszahlungsablauf. Bei einem direkten Kauf von einer Privatperson kommen Risiken wie falsche Zahlungsbestätigungen, Betrug oder persönliche Unsicherheit beim Treffen hinzu.

Ein typischer Kaufablauf

Zuerst prüfst du die Identität des Unternehmens und rufst die Webseite oder App über einen verlässlichen Weg auf. Eröffne ein Konto nur, wenn du die Bedingungen verstanden hast. Viele Anbieter verlangen eine Identitätsprüfung. Diese wird häufig KYC genannt, die Abkürzung für «Know Your Customer».

Danach zahlst du nach den offiziellen Anweisungen Franken ein. Vor dem Kauf kontrollierst du, wie viele Bitcoin du für den Gesamtbetrag tatsächlich erhältst. Bei einem sofortigen Marktauftrag hängt der Ausführungspreis von den verfügbaren Angeboten ab. Ein Auftrag mit Preisgrenze, Limit genannt, kann dagegen unausgeführt bleiben.

Wenn du selbst verwahren möchtest, richtest und prüfst du deine eigene Wallet vor der Auszahlung. Du gibst deren Empfangsadresse an und kontrollierst, dass Anbieter und Wallet dasselbe unterstützte Netzwerk verwenden. Eine erste kleine Auszahlung kann den Ablauf testen. Sie ersetzt nicht die erneute Prüfung jeder späteren Adresse.

Kosten vollständig betrachten

Eine offen ausgewiesene Handelsgebühr ist nur ein möglicher Kostenbestandteil. Hinzukommen kann ein Spread: die Differenz zwischen Kauf- und Verkaufspreis beziehungsweise ein im angebotenen Kurs enthaltener Aufschlag. Weitere Kosten können für Einzahlung, Währungswechsel oder Auszahlung entstehen.

Erfundenes Beispiel: Du setzt CHF 100 ein. Der Anbieter berechnet CHF 2 Handelskosten und CHF 3 für die anschliessende Auszahlung. Vor Kursbewegungen und einem möglichen Spread verbleiben rechnerisch CHF 95 Gegenwert auf deiner Wallet. Bei kleinen Beträgen fallen feste Kosten prozentual besonders stark ins Gewicht.

Vergleiche deshalb den tatsächlich ankommenden Bitcoin-Betrag bei gleichem Frankeneinsatz. Beachte auch, ob Auszahlungsgebühren pauschal festgelegt werden oder vom Netzwerk abhängen. Nicht jede Gebühr, die ein Anbieter verlangt, fliesst vollständig an Miner.

Anbieter prüfen ohne falsche Sicherheit

Die FINMA veröffentlicht Informationen zu bewilligten Instituten und Warnungen. Prüfe die genaue Gesellschaft und die konkrete Tätigkeit. Ein fehlender Eintrag auf einer Warnliste ist kein Sicherheitsnachweis. Eine Bewilligung oder ein Anschluss in einem bestimmten Bereich ist auch keine allgemeine Garantie für jedes angebotene Produkt. [Q17]

Lies ausserdem, ob Auszahlungen möglich sind, welche Nachweise verlangt werden können und wie ein Beschwerdeweg aussieht. Ein erfolgreicher kleiner Test ist hilfreich, beweist aber nicht die langfristige Zahlungsfähigkeit eines Anbieters. Betrüger können anfangs kleine Auszahlungen zulassen, um Vertrauen aufzubauen.

Bitcoin wieder verkaufen

Beim Verkauf an einen Anbieter erhältst du gewöhnlich zunächst eine passende Einzahlungsadresse oder nutzt einen bereits dort verwahrten Bestand. Prüfe vor einer externen Übertragung Mindestbeträge, unterstütztes Netzwerk und erforderliche Angaben. Nach den verlangten Bestätigungen kannst du nach dem vorgesehenen Verfahren verkaufen.

Der Verkaufserlös in Franken muss anschliessend noch auf dein Bankkonto ausgezahlt werden. Bestätigungen im Bitcoin-Netzwerk bedeuten nicht, dass die Bankgutschrift bereits erfolgt ist. Plane Zeit für Prüfungen, Bankarbeitstage und allfällige Nachfragen ein.

Bewahre Kaufbelege, Verkaufsbelege, Gebühren und Transaktionsnachweise auf. Solche Unterlagen erleichtern die eigene Übersicht, Herkunftsnachweise und die Steuererklärung. Teile dabei niemals deine privaten Schlüssel oder Wiederherstellungswörter.

Steuerliche Grundorientierung in der Schweiz

Bitcoin im Privatvermögen ist grundsätzlich als Vermögen zu deklarieren. Private Kapitalgewinne sind grundsätzlich steuerfrei; entsprechende private Verluste sind in der Regel nicht abzugsfähig. Bei gewerbsmässigem Handel, Geschäftsvermögen oder besonderen Einnahmen kann die Behandlung anders ausfallen. [Q18]

Die Einordnung hängt vom Einzelfall ab. Halte die Unterlagen für die zuständige Steuerbehörde bereit und prüfe aktuelle kantonale Vorgaben sowie die Hinweise der Eidgenössischen Steuerverwaltung. Diese kurze Orientierung ersetzt keine Beurteilung deiner persönlichen Situation.

Merksatz: Entscheidend ist der vollständige Weg vom Frankenkonto zum Bitcoin-Bestand und wieder zurück. Prüfe Produkt, Kosten, Verwahrung und Auszahlung vor dem ersten grösseren Betrag.

11 Ist Bitcoin ein Betrug oder Schneeballsystem

Was ein Schneeballsystem kennzeichnet

Bei einem klassischen betrügerischen Schneeball- oder Ponzi-System werden versprochene Auszahlungen wesentlich durch neue Einzahlungen finanziert und über die tatsächliche Herkunft der Erträge wird getäuscht. Frühe Teilnehmer erhalten scheinbare Gewinne, damit weitere Menschen Geld einzahlen. Bleibt der Zufluss aus, bricht das Modell zusammen.

Bei Pyramidensystemen steht häufig das Anwerben weiterer Teilnehmer im Vordergrund. Die Begriffe werden im Alltag teilweise vermischt. Für dich ist die entscheidende Frage: Wird eine Rendite versprochen, deren Grundlage unklar ist und die vom ständigen Zustrom weiterer Einzahler abhängt?

Worin sich das Bitcoin Netzwerk unterscheidet

Das Bitcoin-Protokoll besitzt keinen zentralen Betreiber, der dir eine feste Rendite verspricht oder deine Rückzahlung garantiert. Es ordnet Transaktionen nach öffentlich prüfbaren Regeln. Der Kaufpreis entsteht im Handel zwischen Marktteilnehmern.

Dass spätere Käufer einen höheren oder niedrigeren Preis zahlen, macht einen handelbaren Vermögenswert für sich genommen noch nicht zum Ponzi-System. Es bedeutet aber sehr wohl, dass du beim Verkauf auf zahlungsbereite Käufer angewiesen bist. Ohne ausreichende Nachfrage kann der Preis stark fallen.

Die Aussage «kein klassisches Schneeballsystem» beantwortet deshalb nur eine bestimmte Frage zur Struktur. Sie ist keine Aussage darüber, ob der aktuelle Preis angemessen ist, ob sich ein Kauf lohnt oder ob du Verluste vermeiden wirst.

Was Open Source bedeutet

Die Software von Bitcoin Core ist öffentlich einsehbar. Fachleute können den Quellcode untersuchen, Änderungen vorschlagen und eine eigene Version erstellen. Dieses Prinzip heisst Open Source. Die Möglichkeit zur unabhängigen Kontrolle ist eine wichtige Stärke.

Offener Quellcode beweist aber nicht, dass jede Zeile bereits von ausreichend vielen Menschen geprüft wurde. Er garantiert auch keine Fehlerfreiheit. Ausserdem kann eine gefälschte Wallet eine andere Software enthalten als diejenige, deren Code öffentlich beschrieben wird.

Als Einsteiger wirst du den Code gewöhnlich nicht selbst prüfen. Du verlässt dich auf nachvollziehbare Entwicklungsprozesse, unabhängige Prüfung und vertrauenswürdige Bezugswege. Es ist sinnvoll, diese verbleibenden Vertrauensannahmen offen anzuerkennen. [Q9]

Die unbekannte Identität des Urhebers

Die Identität von Satoshi Nakamoto ist nicht die Stelle, an der heutige Transaktionen genehmigt werden. Ein Auftauchen des ursprünglichen Urhebers würde keine automatische Administratorbefugnis über sämtliche Bitcoin verleihen.

Einfluss wäre trotzdem denkbar, etwa über öffentliche Aussagen, Entwicklungsbeiträge oder den Verkauf eigener Bestände. Technische Kontrolle, wirtschaftlicher Einfluss und persönliche Glaubwürdigkeit sind unterschiedliche Dinge. Auch hier ist eine absolute Aussage wie «die Person kann nichts bewirken» zu weitgehend.

Betrug rund um ein funktionierendes Netzwerk

Ein Betrüger kann eine echte Bitcoin-Adresse verwenden und trotzdem über den Zweck einer Zahlung lügen. Eine gefälschte Anlageplattform kann frei erfundene Gewinne anzeigen. Ein angeblicher Kundendienst kann versuchen, an deine Wiederherstellungswörter zu gelangen.

Dass Bitcoin technisch funktioniert, schützt dich vor diesen Täuschungen nicht. Umgekehrt beweist ein solcher Betrug nicht automatisch, dass das gesamte Protokoll ein betrügerisches Auszahlungssystem ist. Beurteile das Netzwerk und das konkrete Angebot getrennt.

Berechtigte Kritik ernst nehmen

Zu den sachlichen Kritikpunkten gehören hohe Preisschwankungen, aufwendige sichere Verwahrung, Energieverbrauch, öffentliche Nachverfolgbarkeit und begrenzter Platz für Transaktionen auf der Hauptkette. Auch Konzentration bei Dienstleistern und langfristige Fragen zur Finanzierung der Netzwerksicherheit verdienen Aufmerksamkeit.

Ein Angebot, das diese Punkte verschweigt und nur von Gewinnen, Freiheit oder garantierter Sicherheit spricht, vermittelt ein unvollständiges Bild. Eine fundierte Entscheidung muss auch die Möglichkeit einschliessen, dass Bitcoin für deinen Zweck ungeeignet ist.

Merksatz: Bitcoin entspricht nicht der Struktur eines klassischen Ponzi-Systems. Das macht weder jeden Anbieter seriös noch einen Bitcoin-Kauf risikofrei.

12 Häufige Fehler im Umgang mit Bitcoin

Den Kontostand mit Kontrolle verwechseln

Eine App kann einen hohen Bestand anzeigen, obwohl du ihn nicht auszahlen kannst. Bei einem seriösen Verwahrer gelten vertragliche Regeln; auf einer gefälschten Plattform können die Zahlen vollständig erfunden sein.

Prüfe deshalb, wer die Schlüssel kontrolliert und ob ein nachvollziehbares Auszahlungsverfahren existiert. Betrachte eine fehlgeschlagene Auszahlung als Anlass zur Klärung. Überweise nicht blind zusätzliches Geld, nur weil damit angeblich eine Auszahlung «freigeschaltet» werden soll.

Sicherungen verlieren oder offenlegen

Ein Wörter-Backup im selben ungeschützten Behälter wie das Gerät kann gemeinsam verloren gehen. Ein Foto kann automatisch in eine Cloud hochgeladen werden. Eine vermeintlich private Nachricht kann weitergeleitet oder von einem kompromittierten Konto gelesen werden.

Verwende eine passende Offline-Sicherung und einen bewusst gewählten Aufbewahrungsort. Prüfe die Vollständigkeit mit dem vorgesehenen Verfahren. Wenn du den Aufbewahrungsort änderst, aktualisiere auch deine Wiederherstellungs- und Nachlassanweisungen. Die Details dazu stehen in Kapitel 9.

Gefälschte Webseiten und Apps öffnen

Betrüger verwenden ähnliche Namen, Logos und Internetadressen. Auch ein Werbeplatz in einer Suchmaschine oder eine professionell aussehende App ist kein Echtheitsbeweis. Ein Schloss-Symbol im Browser zeigt eine verschlüsselte Verbindung, nicht die Seriosität des Geschäfts.

Rufe bekannte Dienste über eine selbst geprüfte Adresse auf. Prüfe den Herausgeber einer App. Behandle Links aus unerwarteten Nachrichten, Suchanzeigen oder Kommentaren mit Vorsicht. Ein Lesezeichen ist erst dann hilfreich, wenn du die ursprüngliche Adresse verlässlich geprüft hast.

Angeblichem Kundendienst vertrauen

Typische Vorwände lauten, deine Wallet müsse «synchronisiert», «validiert» oder wegen einer Sicherheitslücke «gerettet» werden. Anschliessend sollst du Wörter eingeben, einen QR-Code scannen oder Geld an eine «sichere Adresse» senden.

Beende einen solchen Kontakt und prüfe den Sachverhalt unabhängig. Nutze die Kontaktangaben, die du selbst über die bekannte offizielle Seite aufrufst. Ein seriöser Berater benötigt keine Kopie deiner Wiederherstellungswörter und sollte keine geheime Sicherung für dich aufbewahren.

Am Telefon unter Druck handeln

Ein Anrufer kann sich als Bank, Polizei, Hersteller oder bekannter Berater ausgeben. Namen und angezeigte Rufnummern sind kein ausreichender Nachweis. Besonders gefährlich sind Aufforderungen, während des Gesprächs Fernwartungssoftware zu installieren oder sofort eine Zahlung zu bestätigen.

Lege auf und rufe die betreffende Stelle über eine unabhängig ermittelte offizielle Nummer zurück. Eine echte Rückfrage hält eine Unterbrechung aus. Lasse niemanden per Bildschirmfreigabe bei der Anzeige oder Eingabe deiner geheimen Sicherung zuschauen.

Die falsche Adresse bestätigen

Schadsoftware kann eine kopierte Adresse in der Zwischenablage ersetzen. Betrüger können auch ähnlich aussehende Adressen in einer Transaktionsliste platzieren, in der Hoffnung, dass du sie für eine spätere Zahlung übernimmst.

Beziehe die Adresse frisch über einen verlässlichen Kontakt zum Empfänger. Vergleiche sie mit der Anzeige auf dem Signiergerät. Verwende nicht unbesehen eine Adresse aus einer früheren Transaktionsliste. Eine Testüberweisung prüft einen konkreten Ablauf, aber nicht automatisch jede folgende Überweisung.

Ein technisch gültiger, falsch adressierter Auftrag wird nicht dadurch ungültig, dass du ihn versehentlich bestätigt hast. Du bist dann auf die Mitwirkung des tatsächlichen Empfängers angewiesen, sofern er überhaupt erreichbar ist.

Das falsche Netzwerk auswählen

Manche Plattformen zeigen neben Bitcoin weitere Netzwerke oder Produkte mit ähnlichen Bezeichnungen an. Eine günstiger aussehende Auszahlungsoption kann ein anderes System verwenden. Ein dort dargestellter Bitcoin-Anspruch ist nicht automatisch eine gewöhnliche Bitcoin-On-Chain-Zahlung.

Wähle nur einen Weg, den Sender und Empfänger ausdrücklich unterstützen. Frage vor der Bestätigung nach, wenn die Bezeichnungen unklar sind. Eine Adresse allein und ein vertrautes Bitcoin-Symbol reichen für die richtige Zuordnung nicht in jeder Oberfläche aus.

Zu früh grosse Beträge einsetzen

Die ersten Bedienfehler passieren häufig, bevor man die Anzeigen richtig einordnen kann. Beginne daher, falls du praktisch üben möchtest, mit einem Betrag, dessen Verlust für dich verkraftbar wäre. Berücksichtige, dass feste Gebühren einen sehr kleinen Test unverhältnismässig verteuern können.

Ein sinnvoller Lernablauf besteht aus Verstehen, Sicherung prüfen, kleinem Empfang und kleinem Sendeversuch. Danach solltest du erklären können, was geschehen ist. Du musst nicht im selben Schritt eine grosse Anschaffung oder eine langfristige Anlageentscheidung treffen.

Kursbewegungen als Handlungsbefehl verstehen

Steigende Kurse können die Sorge auslösen, etwas zu verpassen. Fallende Kurse können zu überstürzten Entscheidungen führen. Beides ersetzt keine Prüfung deiner Verpflichtungen und deiner Verlusttragfähigkeit.

Überlege vor einem möglichen Kauf, wozu du den Betrag benötigst und welche Folgen ein erheblicher Verlust hätte. Verwende für einen Lernversuch keinen Kredit. Ein fester Sparrhythmus oder langes Halten beseitigt die Risiken ebenfalls nicht. Auch eine geplante Vorgehensweise darf angepasst werden, wenn sich deine Lebenssituation ändert.

Unrealistische Erträge erwarten

Bitcoin-Besitz erzeugt von sich aus keine zugesicherten Zinsen. Angebote mit festen hohen Erträgen fügen weitere Geschäfte hinzu, beispielsweise Verleih oder Handel. Dadurch entstehen zusätzliche Gegenpartei- und Verlustrisiken.

Aussagen wie «garantierter Gewinn», «kein Risiko» oder «nur heute freischalten» sind ernsthafte Warnzeichen. Überweise auch nach einem Verlust nicht an einen angeblichen Wiederbeschaffungsdienst, der gegen eine Vorauszahlung sichere Rückholung verspricht.

Was du bei einem Verdacht tun kannst

Stoppe zusätzliche Zahlungen und beende verdächtige Kontakte. Sichere Belege, Transaktionskennungen, Nachrichten und verwendete Internetadressen, ohne geheime Schlüssel weiterzugeben. Kontaktiere einen betroffenen Anbieter über seinen unabhängig geprüften offiziellen Weg.

Wenn Zugangsdaten eines Kundenkontos betroffen sind, sichere auch das zugehörige E-Mail-Konto über einen sauberen Zugang. Bei möglicherweise gestohlenen Wallet-Schlüsseln gelten die Schritte aus Kapitel 9. Bei Betrugsverdacht kannst du dich an die zuständige Polizei wenden. Eine Meldung garantiert keine Rückzahlung, kann aber für die Abklärung wichtig sein.

Merksatz: Zeitdruck ist kein Grund, eine Prüfung auszulassen. Wer dich zur Geheimnisweitergabe oder zu einer unverständlichen Sofortzahlung drängt, sollte keinen Zugriff auf dein Vermögen erhalten.

Die wichtigsten Erkenntnisse

Was du über Bitcoin verstanden haben solltest

Bitcoin ist ein offenes Netzwerk und zugleich die Bezeichnung seiner digitalen Werteinheit. Es gibt keine zentrale Bank, die sämtliche Bitcoin-Konten führt. Transaktionen werden anhand gemeinsamer Regeln geprüft und in einer Kette von Blöcken geordnet.

Digitale Signaturen erlauben die Freigabe von Zahlungen. Der Arbeitsnachweis macht eine nachträgliche konkurrierende Transaktionsgeschichte aufwendig. Mehr Bestätigungen erhöhen unter den üblichen Annahmen die Sicherheit. Eine feste Wartezeit oder absolute Unveränderlichkeit gibt es nicht.

Die Ausgabe neuer Bitcoin folgt einem festgelegten Plan mit einer Obergrenze von knapp 21 Millionen. Diese Knappheit garantiert weder Nachfrage noch einen bestimmten Preis. Erhebliche Verluste bleiben auch bei langem Halten möglich.

Bitcoin und Gold haben unterschiedliche Eigenschaften. Bitcoin ist digital und benötigt für die Nutzung technische Infrastruktur. Gold ist physisch vorhanden, muss aber ebenfalls sicher verwahrt und bei einer Übergabe geprüft werden. Keines von beiden ersetzt die elementare Versorgung.

Was vor der praktischen Nutzung zählt

Eine Wallet verwaltet Zugänge und Transaktionen. Sie ist kein Behälter mit Bitcoin-Dateien. Bei Eigenverwahrung kontrollierst du die Schlüssel; bei Fremdverwahrung liegt diese Kontrolle beim Anbieter. Beide Formen haben eigene Risiken.

Wiederherstellungswörter können den Zugang zu vielen Schlüsseln sichern. Ihre Reihenfolge und Vollständigkeit sind entscheidend. Zusätzliche Passphrasen oder besondere Wallet-Verfahren können weitere Daten erfordern. Niemand benötigt diese Geheimnisse, um dir eine gewöhnliche Beratung zu geben.

Geräteverlust muss nicht zum Verlust des Bestands führen, wenn die Wiederherstellung vollständig möglich ist. Ein verlorenes Backup ist dagegen ein dringendes Problem, auch wenn dein Gerät noch funktioniert. Vernichte deinen letzten Zugang nicht durch einen unüberlegten Reset.

Deine kurze Prüfliste

- Ich kann erklären, wer bei meiner gewählten Lösung die privaten Schlüssel kontrolliert.
- Ich kenne den Unterschied zwischen PIN, Wiederherstellungswörtern und einer optionalen Passphrase.
- Meine Sicherung ist vollständig, geschützt und mit dem vorgesehenen Verfahren geprüft.

- Ich habe Empfänger, Netzwerk, Betrag und Gebühren vor jeder Zahlung kontrolliert.
- Ich verstehe, was ich beim Anbieter erwerbe und wie eine Auszahlung funktioniert.
- Ich rechne nicht mit garantierten Kursgewinnen oder festen Erträgen.
- Ich habe auch Krankheit, Geräteverlust und Nachlass bedacht.

Wenn du einen dieser Punkte noch nicht erklären kannst, vertiefe zuerst das entsprechende Kapitel. Es besteht kein Zeitdruck, Bitcoin zu kaufen oder eine komplexe Verwahrung einzurichten.

Vertiefende Begleitung durch Swissration

Dieser kostenlose Leitfaden vermittelt die wesentlichen Grundlagen einschliesslich der Sicherheitsregeln. In einer separaten kostenpflichtigen Beratung können wir deine Ausgangssituation, geeignete Anbieter, Gebühren, Hardware-Wallets und ein persönliches Sicherheitskonzept vertiefen. Auch die Begleitung praktischer Schritte und die Überprüfung einer bestehenden Verwahrung können dazugehören.

Du behältst dabei die Kontrolle über deine Geheimnisse. Informationen zum Vorsorgeangebot findest du auf swissration.ch. Der Leitfaden und eine allgemeine Beratung ersetzen keine bei Bedarf notwendige persönliche Finanz-, Steuer- oder Rechtsberatung.

Glossar

Adresse: Empfangsinformation für eine Bitcoin-Zahlung. Sie legt technisch fest, unter welchen Bedingungen der empfangene Betrag später ausgegeben werden kann.

Backup: Sicherung der Informationen, die für die Wiederherstellung notwendig sind. Bei vielen Wallets umfasst sie eine geordnete Wortliste, bei anderen zusätzliche Daten.

Bestätigung: Aufnahme einer Transaktion in einen akzeptierten Block sowie jeder folgende Block, der darauf aufbaut.

Bitcoin und BTC: Bitcoin bezeichnet das Netzwerk und seine digitale Werteinheit. BTC ist die übliche Abkürzung der Einheit.

Block: Paket von Transaktionen und technischen Angaben, das die Regeln des Netzwerks erfüllen muss.

Blockchain: Geordnete Kette von Blöcken. Neue Blöcke verweisen auf ihre Vorgänger.

Broker: Dienstleister, über den du einen Kauf oder Verkauf abwickeln kannst. Preisstellung und Verwahrung hängen vom Angebot ab.

Cold Storage: Schutz der privaten Schlüssel ausserhalb einer gewöhnlichen internetverbundenen Umgebung.

Dezentralität: Verteilung von Prüfung und Kontrolle auf verschiedene Teilnehmer. Sie schliesst Konzentration in Teilbereichen nicht aus.

Deflation: Anhaltender Rückgang des allgemeinen Preisniveaus. Einzelne günstigere Produkte sind noch keine allgemeine Deflation.

Digitale Signatur: Mathematisch überprüfbare Freigabe mit einem privaten Schlüssel, ohne diesen zu veröffentlichen.

Diversifikation: Verteilung von Vermögen auf unterschiedliche Anlagen und Risiken. Sie garantiert keinen Schutz vor Verlusten.

Doppelausgabe: Versuch, denselben bereits verfügbaren Bitcoin-Betrag in konkurrierenden Zahlungen mehrmals zu verwenden.

Eigenverwahrung: Du kontrollierst die zur Freigabe nötigen Schlüssel und organisierst die Sicherung selbst.

Fiatgeld: Staatlich geprägte Geldordnung ohne festen Einlösungsanspruch in eine vorgegebene Menge eines Rohstoffs wie Gold. Der Franken gehört dazu.

Fork: Verzweigung in der Blockgeschichte oder Aufspaltung aufgrund unterschiedlicher Regeln. Nicht jede vorübergehende Verzweigung schafft ein eigenständiges dauerhaftes Netzwerk.

Fremdverwahrung: Ein Anbieter kontrolliert die Schlüssel und führt die Bestände nach seinen Verfahren und Verträgen.

Full Node: Computer mit Software, die Transaktionen und Blöcke selbstständig vollständig nach den gewählten Bitcoin-Regeln prüft.

Halving: Halbierung der neu geschaffenen Bitcoin pro Block nach jeweils 210’000 Blöcken im Hauptnetz.

Hardware Wallet: Spezialgerät zur geschützten Verwaltung von Schlüsseln und zur Signierung von Transaktionen.

Hash: Rechnerisch erzeugter digitaler Fingerabdruck von Daten. Er dient unter anderem zur Verknüpfung der Blöcke.

Hot Wallet: Wallet, deren Schlüssel in einer gewöhnlichen internetverbundenen Umgebung verwendet werden.

Inflation: Anstieg des allgemeinen Preisniveaus und damit sinkende Kaufkraft der betreffenden Geldeinheit, wenn man einen unveränderten Geldbetrag betrachtet.

Konsensregeln: Regeln, nach denen Teilnehmer beurteilen, ob eine Transaktion oder ein Block gültig ist.

Kryptografie: Mathematische Verfahren zum Schutz und zur Überprüfung von Informationen, beispielsweise für digitale Signaturen.

KYC: Identitätsprüfung eines Kunden. Die englische Abkürzung steht für «Know Your Customer».

Lightning: Zusätzliches Zahlungsnetz auf Basis von Bitcoin, das Zahlungen über miteinander verbundene Kanäle ermöglicht.

Liquidität: Je nach Zusammenhang die Verfügbarkeit von Zahlungsmitteln oder die Möglichkeit, einen Vermögenswert ohne starke Preiswirkung zu handeln. Bei Lightning ist auch verfügbare Kanalkapazität gemeint.

Mempool: Lokaler vorläufiger Speicher eines Netzwerkknotens für gültige, noch nicht bestätigte Transaktionen.

Mining: Wettbewerb um gültige Arbeitsnachweise für neue Blöcke. Miner erhalten nach den Regeln neue Bitcoin und Transaktionsgebühren.

Mining Pool: Zusammenschluss von Minern zur gemeinsamen Organisation der Arbeit und Verteilung der Einnahmen.

Multisig: Verfahren, bei dem mehrere Signaturen erforderlich sind, etwa zwei von drei möglichen Schlüsseln.

Netzwerkgebühr: Betrag, der bei einer On-Chain-Transaktion als Vergütung an den Miner des aufnehmenden Blocks geht. Anbieter können daneben eigene Gebühren erheben.

Öffentlicher Schlüssel: Aus einem privaten Schlüssel ableitbare Information, mit der sich unter anderem Signaturen prüfen lassen. Er ist nicht mit jeder Empfangsadresse identisch.

On Chain: Direkt auf der Bitcoin-Blockchain verarbeitet.

Open Source: Öffentlich einsehbarer Quellcode, der nach den jeweiligen Lizenzbedingungen geprüft, verwendet und verändert werden kann.

Passphrase: Optionale zusätzliche Zeichenfolge für die Ableitung einer Wallet. Sie ist von Geräte-PIN und Wörter-Backup zu unterscheiden.

Peer to Peer: Direkte Kommunikation zwischen Netzwerkteilnehmern ohne eine notwendige zentrale Vermittlungsstelle für jede Verbindung.

Phishing: Täuschung, mit der Angreifer dich zur Preisgabe von Daten oder zur Freigabe einer Handlung bewegen möchten.

PIN: Persönliche Nummer zur Entsperrung eines Geräts oder Zugangs. Sie ersetzt normalerweise kein Wiederherstellungs-Backup.

Privater Schlüssel: Geheime Zahl zur Erfüllung bestimmter Ausgabebedingungen, insbesondere durch digitale Signaturen.

Proof of Work: Arbeitsnachweis durch Rechenaufwand, der zur Absicherung der Blockgeschichte beiträgt.

QR Code: Maschinenlesbares Bild, das Zahlungsinformationen enthalten kann. Es ist kein Beweis für einen vertrauenswürdigen Empfänger.

Reorganisation: Wechsel zu einer konkurrierenden gültigen Blockgeschichte mit mehr kumulierter Arbeit. Dabei können bisherige Bestätigungen entfallen.

Satoshi: Kleinste Einheit auf der Bitcoin-Hauptkette. 100’000’000 Satoshi entsprechen 1 BTC.

Seed Phrase: Verbreitete Bezeichnung für eine geordnete Wortliste zur Wallet-Wiederherstellung. Wallet-Typ und gegebenenfalls Zusatzdaten bleiben zu beachten.

Spread: Unterschied zwischen Kauf- und Verkaufspreis; je nach Angebot kann darin ein Kostenaufschlag enthalten sein.

Transaktion: Technischer Auftrag, der vorhandene Bitcoin-Beträge verwendet und neue Ausgabebedingungen festlegt.

Transaktionskennung: Technische Kennung einer Transaktion, häufig TXID genannt. Sie hilft beim Nachverfolgen des Status.

UTXO: Noch nicht ausgegebener Transaktionsausgang, also ein verfügbarer Betrag mit bestimmten Ausgabebedingungen.

Volatilität: Ausmass der Preisschwankungen. Hohe Volatilität bedeutet, dass sich der Preis stark verändern kann.

Wallet: Software oder eine Kombination aus Software und Gerät zur Verwaltung von Empfang, Bestand und Zahlungen.

Whitepaper: Technisches Konzeptpapier. Das Bitcoin-Whitepaper wurde 2008 unter dem Namen Satoshi Nakamoto veröffentlicht.

Quellen und weiterführende Informationen

Die folgenden Quellen dienen zur Überprüfung und Vertiefung. Die technischen Dokumentationen richten sich teilweise an Fachleute. Du musst sie nicht vollständig lesen, um diesen Leitfaden zu verstehen. Quellenstand und Abrufdatum dieser Ausgabe: 21. Oktober 2026.

Bitcoin.org ist ein Informationsangebot aus dem Bitcoin-Umfeld und keine zentrale Behörde des Netzwerks. Bitcoin Core ist ein wichtiges Softwareprojekt. Herstelleranleitungen beschreiben konkrete Produkte und sind keine unabhängigen Kaufempfehlungen. Bei rechtlichen oder steuerlichen Fragen sind aktuelle amtliche Informationen und deine persönliche Situation massgeblich.

Technische und historische Grundlagen

[Q1] Satoshi Nakamoto: Bitcoin A Peer-to-Peer Electronic Cash System, 2008. Originales Whitepaper; Entwurf gegen Doppelausgaben und Grundprinzip des Arbeitsnachweises. Bezug: Kapitel 1 bis 3.

https://bitcoin.org/bitcoin.pdf

[Q2] Bitcoin Developer Guide: Block Chain. Blockverknüpfung, Prüfung und Auswahl gültiger Ketten. Bezug: Kapitel 2 und 3.

https://developer.bitcoin.org/devguide/block_chain.html

[Q3] Bitcoin Developer Guide: Transactions. Transaktionsausgänge, Ausgabebedingungen und Signaturen. Bezug: Kapitel 2, 3 und 9.

https://developer.bitcoin.org/devguide/transactions.html

[Q4] Bitcoin Developer Guide: Wallets. Schlüsselverwaltung, Wallet-Funktionen und technische Arbeitsweise. Bezug: Kapitel 3, 4 und 9.

https://developer.bitcoin.org/devguide/wallets.html

[Q5] Bitcoin Improvement Proposal 39. Verbreitetes Verfahren für Wiederherstellungswörter und zusätzliche Passphrase. Nicht alle Wallets verwenden dieses Verfahren. Bezug: Kapitel 9.

https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[Q6] Bitcoin.org: Securing your wallet. Grundsätze zu Sicherungen, Offline-Verwahrung und Nachlass. Bezug: Kapitel 9.

https://bitcoin.org/en/secure-your-wallet

[Q7] Bitcoin Core: validation.cpp. Technische Umsetzung der Blocksubvention, insbesondere GetBlockSubsidy. Bezug: Kapitel 6.

https://github.com/bitcoin/bitcoin/blob/master/src/validation.cpp

[Q8] Bitcoin Core: chainparams.cpp. Parameter des Hauptnetzes, Genesisblock, Halbierungsintervall und Zielzeiten. Bezug: Kapitel 1, 3 und 6.

https://github.com/bitcoin/bitcoin/blob/master/src/kernel/chainparams.cpp

[Q9] Bitcoin.org: Frequently Asked Questions. Überblick zu Funktionsweise, Kontrolle und Grenzen; als Quelle aus dem Bitcoin-Umfeld einzuordnen. Bezug: Kapitel 4 und 11.

https://bitcoin.org/en/faq

Geldpolitik und Zahlungspraxis

[Q10] Schweizerische Nationalbank: Die geldpolitische Strategie der SNB. Auftrag, Definition der Preisstabilität und geldpolitischer Rahmen. Bezug: Kapitel 1 und 8.

https://www.snb.ch/de/the-snb/mandates-goals/monetary-policy/strategy

[Q11] Joseph Poon und Thaddeus Dryja: The Bitcoin Lightning Network, 2016. Ursprünglicher technischer Entwurf zu Zahlungskanälen. Konkrete Wallets können weiterentwickelte Verfahren einsetzen. Bezug: Kapitel 7.

https://lightning.network/lightning-network-paper.pdf

[Q12] Lightning Labs: The Lightning Network Overview. Technische Dokumentation zu Zahlungskanälen, Weiterleitung und Liquidität. Ergänzung zu Kapitel 7.

https://docs.lightning.engineering/the-lightning-network/overview

[Q13] Bitcoin.org: Protect your privacy. Öffentliche Transaktionsdaten, Verknüpfbarkeit und Adresswiederverwendung. Bezug: Kapitel 5 und 9.

https://bitcoin.org/en/protect-your-privacy

[Q14] Lugano Plan ₿: Pay in Crypto. Offizielle Projektübersicht zu teilnehmenden Geschäften und angebotenen Zahlungswegen. Teilnahme und Bedingungen können sich ändern. Bezug: Kapitel 7.

https://planb.lugano.ch/pay-in-crypto/

Sicherheit und Schweiz

[Q15] Trezor: Check wallet backup on Trezor Safe 5. Herstellerbeispiel für die Prüfung einer Sicherung ohne Löschen der Wallet. Keine Geräteempfehlung; andere Modelle erfordern andere Anleitungen. Bezug: Kapitel 9.

https://trezor.io/guides/backups-recovery/general-standards/check-backup-on-trezor-safe-5

[Q16] Bitcoin Improvement Proposal 11: M-of-N Standard Transactions. Technische Grundlage von Ausgabebedingungen mit mehreren Signaturen. Bezug: Kapitel 9.

https://bitcoin.org/bip/11/

[Q17] FINMA: Warnungen der FINMA. Amtlicher Zugang zu Warnlisten und Informationen über möglicherweise problematische Marktteilnehmer. Ein fehlender Eintrag bedeutet keine Unbedenklichkeit. Bezug: Kapitel 10 und 12.

https://www.finma.ch/de/finma-public/warnungen/

[Q18] Eidgenössische Steuerverwaltung: Kryptowährungen Besteuerung. Amtliche steuerliche Einordnung von Zahlungs-Token, Privat- und Geschäftsvermögen. Bezug: Kapitel 10.

https://www.estv.admin.ch/de/kryptowaehrungen-besteuerung

[Q19] Schweizerische Nationalbank: Wie Geld durch die Zentralbank und das Bankensystem geschaffen wird, 16. Januar 2018. Erläuterung der Geldschöpfung und ihrer Grenzen. Bezug: Kapitel 1.

https://www.snb.ch/de/publications/communication/speeches/2018/ref_20180116_tjn

Goldbestände, Reserven und Echtheitsprüfung

[Q20] World Gold Council: How Much Gold Has Been Mined? Schätzungen historischer Förderung, oberirdischer Bestände und unterirdischer Reserven. Bezug: Kapitel 6.

https://www.gold.org/goldhub/data/how-much-gold

[Q21] United States Geological Survey: Mineral Commodity Summaries 2026, Appendixes, Appendix C. Abgrenzung von Ressourcen und wirtschaftlich förderbaren Reserven. Bezug: Kapitel 6.

https://pubs.usgs.gov/periodicals/mcs2026/mcs2026-appendixes.pdf

[Q22] Lauren Moïse, LBMA Alchemist, Ausgabe 117: The Silent Risk: Counterfeiting in Precious Metals. Fälschungen, Kennzeichnungen und Prüfung. Bezug: Kapitel 6.

https://www.lbma.org.uk/alchemist/issue-117/the-silent-risk-counterfeiting-in-precious-metals

Veröffentlichung und Sicherheit

Die technischen Erläuterungen sind für Einsteiger vereinfacht. Wo ein Alltagsvergleich Grenzen hat, werden diese benannt. Beispiele mit Frankenbeträgen dienen nur dem Verständnis. Aussagen über eine mögliche künftige Nutzung oder Wertentwicklung sind keine Zusicherungen.

Swissration · Kostenloser Bitcoin-Einsteigerleitfaden · Ausgabe 2.1

Stand: 21. Oktober 2026 · swissration.ch