Erwartungen zu den Auswertungen für Unterrichtseinheit 1

1. Phase 1

In der Phase 1 sollen die SuS zunächst Transaktionen innerhalb ihrer Gruppe durchführen. Alle Teilnehmer tätigen zwei Überweisungen. Dabei soll von allen ein Transaktionsbuch geführt werden, in dem festgehalten wird, wer an wen welche Menge an Münzen überwiesen hat. Im Vorfeld ist dafür zu klären, wie die SuS im Transaktionsbuch bezeichnet werden (siehe Organisation Unterrichtseinheit 1). Wer zuerst alle Transaktionen im Buch eingetragen hat, fertigt eine Kopie davon an und darf diese in die Mitte des Tisches legen. Wurden alle Arbeitsschritte erfüllt, kann eine Auswertungsphase. Ziel ist es, Vor- und Nachteile der Struktur (alle führen das Transaktionsbuch und es liegt eine Kopie in der Mitte) auszuarbeiten. Es ist zu erwarten, dass die SuS nicht von alleine auf die genannten Vorteile kommen. Die Lehrkraft muss eine leitende Rolle einnehmen und die SuS zu den Lösungen führen. Es ist offensichtlich, dass jede(r) TeilnehmerIn alle Transaktionen einsehen kann. Dadurch ergibt sich der Vorteil, dass nichts gefälscht werden und damit schwer betrogen werden kann. Fälschungen würden auffallen, da alle die gleiche Liste besitzen müssten. Nachteile sind leichter zu erkennen. Offensichtlich erfordert die bisher gezeigte Struktur einen hohen Arbeitsaufwand. Bei der Suche nach Fehlern müssten alle Listen durchsucht werden, was sowohl zeit- als auch arbeitsintensiv ist.

2. Phase 2

Um dieses Problem zu umgehen, soll eine weitere Struktur, die Blockchain, eingefügt werden. Mit Hilfe dieser Struktur wird der Aufwand, eine Fälschung ausfindig zu machen, theoretisch verringert. Die SuS schlüpfen dafür in neue Rollen: die Miner und die Händler. Aufgabe der Miner ist es, ihrer Beschreibung entsprechend ein Zahlenrätsel zu lösen. Ist dies geschafft, wird mit Hilfe des Arbeitsblattes „Blocknamen berechnen“ ein Block für eine bereits bestehende Blockchain erstellt. Die Lehrkraft entscheidet selbst, wie oft dieser Vorgang durchgeführt werden soll. Es sollten allerdings wenigstens drei Blöcke erstellt werden, um den Vorgang zu verinnerlichen. Sollten die HändlerInnen einen Leerlauf haben, können diese als Hilfen bei den Minern einspringen. Daraus resultiert der Vorteil, dass das Zahlenrätsel potentiell doppelt so schnell gelöst werden kann. Dieser Vorteil sollte in der Auswertungsphase aufgegriffen werden.

Es ist zu erwarten, dass die Aufgabe der Blockberechnung nicht ohne Weiteres gelingt. Es wird empfohlen, zunächst mit einer an der Tafel angebrachten Blockchain das erste Beispiel gemeinsam mit der Klasse durchzugehen. So können alle SuS das Anfügen eines Blockes an die Kette verfolgen. Danach kann selbstständig gearbeitet werden. Bei der Berechnung des Blocknamens handelt es sich um ein Verfahren, welches es den SuS möglichst schwer bzw. unmöglich machen soll, einen Block zu fälschen.

Ein mögliches Erwartungsbild für einen erstellten Block sieht bspw. folgendermaßen aus:

Gruppennamen:

LBNB = 122142, ABCD = 1234, EFHI = 5689

Quersummen: LBNB = 8, ABCD = 10, EFHI = 28

Transaktionen:

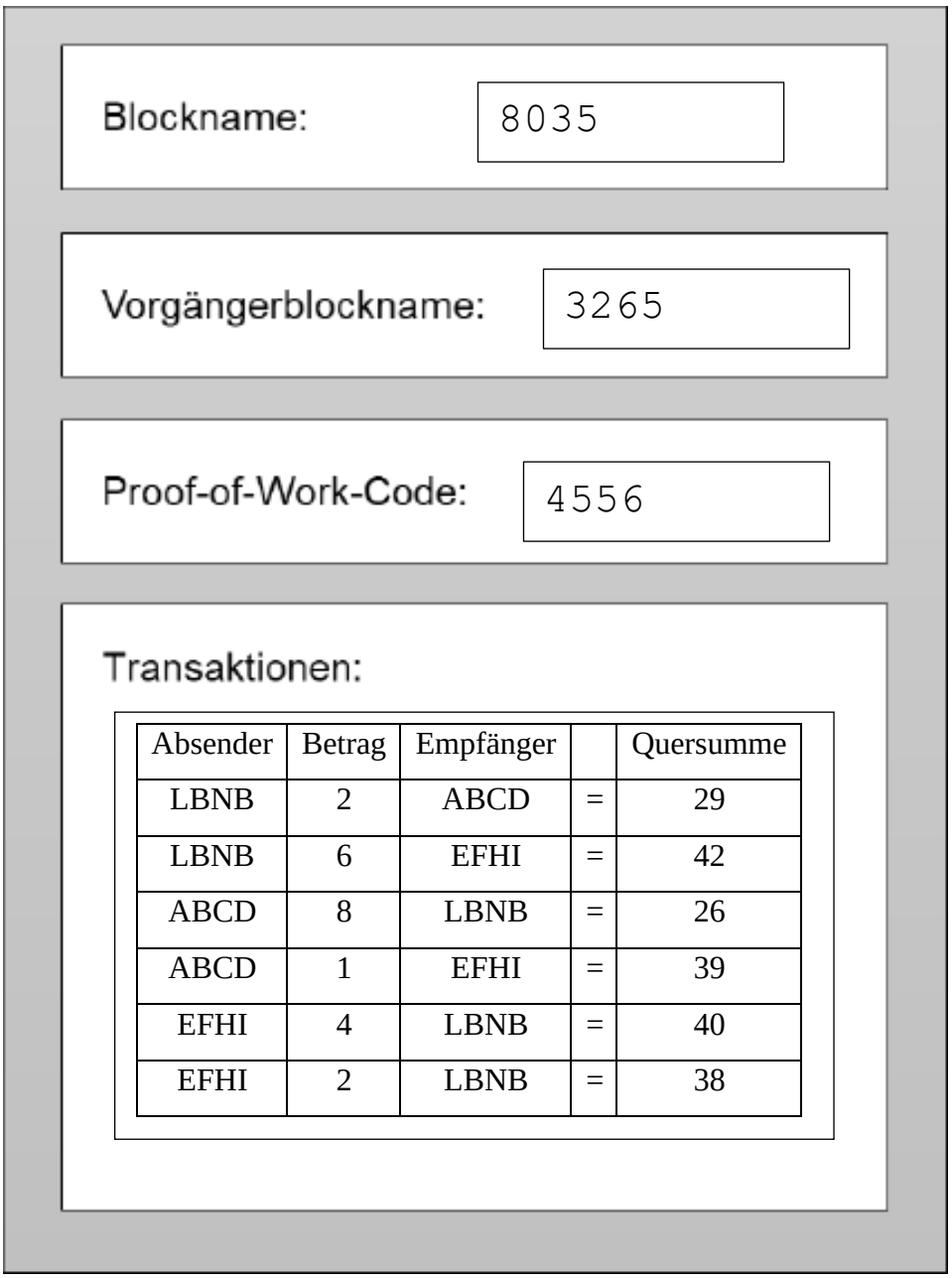
Absender	Betrag	Empfänger		Quersumme
LBNB	2	ABCD	=	29
LBNB	6	EFHI	=	42
ABCD	8	LBNB	=	26
ABCD	1	EFHI	=	39
EFHI	4	LBNB	=	40
EFHI	2	LBNB	=	38

Proof-of-Work-Code: 4556

Vorgängerblockname: 3265

Blockname: 8035

Daraus ergäbe sich bspw. folgendes Muster für den Block (siehe nächste Seite):



Absender	Betrag	Empfänger		Quersumme
LBNB	2	ABCD	=	29
LBNB	6	EFHI	=	42
ABCD	8	LBNB	=	26
ABCD	1	EFHI	=	39
EFHI	4	LBNB	=	40
EFHI	2	LBNB	=	38

Es ist zu erwarten, dass die Erstellung eines Blockes eine gewisse Zeit benötigen wird. Während der Block berechnet wird, können die anderen Mitglieder des Tisches bereits am nächsten Block arbeiten. Ebenso kann aber auch der Händler die Berechnung übernehmen. Im nächsten Schritt soll sich eine Gruppe auflösen. Die entsprechenden SuS erhalten die neue Rolle „Gast“ durch die sie als externe Händler in andere Gruppen gehen können.

In der anschließenden Auswertungsphase ist von der Lehrkraft auf die Eigenschaft der Transparenz der Kette einzugehen. Auch hier lässt sich beobachten, dass durch die Kette genaustens nachverfolgt werden kann, wieviel an welche Teilnehmer überwiesen wurde. Eine Gemeinsamkeit zur ersten Struktur ist, dass das Transaktionsbuch auch hier existiert. Nur bildet es einen Bestandteil eines Blockes. Es ist zu erwarten, dass die SuS hier die Frage

nach dem Sinn der Blockerstellung stellen. Sollte dies geschehen, kann die Lehrkraft umgehend auf Phase 3 springen. Andernfalls müssen auch die Handlungsschritte ausgewertet werden. Die SuS sollten den Vorteil vom Minen erkannt haben, da sie dort Belohnungen erhalten, wenn sie das Rätsel lösen. Ein großer Nachteil ist hier jedoch auch die hohe Arbeitslast beim Erstellen eines Blockes. Weitere Überlegungen sind zum Einbinden weiterer Miner und Außenstehender nötig. Weitere Miner erhöhen die Rechenleistung, wodurch schneller Blöcke erstellt werden können und die Beteiligung zusätzlicher Händler erhöht die Belohnung bei der Blockerstellung. Es ist zu erwarten, dass die SuS diese Umstände bemerken.

3. Phase 3

Für Phase 3 wird eine offene Diskussion und Vorführung mit der Klasse angestrebt. Die Frage lautet: „Fallen Fälschungen jetzt schneller auf?“ bzw. „Welchen Sinn hat das Rechnen für die Blockerstellung?“. Die Lehrkraft kann mit einer bestehenden Blockchain zeigen, dass Fälschungen unmöglich sind. Da bei der Änderung einer einzigen Zahl, der Blockname im eignen Block sowie der Vorgängerblockname im nächsten Block nicht mehr stimmt. Die Datenstruktur ist damit vor Manipulationen gesichert und anstatt, dass alle Listen durchgesehen werden müssen, fallen mögliche Versuche hier sofort auf.

4. Fazit Unterrichtseinheit 1

Mit den in der Unterrichtseinheit 1 getätigten Arbeitsschritten wurden das Prinzip der Transparenz sowie der Manipulationssicherheit näher betrachtet. Ebenso wurde die Arbeitsweise der Blockchain bei Kryptowährungen analysiert. Damit lassen sich bereits erste Bewertungen zur Blockchain ableiten, ohne diese näher bestimmt zu haben. Das Prinzip der Dezentralität kann in diesem Teil auch angesprochen werden. Es ist jedoch zu erwarten, dass die SuS diesen Aspekt nicht sofort erkennen, da sie Transaktionen „über die Blockchain“ abwickeln. Das kann in der nächsten Unterrichtseinheit aufgegriffen werden.