

Lösungsvorschläge

Lösungsvorschlag E.2:

Eine Musterlösung ist hier nur bedingt sinnvoll, da es explizit um die Bewertung durch die Schüler*innen geht und eben nicht um eine objektive Bewertung. Trotzdem sind an dieser Stelle kurz die wichtigsten Erkenntnisse aus dem Arbeitsheft zusammengefasst:

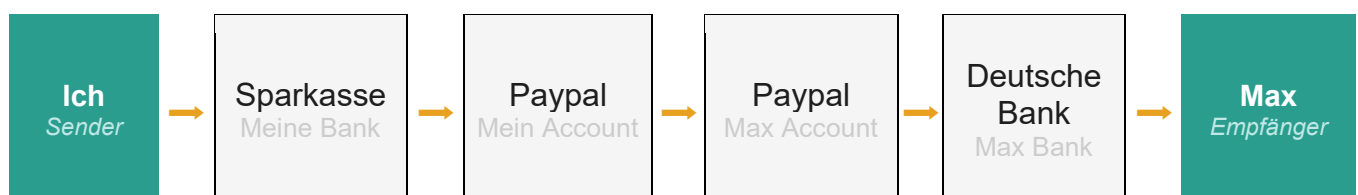
Behauptung	Erklärung: Warum ist das von Vorteil für Bitcoin oder dessen Nutzer*innen? (falls du dir unsicher bist, recherchiere im Internet)	Lösungsvorschlag: Wie bewertest du diesen Aspekt jetzt?
Bitcoin ist anonym.	Die Nutzer*innen können Transaktionen tätigen, ohne dass diese von irgendjemandem zugeordnet werden können.	Bitcoin ist eigentlich nur bedingt anonym, da es mir gar nicht möglich ist Bitcoin vollständig anonym zu erwerben. Die Transaktionen sind außerdem immer öffentlich einsehbar.
Bitcoin ist schnell.	Man kann jederzeit überall auf der Welt jemandem Bitcoin schicken.	Bitcoin ist im Vergleich zu klassischen Onlinezahlungen sogar sehr langsam, da nur 7 Transaktionen pro Sekunde möglich sind.
Bitcoin ist dezentral.	Durch die Dezentralität muss man keiner zentralen Institution vertrauen.	Die Dezentralität ist gar nicht das wichtige, sondern eher die Vertrauensfrage. Die weise in der Bitcoin das Hauptbuch dezentral speichert, hilft dabei, dass keiner zentralen Bank oder ähnlichem vertraut werden muss.

Zusätzliche Aspekte könnten beispielsweise sein: Unabhängigkeit von Fiatgeld, endliche Anzahl an Bitcoins, hohe Rendite als Investment, besonders sicher, ...
Die Vor- und Nachteile müssen hierbei im Einzelfall betrachtet werden.

Lösungsvorschlag 1.1:

Mögliche Orte könnten beispielsweise sein: lokal auf dem Smartphone, Google Bilder, Apple Cloud, Dropbox, ... oder eine Kombination daraus.

Lösungsvorschlag 1.4:



Lösungsvorschlag 1.5:

	Vorteile	Nachteile
Bargeld	Datenschutz (niemand erfährt davon)	-Bargeld muss passend gewechselt werden (aufwändig) -Dauert länger
Onlinezahlung/Überweisung	Käuferschutz	-Teilweise zusätzliche Kosten -kann technische Probleme haben

Lösungsvorschlag Abschlusssaufgabe 1:

Vorteile von Drittparteien	Nachteile von Drittparteien
Käuferschutz ist ein Vorteil für Nutzer*innen von Drittparteien, da die Drittpartei sicherstellt, dass man sein Geld zurückerhält, falls die andere Transaktionspartner*in ihre Versprechen nicht einhält.	Datenschutz möglicherweise ein Nachteil von Drittparteien, da diese theoretisch speichern können, welche Transaktionen sie abgewickelt haben.
Vergessen meiner PIN: Vergesse ich Zugangsdaten, kann ich diese in der Regel wieder zurückgewinnen, indem ich den Anbieter/Drittpartei kontaktiere.	Single Point-of-Failure: Wenn die Drittpartei ausfällt, kann die Transaktion nicht mehr ausgeführt werden. Bspw. Paypal-server oder die eigene Bank.
	AGBs Der Drittanbieter macht die Regeln, an die ich mich als Kunde halten muss. Je nachdem wie diese Regeln sind, kann das problematisch sein.

Lösungsvorschlag 2.1:

Anna: 0 Punkte Tom: 5 Punkte

Lösungsvorschlag 2.2:

Da sich dieser aus den Transaktionen jederzeit berechnen lässt.

Lösungsvorschlag 2.3:

Anna hat keine Punkte

Lösungsvorschlag 2.4:

Beispielsweise durch das Hinzufügen/Löschen von Transaktionen.

Lösungsvorschlag 2.5:

Beispielsweise durch das Herausreißen von Seiten oder das anderweitige Löschen von Transaktionen.

Lösungsvorschlag 2.6

Vorschlag	Vorteile	Nachteile
Tom wird der neue Hüttenpunktwächter. Er verwaltet das Hauptbuch in seinem Zimmer und Transaktionen werden nur von Tom in das Buch geschrieben.	Einfaches praktikables System.	Die Gruppe muss Tom vertrauen, dass Tom das Buch fair verwaltet. Tom hat die Monopolstellung und kann Transaktionen löschen, oder sogar gar nicht erst aufschreiben.
Das Hauptbuch wird dreimal kopiert, sodass es nun vier gleichwertige Kopien des Hauptbuchs gibt. Jede*r Teilnehmer*in erhält nun eine gleichwertige Kopie des Hauptbuches. Transaktionen müssen ab nun allen Teilnehmer*innen mitgeteilt werden, damit diese kopiert werden können.	Es muss nicht mehr Tom alleine vertraut werden.	Es ist unklar wie die Gruppe damit umgeht, falls verschiedene Versionen des Hauptbuchs entstehen. Was ist wenn jemand eine Transaktion nicht mitbekommen hat? Wirkt sehr aufwändig.

Lösungsvorschlag Abschlussaufgabe 2:

	Hüttenpunkte	Bitcoin
Wie wird unterschrieben?	Die bezahlende Person unterschreibt eine Transaktion physisch im Hauptbuch.	Transaktionen werden von der zahlenden Person mit digitalen Unterschriften signiert: Dabei wird ein asymmetrisches Verschlüsselungsverfahren verwendet.
Wie wird das Hauptbuch gespeichert?	Als physisches Buch entweder bei Tom als Hüttenpunktwächter, oder indem jede*r Teilnehmer*in eine eigene Kopie bekommt (Je nach Vorschlag aus 2.6)	Das Hauptbuch wird auf der Blockchain gespeichert: Jede Person kann auf diese Zugreifen oder diese sogar speichern. Es ist damit ein öffentliches Hauptbuch.

Lösungsvorschlag 3.2:

Timon findet eine Person, Bspw. Lukas, die bereits Teil des Hüttenpunktesystems ist. Timon überlegt sich nun sein eigenes Synonym (Bspw. Ernie) und teilt dies Lukas mit und bezahlt Lukas seine zwei Euro. Lukas schickt daraufhin 2 Hüttenpunkte an Timons neues Synonym:

#	Von	An	HP
07	Elmo	Ernie	2

Lösungsvorschlag 3.3:

Timon kennt nun Lukas Pseudonym und andersherum. Die meisten anderen Teilnehmer*innen können wahrscheinlich auch auf Timons Pseudonym schließen.

Lösungsvorschlag 3.4:

	Hüttenpunkte	Bitcoin
Wie werden die Einträge anonymisiert?	Teilnehmer*innen erscheinen nicht mit Klarnamen, sondern mit Pseudonymen.	Teilnehmer*innen erscheinen nicht mit Klarnamen, sondern mit Wallet-Adressen . Die Wallet Adresse ist eng mit der digitalen Signatur verbunden, da sie sich aus dem public Key der asymmetrischen Verschlüsselung ergibt.
Wie könntest du deine ersten Coins/Punkte erwerben?	Siehe 3.3	<i>Recherchiere: Wo musst du dich eventuell registrieren oder bist bereits registriert? Wie bezahlst du für die gekauften Bitcoin?:</i> Ich muss mich bei einer Kryptobörse registrieren wie bspw. Bison, Kraken oder Coinbase und dieser Kryptobörse Geld per herkömmlicher Onlinetransaktion schicken. Daraufhin erhalte ich von der Kryptobörse Bitcoin an meine angegebene Walletadresse. Oft verwalten diese Kryptobörsen sogar mein Wallet für mich.

Lösungsvorschlag 3.5:

Zumindest die Kryptobörse über die ich die Bitcoin gekauft habe kann nun meine Transaktionen zu mir zuordnen. Wenn diese Kryptobörse auch die Identitäten anderer Walletadressen kennt, kann sie unter Umständen sogar die Identität meiner Transaktionspartner*innen zuordnen.

Lösungsvorschlag 3.6:

Eine klassische Bank kennt zwar meine Transaktionen, veröffentlicht jedoch keine Transaktionshistorie dieser, auch nicht anonymisiert. Dahingegen ist meine Transaktionshistorie bei Bitcoin öffentlich, wenn auch anonymisiert, der Anbieter über den ich die Bitcoin gekauft habe kann diese jedoch trotzdem zuordnen.

Lösungsvorschlag 4.1:

Bei Zahlen bis drei hat das Quadrat weniger als zwei Ziffern.

Lösungsvorschlag 4.2:

Eingabezahl	Quadrat	Hashwert
-------------	---------	----------

42	1764	76
99	9801	80
13	169	16

Lösungsvorschlag 4.3:

Ja Bspw. 45 und 35: $\text{Hashq}(45) = 02 = \text{Hashq}(35)$; $45^2 = 2025$, $35^2 = 1225$

Lösungsvorschlag 4.4:

Eingabezahl	Quadrat	Hashwert
65	4225	22
76	5776	77

Lösungsvorschlag 4.5:

a) Letztlich muss sowieso alles in Binär übersetzt werden, bevor es gehashed wird. Die Website benutzt ein UTF-8 Encoding um sowohl Zahlen als auch Buchstaben in eine Zahlenkette zu übersetzen.

b) Der Output wird im Hexadezimalsystem angezeigt, um weniger Platz zu verwenden als die zehner- oder Binärdarstellung.

c) Die Hashwerte sind sich gar nicht ähnlich, sondern ändern sich vollständig.

Lösungsvorschlag 4.6:

2^{256} verschiedene Hashwerte.

Lösungsvorschlag Abschlussaufgabe 4:

Bspw. Eingabewert „1234“

Ich würde wahrscheinlich 16* Länger brauchen, da die Hexdarstellung 16 mögliche Zeichen hat, wovon nur ein Zeichen die 0 ist. Das geht nicht schneller, da SHA-256 eine kryptographische Hashfunktion ist und sich somit nicht der Eingabewert rückwärts berechnen lässt.

Lösungsvorschlag 5.1:

a) Die Gruppe hat keine klaren Regeln wie sie mit Konflikten in den verschiedenen Hauptbüchern umgehen können.

b) Bspw. wenn zwei Personen eine Transaktion getätigt haben, jedoch vergessen haben, diese den anderen mitzuteilen.

Lösungsvorschlag 5.2:

Bspw. einfacher Konsensmechanismus: Bei Konflikten müssen alle Teilnehmer*innen abstimmen und das Buch mit den meisten Stimmen gilt als valides Hauptbuch.

Lösungsvorschlag 5.3:

~4000 Transaktionen

Lösungsvorschlag 5.4:

Da dies der erste Block ist und dieser somit keinen Vorgängerblock hat. Die Nullen signalisieren den Platzhalter.

Lösungsvorschlag 5.5:

- a) Die Felder „Vorgänger“ und „Hash“ werden aus den anderen Feldern berechnet.
- b) der Block, sowie alle Folgeblöcke werden rot. Der Hashwert des Blocks beginnt jetzt nicht mehr mit genügend Nullen und durch die Änderung ändert sich auch der Hashwert des Folgeblocks usw.
- c) nur Blöcke mit grüner Farbe haben eine valide Nonce.
- d) Siehe Mining Arbeitsheft.

Lösungsvorschlag 5.6:

Beim ausprobieren der Hashwerte, habe ich das gleiche gemacht, was beim Bitcoinmining passiert, nur mit einer anderen Hashfunktion und per Hand.

Lösungsvorschlag 5.7:

- a) Alle Blöcke werden Rot.
- b) Jeden Block neu *minen*, vom ersten Block anfangen.
- c) $16^4 = 65536$

Lösungsvorschlag 5.8:

Wenn alle vier minen: $4 \cdot 40\,000 = 160\,000$

Durchschnittlich: $160\,000 / 65\,000 \approx 2,4 \Rightarrow$ Die Gruppe kann ca. 2-3 Blöcke täglich minen.

Lösungsvorschlag 5.9:

Der Miningerfolg kann nur statistisch angegeben werden und hängt vom Zufall ab. Mit mehr oder weniger *Glück* könnte die Gruppe an bestimmten Tagen auch mehr oder weniger Blöcke minen. Allerdings sind die Zahlen so hoch, dass größere Ausreißer statistisch sehr unwahrscheinlich sind.

Lösungsvorschlag 5.10:

Weil sie dafür jede Seite minen müssten, dafür haben sie jedoch nicht die Ressourcen und Zeit.

Lösungsvorschlag 5.11:

Wenn Anna nun eine Transaktion löscht, müsste sie alle Folgenden Blöcke neu minen. Das kann sie alleine wahrscheinlich nicht bewerkstelligen, zumal das offizielle Hauptbuch in dieser Zeit noch weiterwächst.

Lösungsvorschlag Abschlussaufgabe 5:

Kontrolliert eine Partei mehr als 50% der Rechenleistung des Bitcoin Netzwerks, dann kann diese Partei ihre Rechenleistung so verwenden, dass ihre Blockchain immer schneller wachsen wird als alle anderen Versionen. Damit kann diese Partei sogar ältere Blöcke ändern, da ihre temporär kürzere Blockchain die anderen Versionen nach einer gewissen Zeit wieder einholt.

Lösungsvorschlag 6.1:

a) abhängig von Zeit und Tag, Hashwert sollte mit ca. 20 Nullen beginnen (August 2026)

b) Eine Transaktion von 50 Bitcoin von Coinbase an eine Adresse. Der Hashwert beginnt mit 10 Nullen

Lösungsvorschlag 6.2:

Beispielsweise ~3.149

Die Belohnung für einen Block wird nach 210 000 Blöcken halbiert, somit ca. alle 4 Jahre.

Die Belohnung des aktuellen Blocks liegt leicht über 3.125, da die Miner noch Transaktionskosten bekommen, als Anreiz die entsprechenden Transaktionen in den Block aufzunehmen.

Lösungsvorschlag 6.3:

Das Mining ist aufwändig, aber notwendig für das Weiterbestehen von Bitcoin. Ohne Belohnung ist nicht klar, ob Personen einfach so Ressourcen für das Mining ausgeben.

Lösungsvorschlag 6.4:

a) Deutschland verbrauchte 2025 ca. [500TWH Strom](#), somit wäre dies ca. 1/3 des deutschen jährlichen Stromverbrauchs.

b) Pro Person liegt der Co2 Abdruck in Deutschland bei ca. [10 Tonnen](#), somit wäre das der Co2 Abdruck von ca. 10 Millionen Deutschen Personen.

c) 1.6 km^3 sind ca. 1,6 Billionen Liter (Ein olympisches Schwimmbecken fasst 2.5 Millionen Liter, damit wären das 640 000 olympische Schwimmbecken)

Lösungsvorschlag 6.5:

a) Die Blöcke werden immer schneller gemined.

b) Wenn dann auch mehr leute minen, wird die Anzahl geforderter Nullen steigen.

c) Dadurch wird das Mining insgesamt teurer und verwendet mehr Ressourcen und hätte somit höhere Energiekosten.

Lösungsvorschlag 6.6:

a) $4000 \text{ Transaktionen} / 10 \text{ Minuten} = 400 \text{ T/Min}$; $400 \text{ T/min} / 60 \text{ Sekunden} \approx 6,6 \Rightarrow \text{ca. } 7$ Transaktionen pro Sekunde

b) Für eine Weltweit Nutzbare Währung sind dies sehr wenig Transaktionen. Es könnte ein Bottleneck entstehen, sodass man sehr lange auf seine Transaktion warten muss. Über die Zeit könnten sich immer mehr Transaktionen anstauen.

Lösungsvorschlag 6.8:

a) $1 \text{ Jahr} = 525.600 \text{ Minuten}$; $400 \text{ Transaktionen pro Minute}$
 $\Rightarrow 173 \cdot 10^9 \text{ TWh} / 525.600 \cdot 400 \approx 820 \text{ kwh}$

b) Einpersonenhaushalt in Deutschland verbraucht ca. [2000 kwh Strom pro Jahr](#) $\Rightarrow$ ca. $\frac{1}{2}$ - $\frac{1}{3}$ des Jahresverbrauchs einer Person

c) unter einer [Wattstunde](#).