Wie Bitcoin über die Blockchain funktioniert

Grundlagen der Blockchain

- Die **Blockchain** ist ein digitales, dezentrales Kassenbuch (Ledger).
- Alle Transaktionen werden dort chronologisch in Blöcken gespeichert.
- Jeder neue Block enthält eine Referenz auf den vorherigen Block, wodurch eine lange, unveränderliche Kette entsteht.

Dezentralität

1. Das Bitcoin-Netzwerk besteht aus vielen tausend Rechnern (sogenannten „Nodes“) rund um den Globus.
2. Diese Nodes besitzen jeweils eine vollständige Kopie der gesamten Blockchain.
3. Es gibt keine zentrale Instanz oder Behörde, die das Netzwerk steuert. Entscheidungen und Updates werden über einen Konsensmechanismus getroffen, an dem sich alle beteiligten Nodes orientieren.

Konsensmechanismus: Proof of Work

1. Damit ein neuer Block der Blockchain hinzugefügt werden kann, müssen sogenannte **Miner** einen mathematischen Rätsel-Prozess lösen.
2. Dieser Prozess wird als **Proof of Work** bezeichnet und erfordert Rechenleistung sowie elektrische Energie.
3. Ist der richtige Lösungswert gefunden, darf der Miner den neuen Block an die Kette anhängen und erhält dafür eine Belohnung in Bitcoin.
4. Da die Lösung nicht erraten, sondern errechnet werden muss, ist es extrem aufwendig, die Blockchain nachträglich zu manipulieren.

Unveränderlichkeit (Immutability)

1. Jeder Block verweist mittels einer kryptografischen Prüfsumme (Hash) auf den vorherigen Block.
2. Wenn jemand versuchen würde, eine alte Transaktion zu ändern, müsste auch der Hash dieses Blocks und aller nachfolgenden Blöcke neu berechnet werden.
3. Aufgrund der großen Rechnerzahl im Netzwerk und der benötigten Rechenleistung ist dies praktisch unmöglich.
4. Das macht die Blockchain extrem widerstandsfähig gegen Manipulationen.

Kryptografische Sicherheit

1. Transaktionen sind mit privaten und öffentlichen Schlüsseln gesichert.
2. Nutzer besitzen einen privaten Schlüssel (wie ein geheimes Passwort), mit dem sie ihre Bitcoin-

Transaktionen signieren.
3. Nur mit dem richtigen privaten Schlüssel lassen sich Bitcoin bewegen, ein Kopieren der Wallet ist damit zwecklos, sofern der Schlüssel geheim bleibt.
4. Die Blockchain selbst wird durch komplexe kryptografische Verfahren geschützt, die sicherstellen, dass nur gültige, von der Gemeinschaft bestätigte Transaktionen eingefügt werden.

Warum macht das Bitcoin sicher?

1. **Dezentralität**: Da kein einzelner Server ausschlaggebend ist, kann das Netzwerk nicht durch den Ausfall oder die Übernahme eines Einzelnen lahmgelegt oder manipuliert werden.
2. **Kryptografie**: Nur wer den richtigen privaten Schlüssel besitzt, kann über die zugehörigen Bitcoin verfügen.
3. **Transparenz**: Alle Transaktionen sind öffentlich einsehbar, was Betrug oder Fälschungen extrem erschwert.
4. **Hohe Kosten für Angriffe**: Das Ändern oder Manipulieren von Blöcken würde enorme Rechen- und Energiekosten verursachen. Die finanzielle Hürde ist so hoch, dass es sich für potenzielle Angreifer schlicht nicht lohnt.