Bird & Bird

Blockchain 101

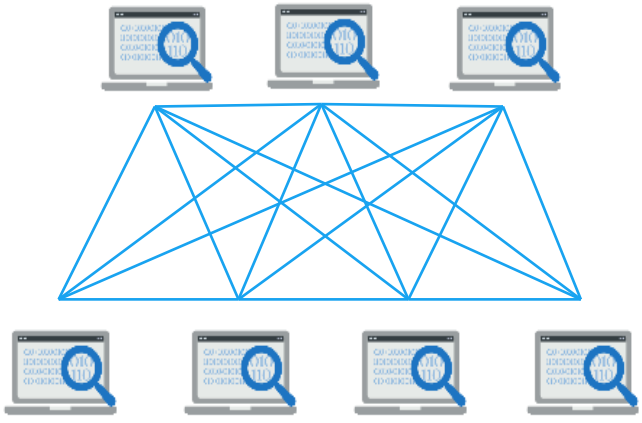
"Blockchain ist im Grunde ein dezentrales Protokoll für Transaktionen, das jede Veränderung transparent erfasst."

Als führende Kanzlei im Technologiebereich fördern wir neue und disruptive Technologien. Dazu gehört die wegweisende Blockchain- bzw. Distributed Ledger-Technologie, die wie zuvor das Internet das Potenzial birgt bestimmte Industriesektoren grundlegend zu revolutionieren. Wer die Zukunft gestalten, die eigene Position behalten oder ausbauen möchte, muss dieser Technologie die nötige Aufmerksamkeit schenken. Wir bieten den kompetenten Einstieg in die Technologie, sowie Know-How zu ihren Varianten, Vorteilen und Anwendungsmöglichkeiten.

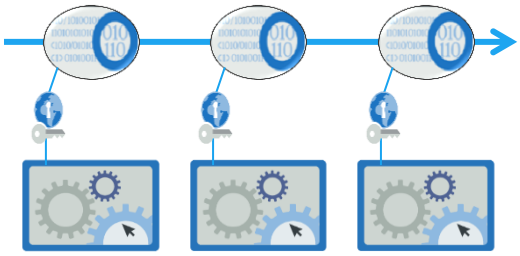
Wie funktioniert eine Blockchain?

Eine Blockchain ist eine dezentrale Datenbank, deren Validierung durch einen Konsensmechanismus erfolgt. Das Besondere an der Blockchain-Technologie ist daher, dass niemand die alleinige Kontrolle über die Datenbank und die Entscheidungsfindung für deren Veränderung hat. Die Technologie ermöglicht somit eine dezentrale und nachträglich unveränderbare Dokumentation von Transaktionsabfolgen innerhalb eines Peer-to-Peer-Netzwerks. Die dezentrale Datenbank ist, anders als bei zentralen Systemen, wie bspw. einem Cloud-Service, dabei auf alle teilnehmenden Rechner bzw. Knotenpunkte (Nodes) im System verteilt, sodass (zumindest in den meisten Fällen) jeder teilnehmende Rechner eine eigene, vollständige Kopie der Datenbank speichert.

Dezentralisierte Datenverarbeitung



verschlüsselte Hashfunktionen



Entschlüsselung mit dem Privaten Schlüssel befähigt zum lesen des Blocks.

Die typische Charakteristik von Blockchain-Technologien gewährleistet eine erhöhte IT- bzw. Daten- und Manipulationssicherheit. Des Weiteren ermöglicht die Technologie die sichere und nachvollziehbare Transaktion beliebiger Vermögenswerte zwischen natürlichen und/oder juristischen Personen - ohne dass hierfür klassische öffentliche oder private Institutionen (oder „Mittler") wie etwa Banken, Grundbuchämter oder andere Dienstleister eingeschaltet werden müssen.

Eine Transaktion wird durch Umwandlung in eine Hashfunktion vergleichbar gemacht und asymmetrisch verschlüsselt. Ein öffentlicher Schlüssel dient der eindeutigen Identifikation des Teilnehmers und ist in der Regel anderen Teilnehmern bekannt (z.B. eine Bitcoin Adresse). Ein privater Schlüssel dient der sicheren Authentifikation und Signierung von Transaktionen. Nur mit der Kombination dieser Schlüssel lassen sich Transaktionen auf der Blockchain nachvollziehen. Innerhalb des Netzwerks wird jede Transaktion nachvollzogen und vor Ausführung verifiziert, denn der Hashwert zur Transaktion unterläuft einer netzwerkweiten Gegenprobe, ob der Absender berechtigt und die Transaktion möglich ist. Erst dann wird sie ausgeführt und der Kette angehangen. Bei der nächsten Transaktion wird entsprechend auch auf diese Daten zurückgegriffen. Sollen nur Teile der Kette dem Empfänger lesbar gemacht werden, bleibt der Rest für zukünftige Transaktionen zur Gegenprobe im Trustsystem von den lesbaren Daten getrennt und in der Hashfunktion verschlüsselt gespeichert.

Blockchain in Stichpunkten

- *Dezentrales Datennetzwerk: Alle* Daten werden auf allen teilnehmenden Rechnern gespeichert und liegen dort zur Gegenprobe per Konsensmechanismus bereit.
- *Ein demokratischer Konsensmechanismus:* ob proof-of-work oder proof-of-stake, Teilnehmer der Blockchain validieren die Transaktionen innerhalb des Netzwerks.
- *Konsensmechanismen:* Im proof-of-work Verfahren sagt die Mehrheit was stimmt. Bei proof-of-stake ergibt sich Sicherheit aus den Anteilen der Teilnehmer.
- *Sichere Datenverwaltung und Übermittlung:* Jede Transaktion wird vom gesamten Netzwerk validiert, bevor sie endgültig in die Datenbank aufgenommen wird.
- *Nicht manipulierbare Datenbank:* der Konsensmechanismus gewährleistet die Richtigkeit der dezentralen Datenbank bzw. der durchgeführten Transaktionen.
- *Möglichkeit von **„Smart Contracts“**:* automatisierte Ausführung bei Eintritt festgelegter Voraussetzungen– ohne menschliche Prüfung, Bestätigung oder Aktion.
- *Transparenz:* Jeder Teilnehmer kann jederzeit alle Transaktionen einsehen.

Unsere Blockchainspezialisten

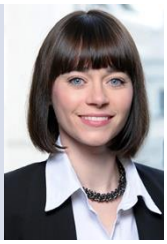
Dr. Michael Jünemann
Partner, Banking & Finance
Tel: +49 (0)69 74222 6230
michael.juenemann@twobirds.com

Lennart Schüssler
Partner, Commercial
Tel: +49 (0) 211 2005 6377
lennart.schuessler@twobirds.com

Johannes Wirtz
Associate, Banking & Finance
Tel.: +49 (0)69 74222 6267
johannes.wirtz@twobirds.com

Oliver Schmidt
Associate, Commercial
Tel: +49 (0) 211 2005 6162
oliver.schmidt@twobirds.com

Dr. Angela Kast
Associate, Banking & Finance
Tel.: +49 (0)89 3581 6233
angela.kast@twobirds.com



Mehmet Baki Alacayir
Associate, Commercial
Tel: +49 (0) 211 2005 6185
mehmet.baki.alacayir@twobirds.com

Julia Fröhder
Associate, Banking & Finance
Tel: +49 (0)69 74222 6268
julia.froehder@twobirds.com

Liliana Rodrigues-Kaps
Rechtsanwältin, Banking & Finance
Tel: +49 (0) 69 74222 6132
liliana.rodrigues-kaps@twobirds.com