Bitcoin

Bitcoin (BTC) ist eine dezentrale **Peer-to-Peer Kryptowährung**, die ihren Wert ohne Deckung und ohne zentralen Emittenten aufrechterhält. Transaktionen werden von den Teilnehmern eines **global verteilten Netzwerks** bestätigt und in der Blockchain fälschungssicher dokumentiert. Die Funktionsfähigkeit des Systems beruht auf kryptografisch gesicherten Protokollmechanismen und dem **dezentralen Konsens der Netzwerkteilnehmer**. Eine institutionelle Steuerung findet nicht statt.

Die Verwaltung von Bitcoin erfolgt über eine **Wallet**. Diese kann als sog. **Hot Wallet** durch die Nutzung einer lokal ausgeführten Wallet-Software auf einem internetfähigen Endgerät erstmalig erzeugt werden. Dabei wird im Rahmen der Einrichtung eine **Seed Phrase** (12-24 Wörter) generiert, aus der anschließend die für die Verfügung über Bitcoin erforderlichen Schlüssel abgeleitet werden.

Für ein höheres Sicherheitsniveau kann eine Wallet als sog. **Cold Wallet** über ein separates **Hardware-Gerät** (z. B. BitBox, Ledger oder Trezor) angelegt werden. Im Rahmen dieses Vorgangs wird die Seed Phrase innerhalb des Hardware-Geräts erzeugt und dort angezeigt.

Aus der Seed Phrase wird mathematisch ein privater Schlüssel (Private Key) abgeleitet, aus dem durch kryptografische Berechnung ein öffentlicher Schlüssel (Public Key) und daraus anschließend die Bitcoin-Adresse erzeugt werden.

Eine Seed Phrase besteht aus **12 bis 24 Wörtern** und dient als menschenlesbare Sicherungsform der zugrunde liegenden Zugangsdaten. Sie ermöglicht es, die Wallet einschließlich aller zugehörigen Schlüssel und Adressen auf einem anderen Endgerät oder auf einer Hardware-Wallet wiederherzustellen **(Backup)**.

Sie ist damit der maßgebliche Sicherungs- und Wiederherstellungsmechanismus der Schlüsselstruktur der Wallet und der darüber kontrollierten Bitcoin-Bestände.

Obwohl Wallets häufig als „digitale Geldbörsen“ bezeichnet werden, werden Kryptowährungen nicht in der Wallet gespeichert, sondern auf der Blockchain. Wallets verwalten die **privaten Schlüssel (Private Key)**, die das **digitale Signieren von**

Transaktionen und damit die Übertragung von Bitcoin ermöglichen. Die Signatur weist gegenüber dem Netzwerk nach, dass der Inhaber der Schlüssel zur Verfügung über die zugehörigen Bitcoin berechtigt ist.

Im Netzwerk sichtbar ist die **Bitcoin-Adresse**, die dem **Empfang von Bitcoin** dient, ohne hierdurch Zugriff auf die zugehörigen Bestände zu vermitteln. Sie kann öffentlich **ohne Sicherheitsrisiko** geteilt werden. Die Bitcoin-Adresse wird aus dem Public Key abgeleitet. Der **Public Key** dient der **Verifikation digitaler Signaturen** und ermöglicht dem Netzwerk die Prüfung, ob eine Transaktion mit dem zugehörigen Private Key autorisiert wurde.

Bei sog. **Custodial Services** (z. B. Trade Republic, Coinbase) liegt der Private Key beim Verwahrer und nicht beim Nutzer. Nutzer solcher Dienste halten keine "eigenen" Bitcoin auf der Blockchain, sondern lediglich schuldrechtliche Ansprüche gegenüber dem Anbieter (z. B. über Sammelverwahrung oder derivative Abbildungen wie ETNs).

Die Kontrolle über Bitcoin folgt allein aus der Kontrolle über die privaten Schlüssel **(„Not your keys, not your coins")** und ist damit maßgeblich für die wirtschaftliche Zuordnung und die faktische Verfügungsmacht.

Konsens im dezentralen Netzwerk

Wird eine Transaktion initiiert, erzeugt die Wallet-Software eine protokollkonforme Transaktion und signiert sie mit dem Private Key des Absenders. Die signierte Transaktion wird anschließend an die mit der Wallet **verbundene Node** übermittelt. Die empfangende Node überprüft automatisiert die Regelkonformität der Transaktion. Ist die Transaktion regelkonform, wird sie im sogenannten **Mempool** gespeichert – einer lokalen Warteliste für gültige, aber noch nicht bestätigte Transaktionen – und an verbundene Peers im Netzwerk weitergeleitet.

Diese prüfen die Transaktion erneut eigenständig und verbreiten sie weiter, sodass sie sich innerhalb kurzer Zeit im gesamten Peer-to-Peer-Netzwerk ausbreitet.

Miner durchsuchen ihren lokalen Mempool, der gültige, aber noch unbestätigte Transaktionen enthält, und wählen daraus – in der Regel nach wirtschaftlichen Kriterien wie der Höhe der Transaktionsgebühren – diejenigen aus, die sie in den nächsten Block aufnehmen möchten. Aus diesen Transaktionen erstellen sie einen vollständigen Blockentwurf („Blockkandidat“), der bereits alle notwendigen Bestandteile enthält, jedoch erst durch einen erfolgreichen **Proof of Work** zu einem gültigen Block wird. Dieser Block enthält neben den Transaktionen auch einen Verweis auf den vorherigen Block der bestehenden Blockchain.

Im Proof-of-Work-System konkurrieren Miner darum, den nächsten Block zur Blockchain hinzuzufügen. Technisch besteht ihre Aufgabe darin, durch wiederholte Berechnung einen Hash zu erzeugen, der den vom Protokoll vorgegebenen Schwierigkeitsanforderungen entspricht. Die Wahrscheinlichkeit, einen gültigen Hash zu finden ist proportional zur eingesetzten Rechenleistung.

Wird schließlich ein **Hash** erzeugt, gilt der Block als gültig erzeugt. Dieser Hash fungiert als Arbeitsnachweis: Er belegt, dass messbarer Rechenaufwand betrieben wurde. Der Block wird anschließend an das Netzwerk übermittelt und von den Nodes überprüft. Die Nodes prüfen erneut, ob der Arbeitsnachweis korrekt ist, alle enthaltenen Transaktionen weiterhin gültig sind und der Block ordnungsgemäß an den vorherigen Block anknüpft. Wird der Block akzeptiert, wird er an die bestehende Blockchain angehängt. Die darin enthaltenen Transaktionen gelten ab diesem Zeitpunkt als bestätigt.

Kommentiert [Y1]: Definition sinnvoll? zB Ein Hash ist ein mathematischer Fingerabdruck von Daten, der zur Verkettung von Blöcken und zur Sicherung der Integrität der Blockchain verwendet wird.

Da jeder neue Block den Hash seines Vorgängers enthält, entsteht eine fortlaufende Verkettung von Blöcken. Im Netzwerk gilt diejenige Blockkette als maßgeblich, die die größte kumulierte Rechenarbeit aufweist. Auf diese Weise bildet sich eine einheitliche, verbindliche Blockchain, auf die sich alle Teilnehmer des Netzwerks einigen.

FAQ

Kann Bitcoin verboten oder abgeschaltet werden?

Bitcoin kann technisch nicht abgeschaltet werden, da das Netzwerk dezentral und weltweit betrieben wird. Staaten können jedoch den Zugang regulieren, etwa durch Vorgaben für Börsen, Banken und Dienstleister. Das betrifft die Nutzung und den Handel, nicht aber das Bitcoin-Netzwerk selbst.

Was passiert bei Verlust der Seed Phrase?

Geht die Seed Phrase verloren, ist der **Zugriff auf die zugehörigen Bitcoin dauerhaft nicht mehr möglich**. Es existiert keine zentrale Stelle, die den Zugang wiederherstellen oder zurücksetzen kann. Bitcoin bleiben zwar technisch in der Blockchain bestehen, können jedoch **nicht mehr bewegt oder genutzt werden** und gelten wirtschaftlich als verloren. Eine rechtliche oder technische Wiederherstellung ist faktisch nicht möglich.

X-Account-Beitrag:

1. **Ist Bitcoin anonym?**

Nein. Bitcoin ist nicht anonym, sondern pseudonym. Transaktionen sind dauerhaft öffentlich in der Blockchain einsehbar und einzelnen Bitcoin-Adressen zugeordnet. Diese Adressen sind nicht direkt mit Klarnamen verknüpft, können jedoch durch Auswertung von Transaktionsdaten und zusätzlichen Informationen (z. B. von Krypto-Plattformen) einer Person zugeordnet werden.

2. **Umwandlung Hot Wallet in Cold Wallet/ Wiederherstellung der Wallet**

alternativ kann eine bestehende Seed Phrase zur Wiederherstellung importiert werden

3. Costudial Service – Coinbase AGB??

Fragen

- Gewerbliche Tätigkeit / Betriebsvermögen (bitte bei den ersten zwei nur eins ankreuzen!)
- Privatvermögen

Blog-Beitrag: Ist BTC eine Sache?

Kampf gegen Fake-News: BAG

Für die Transaktion von einem Wallet auf ein anderes Wallet werden zwei Schlüssel benötigt. Der eine ist ein öffentlicher Schlüssel (sog. Public Key), der mit einer E-Mail-Adresse bzw. mit einer Kontonummer vergleichbar ist. Bei dem anderen handelt es sich um einen privaten Schlüssel (sog. Private Key), vergleichbar mit einem Passwort, der es dem Inhaber des Wallets ermöglicht, über das zu seinen Gunsten bestehende Guthaben zu verfügen *(vgl. Höring DStZ 2022, 520, 521)*. Zur Übertragung nimmt der Übertragende Bezug auf eine frühere, seinem Wallet gutgeschriebene Transaktion von Zähleinheiten der Kryptowährung in mindestens der zu übertragenden Anzahl und gibt den Public Key des Empfängers an. Anschließend signiert der Übertragende die Transaktion mit seinem Private Key und überträgt die Transaktion an das Netzwerk *(vgl. BMF-Schreiben vom 6. März 2025 Rn. 18, 21, BStBl. I S. 658; OLG Braunschweig 18. September 2024 – 1 Ws 185/24 – zu II 3 a cc (1) der Gründe; Bachert CR 2021, 356 f.)*.

Das Netzwerk überprüft anhand der übermittelten Daten unter Verwendung eines Konsensmechanismus, ob das anweisende Wallet ausreichend Zähleinheiten der Kryptowährung enthält und die Transaktion tatsächlich mit

dem entsprechenden Private Key signiert wurde. Ist das der Fall, wird die Transaktion akzeptiert und in das „digitale Kassenbuch“ (sog. Ledger) der Kryptowährung eingetragen *(vgl. BMF-Schreiben vom 6. März 2025 Rn. 21, BStBl. I S. 658; vgl. zu Bitcoin Ammann CR 2018, 379)*.