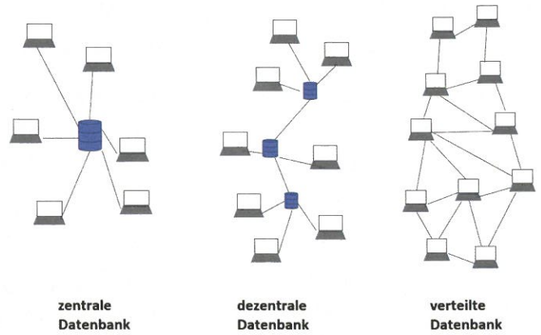
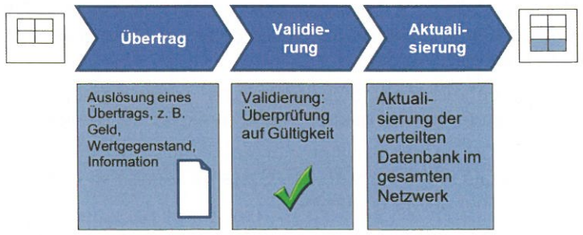
1.3.5 Distributed-Ledger-Technologie (DLT)

1.3.5.1 Grundlagen

Als Distributed Ledger (verteiltes Kontenbuch) wird eine verteilte Datenbank bezeichnet. In einer verteilten Datenbank sind die Daten auf jedem teilnehmenden Rechner im weltweiten Netz gespeichert.



Neue Datensätze können von jedem Teilnehmer selbst hinzugefügt werden, jeder Teilnehmer hat Schreibrechte, z. B. für die Bestätigung eines Wertübertrages. Ein anschließender Aktualisierungsvorgang stellt allen Teilnehmern den aktuellen Datenbestand zur Verfügung.



Erzeugt ein Teilnehmer durch eine neue Transaktion, z. B. Übertragung eines Geldbetrage, einen neuen Datensatz, so wird dieser zunächst auf seine Gültigkeit geprüft. Die Prüfung geschieht durch einen Konsensmechanismus.

Dieser Mechanismus legt fest, welche Bedingungen erfüllt werden müssen, um dem Kontenbuch (ledger) eine neue gültige Transaktion hinzuzufügen.

Konsensmechanismen zur Gültigkeitsprüfung

Name	Beschreibung
Proof-of-Work = Arbeitsnachweis	Arbeitsnachweis durch den Einsatz von Rechenaufwand eines Teilnehmers.
Proof-of-Stake = Anteilsnachweis	Anteilsnachweis durch Gewichtung der einzelnen Teilnehmer aus Teilnahmedauer und Vermögen („Stake")
PBFT (Practical Byzantine Fault Tolerance, = Praktische byzantinische Fehlertoleranz)	Einigung einer Mindestanzahl von Teilnehmern auf die Gültigkeit einer Transaktion

Mit **Proof-of-Work** wird Arbeitsaufwand eines Teilnehmers gewichtet, z. B. um ein Zufallswort, eine „Nonce", zu finden. Damit soll der Anwender abgehalten werden, einen Dienst übermäßig in Anspruch zu nehmen oder missbräuchlich zu verwenden.

Bei der Kryptowährung Bitcoin ist dieser Arbeitsnachweis das zeit- und energieintensive „Mining".

Proof-of-Stake gewichtet die Teilnahmedauer eines Teilnehmers am Netzwerk und sein Vermögen, Transaktionen durchzuführen.

PBFT erfordert eine Mindestanzahl an Teilnehmern für die Gültigkeit einer Transaktion.

Offene und geschlossene Distributed Ledgers

Offene und geschlossene Netzwerke von Distributed Ledgers unterscheiden sich durch die Möglichkeit des Zugangs der Teilnehmer. In offenen (unpermissioned = unregistrierten) Ledgers hat jeder nach einfacher Authentifizierung Zugang. In geschlossenen (permissioned = auf einen angemeldeten Teilnehmerkreis beschränkten) Netzwerken werden die Teilnehmer registriert und müssen bestimmte Voraussetzungen für den Zugang zum Kontenbuch erfüllen. Zum Beispiel kann ein geschlossenes Distributed Ledger für alle Kunden oder Lieferanten eingerichtet werden.

In offenen Netzwerken (unpermissioned) mit einem unbeschränkten Teilnehmerkreis ist der Konsensmechanismen Proof-of-Work üblich. Dies geschieht, indem der Teilnehmer eine bestimmte Rechenleistung oder eine Zeitverzögerung erlauben muss.

Proof-of-Work wird z. B. bei der Kryptowährung Bitcoin angewendet. Auch E-Mail-Provider verwenden teilweise dieses Konzept, indem sie den Versand einer E-Mail um wenige Sekunden verzögern. Dies stört einen normalen Anwender kaum, erschwert aber den Versand von Spam-Mails erheblich.

Proof-of-Stake wird bei permissioned ledgers angewendet (z. B. geplante Anwendung bei der Kryptowährung Ethereum). Dieser Mechanismus benötigt weniger Rechenkapazität, da die Teilnehmer bereits durch eine mehrstufige Anmeldung legitimiert sind.

Vorteile der Distributed-Ledger-Technologie

Gegenüber herkömmlicher Datenverwaltung zeigt die DLT folgende Vorteile:

- Transparenz und Unveränderbarkeit: Jeder Teilnehmer kann im verteilten Kontenbuch die gesamten Datenveränderungen einsehen. Dadurch werden die Transaktionen für alle nachvollziehbar.
- Transaktionen können ohne vorgesetzte Zentralinstanzen abgewickelt werden (P2P = peer to peer).
- Sicherheit: auch bei Ausfall eines Teils des Netzwerks sind die gesamten Daten vorhanden.

1.3.5.2 Blockchain

Blockchain (= Blockkette) basiert auf dem Konzept der Distributed-Ledger-Technologie (DLT). Eine Blockchain ist eine stetig erweiterbare Liste von Datensätzen, die zu Blöcken verbunden werden. Diese Blöcke werden durch kryptografische Verfahren miteinander verkettet. Dazu wird am Ende eines jeden Blocks eine Prüfsumme gebildet. Der Beginn des nächsten Blocks enthält vor dem ersten Datensatz einen Verweis auf die Prüfsumme des vorhergehenden Blocks.