So funktioniert eine Transaktion mit und ohne Blockchain-Technologie

Anton und Anna möchten eine Transaktion an Kim veranlassen

Anton

Anna

ohne Blockchain

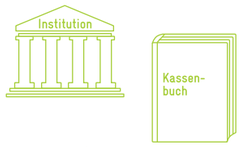
Anton sendet den Auftrag an eine zentrale Institution, z.B. eine Bank.

mit Blockchain

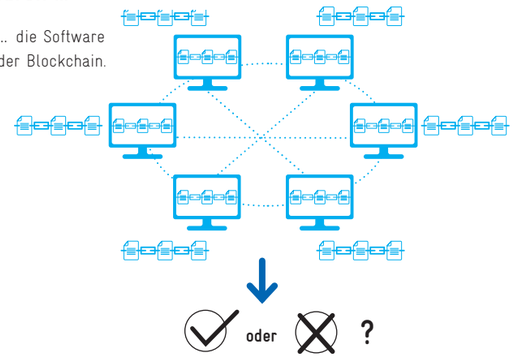
Anna sendet den Auftrag an ein Blockchain-Netzwerk.

Ob die Transaktion zulässig ist, wird geprüft durch ...

... die zentrale Institution anhand ihres zentral geführten Kassenbuchs.



... die Software der Blockchain.



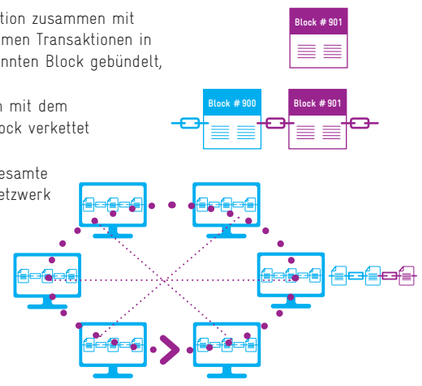
Falls die Transaktion zulässig ist, wird ...

... dem zentralen Kassenbuch ein Eintrag hinzugefügt.

... die Transaktion zusammen mit anderen legitimen Transaktionen in einem sogenannten Block gebündelt,

kryptografisch mit dem vorherigen Block verkettet

und an das gesamte Blockchain-Netzwerk kommuniziert.



Um zu überprüfen, ob die Transaktion ausgeführt wurde, ...

... können Anton und Kim bei der zentralen Institution nachfragen.

... können Anna und Kim in der Blockchain nachsehen.

Ablauf der Transaktionen

Anton und Anna einigen sich jeweils mit Kim auf ein Geschäft, für das Kim 50 Euro bekommt. Anna führt die Transaktion über eine Blockchain aus, Anton über eine zentrale Instanz wie eine Bank.

Anton beauftragt die Bank, 50 Euro an Kim zu überweisen. Die Bank prüft anhand ihres zentralen Kassenbuchs, ob die Transaktion zulässig ist. Anna sendet den Wert von 50 Euro über die Blockchain. Dort überprüfen Teilnehmende des Netzwerks, ob die Transaktion zulässig ist.

Die Bank führt Antons Transaktion aus, belastet Antons Konto mit 50 Euro und schreibt Kim 50 Euro gut. Diese Transaktion wird im Kassenbuch verbucht. Annas Transaktion wird mit anderen Transaktionen in einem Block zusammengefasst, erhält einen digitalen Fingerabdruck, den sogenannten Hash, und wird dann an das gesamte Blockchain-Netzwerk kommuniziert. Der neue Block wird mit dem vorherigen Block verkettet, indem auf den Hash des Vorgängers verwiesen wird.

Um die Transaktion mit Anton zu prüfen, kann Kim in ihrem Bankkonto nachsehen. Um die Transaktion mit Anna zu prüfen, kann Kim den Block mit ihrer Transaktion einsehen.

Unterschiede zwischen den Transaktionen

Bei Transaktionen ohne Blockchain-Technologie muss man darauf vertrauen, dass die zentrale Institution die Transaktion verlässlich durchführt, Daten sicher verwahrt und nur für Zwecke verwendet, denen zugestimmt wurde. Für diese Dienste fallen mitunter hohe Gebühren an. Bei der Verwendung von Blockchain-Technologien muss man darauf vertrauen, dass die Technik der Blockchain einwandfrei funktioniert.

Bei Blockchain-Technologien ist klar festgelegt und einsehbar, welche Transaktionen zulässig sind. Bei Transaktionen ohne Blockchain-Technologie müssen die Nutzungsbedingungen der zentralen Institution interpretiert werden, um zu verstehen, welche Transaktionen legitim sind. Die zentrale Institution kann diese Bedingungen aber anders interpretieren und einseitig ändern.

Die Computer des Blockchain-Netzwerks müssen einen Konsens bilden. Die dafür nötigen Konsensmechanismen können aber, wie im Fall der Bitcoin-Blockchain, sehr viel Energie verbrauchen.

In einer Blockchain gespeicherte Transaktionen können später praktisch nicht verändert werden. Eine zentrale Institution hat dagegen die Möglichkeit, Transaktionen zu ändern oder zu löschen. Zudem kann ein erfolgreicher Cyberangriff auf eine zentrale Institution dazu führen, dass ihre Dienste nicht verfügbar sind. In einer Blockchain ist das Kassenbuch auf vielen verschiedenen Computern gespeichert, sodass die Daten auch dann verfügbar sind, wenn einige Computer ausfallen.

Das Speichern einer Transaktion in einem zentralen Kassenbuch ist schnell und benötigt wenig Ressourcen. Das Speichern einer Transaktion in einer Blockchain benötigt mehr Ressourcen, weil die Transaktion an alle Computer im Netzwerk gesendet und von ihnen gespeichert wird. Hieraus entsteht u.a. ein höherer Speicherbedarf.

Um den aktuellen Stand gespeicherter Transaktionen zu erfahren, muss erst eine Anfrage an die zentrale Institution gestellt werden. Die in einer Blockchain gespeicherten Transaktionen sind für die Teilnehmenden der Blockchain direkt einsehbar.

Neben Transaktionen speichert eine zentrale Institution auch Daten ihrer Nutzerinnen und Nutzer wie Namen, Passwörter oder Kreditkartendaten. Zwar treffen diese Institutionen Vorkehrungen gegen Datendiebstahl, aber diverse Hacks zeigen, dass diese Vorkehrungen keine vollständige Sicherheit bieten.

Glossar:

Ein **Kassenbuch** erfasst und speichert (unter Umständen digital) Transaktionen. **Transaktionen** sind eine Abfolge von Schritten, die eine logische Einheit bilden. Sie können dabei ganz unterschiedliche Dinge umfassen: das Überweisen von Geld von einer Person an eine andere, aber auch Posts in sozialen Medien oder das Teilen von Informationen zwischen Unternehmen oder Behörden.

Eine **zentrale Institution** führt das Kassenbuch. Die zentrale Institution besitzt dabei die alleinige Kontrolle über das Erfassen und Speichern von Transaktionen. Beispiele sind Banken, Rechtsbeistände oder soziale Medien.

Ein **Netzwerk** besteht aus Computern, die miteinander verbunden sind und so Informationen austauschen können.

Eine **Blockchain** ist ein digitales Kassenbuch, das gleichzeitig auf vielen verschiedenen Computern gespeichert wird. Eine Blockchain besteht aus miteinander verketteten Blöcken.

Blöcke bündeln Transaktionen ähnlich wie auf einer Seite in einem Kassenbuch. Zusätzlich enthält jeder Block Informationen, um ihn unveränderbar mit dem vorherigen Block zu verbinden. Unveränderbar sind dabei sowohl die Transaktionen innerhalb eines Blocks als auch die Reihenfolge der Blöcke.

Konsens beschreibt eine Situation, in der sich alle Computer in Bezug auf den korrekten Stand der Blockchain und der in ihr gespeicherten Transaktionen einig sind.

Konsensmechanismen stellen sicher, dass Konsens zwischen den Computern hergestellt wird, selbst dann, wenn es Computer gibt, die das Netzwerk beispielsweise durch das Versenden falscher Informationen stören wollen.