

## Ausführungen und Erwartungen zur Unterrichtseinheit 2

In diesem Block ist bereits ein Beispielaufgaben (inklusive Erwartungsbild) gegeben, welches sich an dem Infomaterial im allgemeinen Bereich orientiert. Für eine vertiefende und kompakte Lektüre wird die verlinkte Seite, der Kontext, empfohlen. Hier ist allerdings eine kostenlose Anmeldung notwendig, um auf alle Informationen zuzugreifen. Das Aufgabenblatt kann beliebiger Form schriftlich gelöst werden. Ein alternatives Konzept wäre, dass sich zuerst alle SuS in Einzelarbeit die Eigenschaften sowie den Aufbau der Blockchain erarbeiten. Danach können Expertenteam für den Proof-of-Work und den Proof-of-Stake gebildet werden. Die SuS könnten kurze Präsentationen erarbeiten oder sich beide Konzepte gegenseitig erklären. Danach findet wieder eine gemeinsame Diskussion über Chancen und Risiken der Blockchain statt. Informationsmaterial kann aus dem beigefügten Infomaterial, im allgemeinen Bereich, entnommen werden. Die Lehrkraft muss den Schülerinnen und Schüler derartiges Material zur Seite stellen.

Die Unterrichtseinheit 2 hat das Ziel, ein fundiertes, theoretisches und praktisches Wissen bezüglich des Aufbaus und der Funktion der Blockchain herzustellen. Dabei soll der Vorgang zur Blockerstellung mit Hilfe von zwei verschiedenen Methoden, dem Proof-of-Work sowie dem Proof-of-Stake, näher beleuchtet werden.

Die SuS sollen

- die Bestandteile und deren jeweilige Funktionen einer Blockchain nennen.
- den Vorgang zur Blockerstellung beim Proof-of-Work sowie beim Proof-of-Stake erklären.
- die Unterschiede der Proof-Methoden erläutern.
- erste Chancen und Risiken der Blockchaintechnologie bewerten.

Zu Beginn der Unterrichtseinheit empfiehlt es sich, die Funktion von Hashes zu erklären. Dies kann mit Hilfe der von CS Unplugged erstellten Aktivität 6, "Schiffe versenken", getan werden. In diesem Spiel wird die Suche mit Hilfe von Hashadressen thematisiert. Die Lehrkraft kann dieses Spiel von mehreren SuS-Gruppen durchführen lassen. Anschließend eignet sich eine Diskussion bzw. Klärung bezüglich des Begriffs "Hash".

Ein Hash reduziert eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge fester Länge. Hashwerte werden bspw. bei Prüfsummen verwendet und mit den Zeichen des Hexadezimalsystems (0 - F) codiert. An dieser Stelle lassen sich Parallelen zu Themen aus dem Bereich "Prinzipien der Datenübertragung verstehen" ziehen.

Mit Hilfe von Hashadressen lassen sich Daten schnell finden und zuordnen. Ist die Hashadresse bekannt, lässt sich durch eine einfache Rechnung sofort herausfinden, an welcher Stelle das Objekt steht. Bei der Blockchain ist nur die Stelle bekannt, an der das nächste Objekt stehen muss, aber die Hashadresse nicht. Diese gilt es zu finden. In Bezug zu dem Beispiel aus CS-Unplugged: Es gibt einen Haufen ungeordneter Schiffe, die alle verschiedene Adressen besitzen. Es passt immer nur ein Schiff an eine einzige Stelle. Nun muss immer zur jeweiligen Stelle herausgefunden werden, welches Schiff dort reingehört.

Dieses Beispiel bietet einen erleichternden Einstieg in die Erstellung von Blockchains und klärt gleichzeitig den Begriff des Hash. Einen passenden Auszug zu der Lektion aus CS-Unplugged ist in diesem Bereich, auf deutscher Sprache, enthalten.

Für den Vorgang zur Ermittlung der Nonce bietet es sich an, dieses Beispiel praktisch, mit Hilfe eines Hashrechners (siehe Hashgenerator), durchzugehen. Ein passendes Beispiel ist auf der Seite "Der Kontext", unter "Nonce und Difficulty" zu finden. Dabei soll verdeutlicht werden, dass die Nonce nur durch Ausprobieren ermittelt werden kann.

Bei der Bewertung bezüglich möglicher Chancen und Risiken lassen sich weitere, vertiefende Themenfelder behandeln. Diese können bereits in der Einheit 2 angesprochen werden. Ein Beispiel dafür ist das Belohnungssystem vom Proof-of-Work. Wer am meisten Rechenleistung besitzt, hat theoretisch die höchste Chance einen neuen Block freizuschalten. An dieser Stelle können aktuelle Bezüge zu den Problemen des Minings gezogen werden. Die stetig wachsende Teilnehmendenzahl bei bspw. Bitcoin sorgt dafür, dass Miner ihre Rechenleistung immer weiter erhöhen wollen und müssen. Dadurch entsteht ein Wettbewerb, wer die höchste Rechenleistung besitzt. Das sorgt für einen enormen Stromverbrauch und kann folglich Auswirkungen auf lokale Stromnetze haben und mögliche Umweltschäden verursachen bzw. beschleunigen. Es gibt bereits Länder, die das Minen unter Strafe stellen bzw. dies in Erwägung ziehen. So ist das Mining vom Bitcoin bspw. bereits in China komplett verboten<sup>1</sup>. Gleichzeitig hat der EZB in einem Gutachten die Wahrscheinlichkeit als hoch eingeschätzt, dass Proof-of-work basiertes Mining ebenfalls zukünftig in Deutschland und der EU verboten wird<sup>2</sup>

Durch die Eigenschaften der Blockchain versuchen viele Anwender diese zu nutzen. Die SuS sollten nach dieser Unterrichtseinheit dazu in der Lage sein zu bewerten, aus welchem Grund dies so ist. Anwender müssen sich nicht mehr auf eine Bank bzw. andere Dritte verlassen, wenn sie Daten speichern oder andere Operationen durchführen wollen. Ein Geschäft würde direkt zwischen zwei Parteien laufen.

In der folgenden Unterrichtseinheit (3) werden weitere Anwendungsfälle, außerhalb von Kryptowährungen, betrachtet. Dies ermöglicht die Festigung eines tiefgreifenderen Wissens bezüglich der Blockchain und erlaubt es den SuS die Thematik vertieft zu bewerten. Dabei sollte dringend auch auf Gefahren eingegangen werden (Bsp. NFT-Scams), die mit der Blockchain einhergehen.

---

<sup>1</sup> Wurzel, Steffen: China verbietet Kryptogeld-Handel, <https://www.tagesschau.de/wirtschaft/finanzen/china-kryptowaehrungen-101.html>, 14.09.2022.

<sup>2</sup> Hoppmann, Daniel: EZB-Report hält Bitcoin-Mining-Verbot für „wahrscheinlich“. <https://www.btc-echo.de/news/ezb-report-haelt-bitcoin-mining-verbot-fuer-wahrscheinlich-146846/>, 14.09.2022.