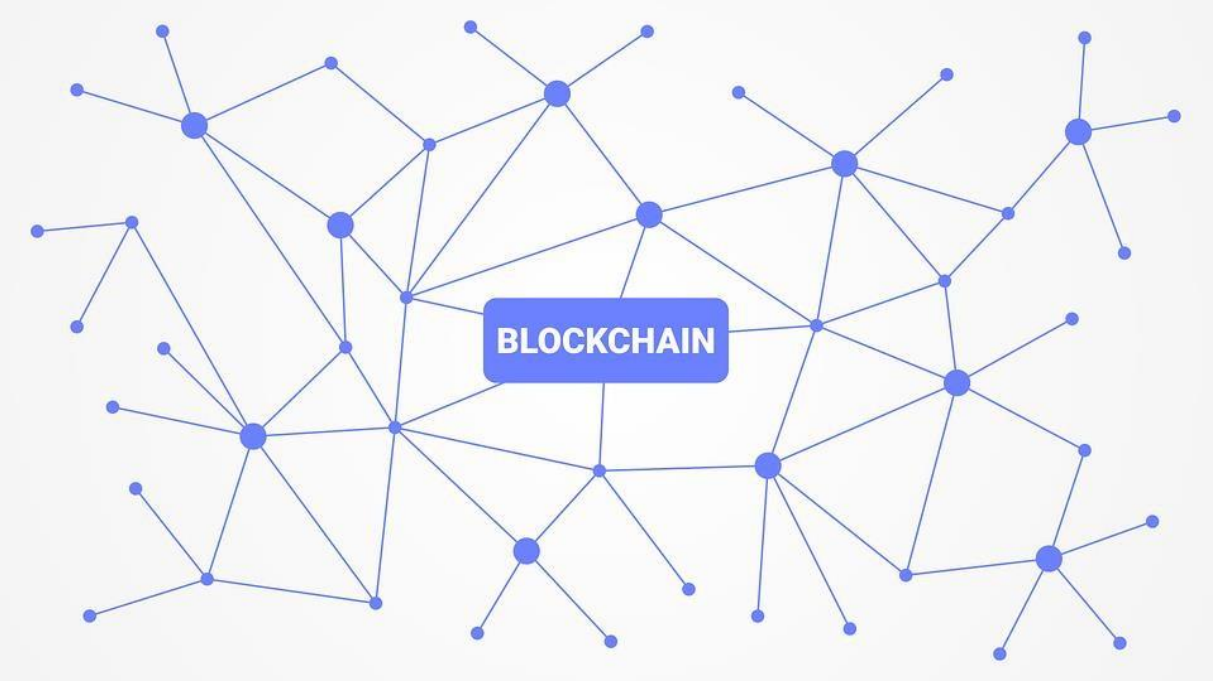
Konzept und Funktionsweise von Blockchains



https://pixabay.com/de/vectors/block-kette-kryptow%c3%a4hrung-netzwerk-3277335/, 03.02.2022

1. Das Blockchain-Netzwerk[1]

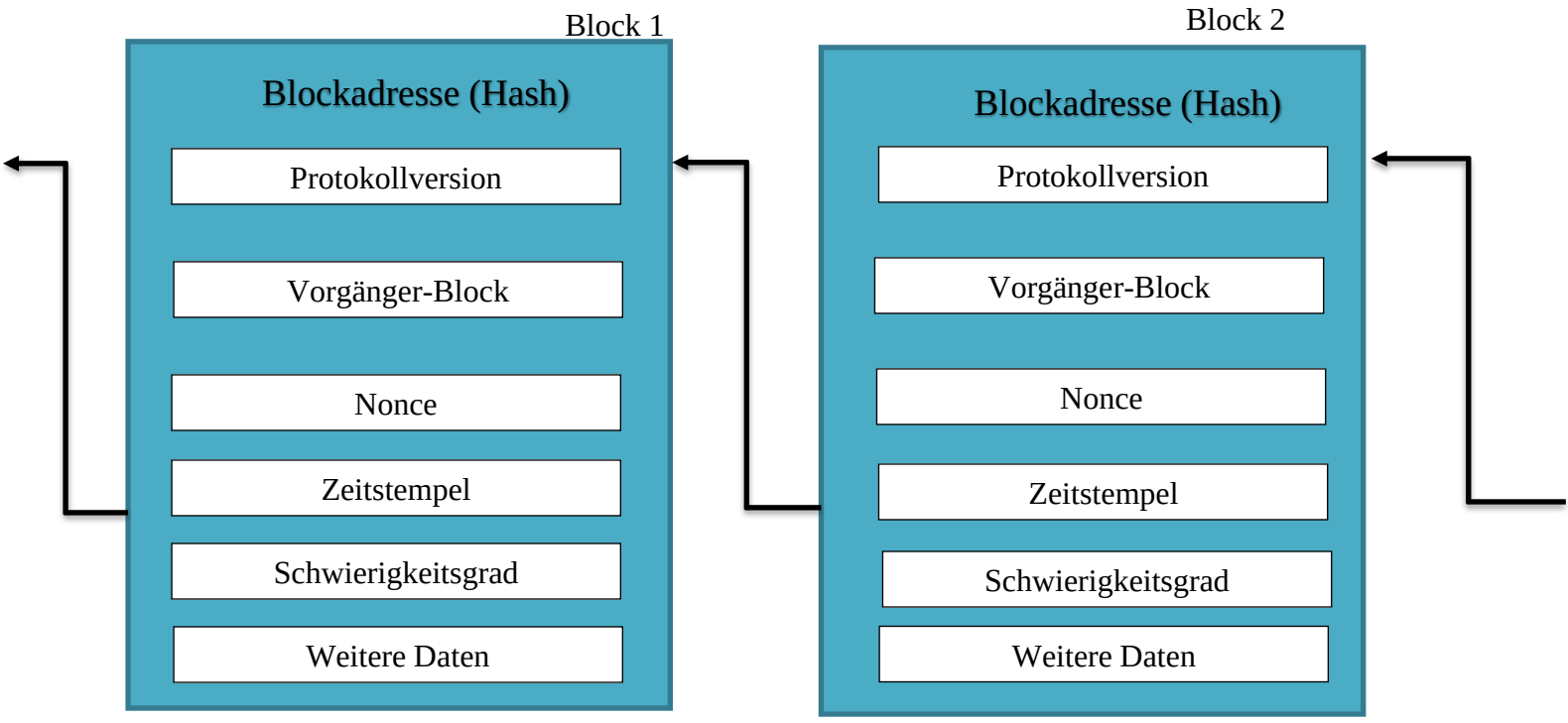
Die Blockchain bezeichnet eine Datenstruktur, die folgende Eigenschaften erfüllt:

- **Dezentralität:**
  Die Daten werden nicht zentral, auf einem Server, gespeichert. Jeder Client besitzt eine Kopie aller Daten und fungiert dadurch selbst als Server.
- **Transparenz:**
  Da alle Clients jederzeit eine Kopie der Daten besitzen, ist ständig einsehbar welcher Nutzer zu welchem Zeitpunkt eine Operation auf der Datenstruktur durchgeführt hat.
- **Manipulationssicherheit**
  Das Manipulieren oder Löschen von Daten ist nahezu unmöglich, da alle Clients ein solches Ereignis sofort bemerken würden.

Durch die Eigenschaften der Datenstruktur können Daten von der Blockchain nicht gelöscht werden. Ist einmal etwas darauf gespeichert, befinden sich die Daten dort permanent. Das unterscheidet die Blockchain von einer normalen Datenbank, die von ihrem Inhaber nachträglich verändert werden kann.

[1] Der Kontext: https://map.derkontext.com/blockchain#m=12/2089.20913/812.5249,p=5, 04.02.2022

2. Aufbau der Blockchain[2]



Eine Blockchain besteht aus mehreren Blöcken, die in einer Kette angeordnet sind. Dabei besitzt jeder Block einen Verweis auf seinen Vorgänger.

- In der Blockadresse (dem Hash) steht der eindeutige Name des Blockes drin.
- Die *Protokollversion* gibt das Regelwerk an, unter dem der Block erstellt wurde.
- Die *Nonce* (*number used once)* ist eine Zahl, mit dessen Hilfe die Blockadresse errechnet wird. Mit ihrer Hilfe soll der Proof-of-Work erfüllt werden.
- Der *Zeitstempel* bildet den genauen Zeitpunkt ab, an dem der Block erstellt wurde.
- Der *Schwierigkeitsgrad* gibt an, mit welcher Schwierigkeit der Block erstellt wird.
- In *weiteren Daten* kann alles Weitere geschrieben werden, was gespeichert werden soll. Je nachdem, wofür die Blockchain genutzt wird.

[2] Tilman Walter Neuhaus: Die Blockchain im Stufenmodell: Grundlagen und Anwendungen in unterschiedlichen Komplexitätsstufen, Universität Rostock, S. 9

3. Blockerstellung mit dem Proof-of-Work[3]

Der *Proof-of-Work* ist der älteste Algorithmus, der zur Erstellung von Blockchains genutzt wird. Hier lösen alle teilnehmenden Geräte eine komplexe Aufgabe. Wer das am schnellsten schafft, erzeugt den nächsten Block in der Blockchain. Die Lösung wird von allen Teilnehmenden überprüft und wenn sie richtig ist, erhält man (im Normalfall) eine Belohnung. Ist sie falsch, muss weitergerechnet werden.

Der Proof-of-Work wird beispielsweise bei Bitcoin benutzt. Diejenigen, die dort einen neuen Block erstellen, erhalten Bitcoins als Belohnung. Dort wird auf folgende Weise ein neuer Block erstellt:

- Die Rechenaufgabe lautet: „`Finde eine Nonce, mit welcher der Proof-of-Work erfüllt wird.`“
- Der *Proof-of-Work* wird durch den *Schwierigkeitsgrad* festgelegt. Dieser gibt an, wie viele Nullen am Anfang der *Blockadresse/dem Hash* stehen müssen,
- Dazu haben alle Teilnehmer einen Hash gegeben. Dieser wird über komplizierte Rechenverfahren mit den Zahlen aus der *Nonce* verknüpft. Entsteht dabei die geforderte *Blockadresse,* ist die Aufgabe gelöst.
- Die *Nonce* kann hier nur durch Ausprobieren ermittelt werden. Die Teilnehmer, welche die meiste Rechenleistung besitzen, können die meisten Zahlen ausprobieren und haben damit die höchsten Chancen einen neuen Block zu erstellen.
-

4. Blockerstellung mit dem Proof-Of-Stake[4]

Beim *Proof-of-Stake* sperren aktive Teilnehmer einen Teil ihrer Währung in ein virtuelles Portmonee. Dieser kann dann vorerst nicht mehr ausgegeben werden. Dieses Prinzip nennt man *Stake* (*Einsatz*). Auch beim Proof-of-Stake muss ein mathematisches Rätsel gelöst werden. Anders als beim Proof-of-Work hängt die Schwierigkeit allerdings von der Anzahl der eingesetzten Währung ab und wie lange diese bereits im virtuellen Portmonee liegen. Je größer diese Zahlen jeweils sind, umso geringer ist die Schwierigkeit des Rätsels für den entsprechenden Teilnehmenden. Auch bei diesem Verfahren wird eine Belohnung dann ausgezahlt, wenn jemand das Rätsel zuerst löst. Die Belohnung ist umso höher, je größer der

[3] Der Kontext: https://map.derkontext.com/blockchain#m=9/1832.84494/565.23998,p=38, 03.02.2022
[4] Der Kontext: https://map.derkontext.com/blockchain#m=9/1949.58746/585.5662,p=41, 03.02.2022

Einsatz und dessen Verweildauer in dem virtuellen Geldbeutel ist. Der Einsatz kann jederzeit wieder aus dem Portmonee rausgeholt werden.

5. Chancen und Risiken der Blockchain[5][6]

Aufgrund der Eigenschaften von der Blockchain lässt sich eine deutliche Richtung für deren Nutzung erkennen. Alles, was dezentral funktionieren solle, kann auf einer Blockchain laufen. Genauso kann alles, was als digitales Produkt einzigartig sein soll (Musik, Bilder, Texte, etc.) mittels Blockchaintechnologie eindeutig zugeordnet werden.

Bis heute ist es bei digitalen Inhalten oft schwierig die ursprünglichen Herausgeber festzustellen oder zu verhindern, dass diese 1:1 kopiert werden. Raubkopien sind oft der Fall. Werden jedoch solche Produkte mit einem Hash versehen und auf einer Blockchain gespeichert, ist der Urheber bzw. die Uhrheberin immer eindeutig nachweisbar.

Ein Risiko liegt in allerdings der Beschaffenheit der Blockchain. Sobald ein neuer Block entsteht, können alle alten Blöcke nicht mehr verändert werden. D.h. Daten, die sich auf dieser Kette befinden, sind nicht löschbar.

Ein weiteres aktuelles Risiko der Blockchain liegt im *Proof-of-Work*, bei dem Stromverbrauch. Derzeit wollen möglichst viele Miner so viele Bitcoins wie möglich erhalten. Damit brauchen sie viel Rechenleistung, was einen enormen Stromverbrauch voraussetzt. Versuchen also einige 10.000 oder 100.000 Miner gleichzeitig ihre Aufgabe zu erfüllen, braucht es viel Energie. Derartiger Energieverbrauch hat beispielsweise negative Auswirkungen auf das Klima.

[5] Der Kontext: https://map.derkontext.com/blockchain#m=9/2356.74081/486.88835,p=10, 03.02.2022
[6] https://map.derkontext.com/blockchain#m=9/2181.90099/435.06573,p=9, 03.02.2022