

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

E.1

Einstiegsaufgabe 1: Schau dir das verlinkte Video an und beantworte die folgenden Fragen.

ALL IN #bitcoin! Aus Überzeugung

<https://www.youtube.com/watch?v=R6gmTuI1Yp0>



1. Was ist die Kernaussage des Videos?

2. Überzeugt dich das intuitiv? Erläutere kurz warum oder warum auch nicht.

Befürworter von Bitcoin argumentieren oft, dass Bitcoin viele Vorteile gegenüber klassischen Währungen habe. In der folgenden Tabelle ist eine Auswahl solcher Behauptungen zusammengestellt.

E.2

Einstiegsaufgabe 2: Vervollständige die Tabelle auf der nächsten Seite. Recherchiere dafür unter anderem im Internet.

Ergänze die Tabelle außerdem um mindestens eine weitere Behauptung, die du bei der Recherche gefunden hast.

Anmerkung: Die letzte Spalte soll dabei vorerst freigelassen werden, diese wird im Verlauf des Arbeitsheftes gefüllt.

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Behauptung	Erklärung: Warum ist das von Vorteil für Bitcoin oder dessen Nutzer*innen? (falls du dir unsicher bist, recherchiere im Internet)	Vorläufige Internetrecherche (maximal 2 Minuten): Wie plausibel wirkt das?	Später auszufüllen: Wie bewertest du diesen Aspekt jetzt?
Bitcoin ist anonym.			
Bitcoin ist schnell.			
Bitcoin ist dezentral.			
<i>Eigene Behauptung</i>			
<i>Eigene Behauptung</i>			

Abschnitt 1: Wem muss ich vertrauen?

Motivation von Bitcoin

1.1

Aufgabe 1.1 Schau einmal kurz auf dein Smartphone und überlege dir, wo deine persönlichen Bilder gespeichert sind: 💡

Hinweis: Wenn du dieses Symbol siehst, bedeutet das, dass es zu dieser Aufgabe Hinweise im Hinweisheft gibt: 💡

1.2

Aufgabe 1.2 Stelle dir vor, ein Cloud-Anbieter, bei dem du deine Fotos gespeichert hast, würde morgen Pleite gehen und müsste seine Server abschalten:

a) Was glaubst du passiert mit deinen Fotos?

(b) Begründe, für wie realistisch du es hältst, dass dein Anbieter morgen Pleite geht und seine Server abschalten muss:

1.3

Aufgabe 1.3 Wähle einen Cloud-Anbieter, den du selbst verwendest und beschreibe, wobei du diesem konkret vertrauen musst und welche Vorteile du durch die Verwendung der Cloud hast:

Ich vertraue _____, dass...

Weil ich folgende Vorteile durch die Verwendung von _____ habe:

Was hat das Ganze jetzt mit Geld und Bitcoin zu tun?

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Ähnlich wie du dem Betreiber einer Cloud für Bilder vertrauen musst, musst du auch bei Zahlungen (insbesondere wenn diese nicht über Bargeld passieren), bestimmten Parteien vertrauen:

1.4

Aufgabe 1.4 Erinner dich, wann du das letzte Mal etwas **ohne** Bargeld bezahlt hast: 💡

Wie hast du dabei bezahlt (bspw. Überweisung, Paypal, GooglePay, ...)?

Vervollständige das Flussdiagramm für deine letzte Zahlung, indem du einzeichnest, über welche Anbieter/Institutionen dein Geld gewandert ist:



1.5

Aufgabe 1.5 Überlege dir, wann du zuletzt eine Bargeld-Transaktion getätigt hast: Welche Vor- bzw. Nachteile hätte es gehabt, wenn du diese Zahlung per Onlinezahlung (oder Überweisung) getätigt hättest? 💡

	Vorteile	Nachteile
Bargeld		
Onlinezahlung/Überweisung		

Onlinezahlungen sind in der Regel nur mit der Beteiligung von Drittparteien möglich. Das Ziel von Bitcoin ist es eine Onlinezahlung zu ermöglichen, bei der ähnlich zum Bargeld auch auf Drittparteien verzichtet wird. Inwiefern dieses Ziel Sinnvoll ist, schauen wir uns in der nächsten Aufgabe an:

📖 Begriff: Dritte Partei/Drittanbieter

Eine Partei/Entität (wie bspw. eine Bank), die bei der Transaktion zwar beteiligt ist, jedoch nicht selbst Sender oder Empfänger ist und neutral vermittelt.

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Beispiel:

Tom möchte ein Buch beim Onlineshop seiner Buchhandlung bestellen. Die Transaktionspartner sind Tom und der Onlineshop, je nachdem welche Zahlungsart er verwendet, sind Parteien wie Paypal, seine Bank und/oder die Bank des Onlineshops Drittparteien bei der Transaktion.

1

Abschlussaufgabe 1:

Auch Bitcoin

Ordne die folgenden Aspekte danach, ob sie einen Vor- oder Nachteil von Drittparteien beschreiben. Begründe jeweils kurz deine Einordnung:

- Käuferschutz
- Datenschutz
- Single point-of-Failure
- AGBs
- vergessen deiner PIN

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.	

Du solltest jetzt wissen, welches Ziel Bitcoin hat und welches Problem es damit lösen möchte. In den nächsten Abschnitten schauen wir uns genauer an, wie Bitcoin dieses Ziel technisch versucht umzusetzen.

Abschnitt 2: Buchhaltung als Währung?

Grundlegende Struktur von Bitcoin

Im Verlauf des Arbeitshefts werden wir verschiedene Eigenschaften von Bitcoin erst anhand eines fiktiven Szenarios darstellen, bevor wir uns anschauen, wie diese bei Bitcoin funktionieren:

Vier Freund*innen – Anna, Lukas, Sara und Tom – verbringen ein Wochenende in einer Selbstversorgerhütte. Sie wollen, dass die anfallende Hausarbeit fair verteilt wird. Dafür überlegen sie sich folgendes System: Die **Hüttenpunkte**. Jede*r startet mit 10 Hüttenpunkten und kann diese für kleinere Gefallen (wie Bspw. Abwasch machen, Aufräumen, Kochen, ...) an andere geben. Festgehalten werden die Punkte in einem Buch, welches im Wohnzimmer über dem Kamin aufbewahrt wird. Am letzten Tag sieht das Buch wie folgt aus:

#	Von	An	HP
00	Anna, Lukas, Sara und Tom bekommen jeweils 10 Hüttenpunkte (HP)		
01	Anna	Lukas	4
02	Lukas	Sara	6
03	Sara	Tom	2
04	Anna	Tom	5
05	Anna	Sara	1
06	Tom	Lukas	12

Beispielsweise könnte folgendes geschehen sein:

- Lukas kochte Mittagessen für Anna und bekam dafür 4 Punkte von Anna usw.

Begriff: Hauptbuch/Ledger

Den Ort, an dem die Liste an Transaktionen festgehalten wird, nennen wir **Hauptbuch**. Im Englischen wird meist der Begriff „**Ledger**“ verwendet.

2.1

Aufgabe 2.1: Wie viele Hüttenpunkte haben Anna und Tom jeweils nach Transaktion 06?

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

2.2

Aufgabe 2.2: Warum muss der Gesamtpunktestand der Teilnehmer*innen nicht zusätzlich aufgeschrieben werden?

2.3

Aufgabe 2.3: Anna möchte nun Tom 4 Punkte dafür bezahlen, dass er ihren Abwasch macht. Welches Problem entsteht dabei? 💡

2.4

Aufgabe 2.4: Beurteile für wie sicher du das aktuelle System hältst. Ist es möglich für Teilnehmer*innen zu betrügen? 💡

Erinerrung: Wie wird das Buch aufbewahrt?

2.5

Aufgabe 2.5: Als erste Sicherheitsmaßnahme führt die Gruppe Unterschriften ein. Bei jeder Transaktion muss die Person, welche die Punkte abgibt, die Transaktion unterschreiben. Wie könnte ein*e Teilnehmer*in jetzt noch betrügen? (wir gehen davon aus, dass die Unterschriften nicht gefälscht werden können.) 💡

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

2.6

Aufgabe 2.6: Um das System noch sicherer zu machen haben sie zwei Vorschläge, die sie in Kombination mit den Unterschriften verwenden könnten. Beurteile die einzelnen Vorschläge und trage Vor- und Nachteile der Vorschläge in die Tabelle ein. 💡

Vorschlag	Vorteile	Nachteile
Tom wird der neue Hüttenpunkt- wächter. Er verwaltet das Hauptbuch in seinem Zim- mer und Transaktionen wer- den nur von Tom in das Buch geschrieben.		
Das Hauptbuch wird dreimal kopiert, sodass es nun vier gleichwertige Kopien des Hauptbuchs gibt. Jede*r Teil- nehmer*in erhält nun eine gleichwertige Kopie des Hauptbuches. Transaktionen müssen ab nun allen Teilneh- mer*innen mitgeteilt werden, damit diese kopiert werden können.		

2.7

2.7: Die beiden Strategien unterscheiden sich dadurch, dass das Hauptbuch in einem Fall zentral (von Tom) und im anderen Fall dezentral (von allen) verwaltet wird. Wie steht dies in Verbindung zum Konzept des Vertrauens aus Abschnitt 1? 💡

2.8

2.8: Gehe zurück zur Tabelle aus E.2 und fülle die letzte Spalte zum Aspekt der Dezentralität aus, soweit du kannst.

2

Abschlussaufgabe 2: Bisher haben wir das Prinzip der Buchhaltung am Beispiel der Hüttenpunkte betrachtet. Bitcoins Grundidee basiert genau wie die Hüttenpunkte auf dem Prinzip der Buchhaltung. Recherchiere die zentralen Unterschiede von Bitcoin zu folgenden Konzepten der Hüttenpunkte:

Anmerkung: Es ist völlig ausreichend, ein Schlagwort zu finden und kurz die Idee zu erklären, du musst noch nicht im Detail verstanden haben, wie Bitcoin funktioniert. 💡

	Hüttenpunkte	Bitcoin
Wie wird unter-schrieben?	Die bezahlende Person unter-schreibt eine Transaktion physisch im Hauptbuch.	
Wie wird das Hauptbuch ge-speichert?	Als physisches Buch entweder bei Tom als Hüttenpunktwächter, oder indem jede*r Teilnehmer*in eine eigene Kopie bekommt (Je nach Vorschlag aus 2.6)	

Du solltest jetzt das Prinzip der Buchhaltung und somit die Grundidee von Bitcoin verstanden haben. In den folgenden Kapiteln verwenden wir die Idee der Hüttenpunkte und erweitern diese, um die Besonderheiten von Bitcoin aufzunehmen.

Abschnitt 3: Wie anonym ist Bitcoin?

Anonymität

Angenommen, die Freundesgruppe aus Abschnitt 2 ist jetzt aus dem Urlaub zurückgekommen und entscheidet sich dazu, das System der Hüttenpunkte weiter zu verwenden. Außerdem wollen sie es weiteren Freund*innen erlauben in ihr System einzusteigen.

Allerdings gibt es im erweiterten Freundeskreis mit Sven auch eine Person, die immer genau wissen möchte, wer wann etwas macht und auch schnell eifersüchtig wird, wenn ohne ihn etwas unternommen wird. Um Sven mit dem öffentlichen Buch aller Transaktionen nicht noch mehr Futter zur Überwachung zu geben, entscheidet die Freundesgruppe sich dazu Pseudonyme zu verwenden.

3.1

Aufgabe 3.1:

Für wie sinnvoll hältst du die Maßnahme Pseudonyme zu verwenden?

Die Gruppe hat ihr Hauptbuch nun mit Pseudonymen überarbeitet und die aktuelle Version sieht damit wie folgt aus:

#	Von	An	HP
00	Krümelmonster, Elmo, Oskar und Bert bekommen jeweils 10 Hüttenpunkte (HP)		
01	Krümelmonster	Elmo	4
02	Elmo	Oskar	6
03	Oskar	Bert	2
04	Krümelmonster	Bert	5
05	Krümelmonster	Oskar	1
06	Bert	Elmo	12

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

3.2

Aufgabe 3.2: Tom hat nun einen Freund Timon, der auch gerne mitmachen möchte. Timon ist auch bereit zwei Euro für seine zwei ersten Hüttenpunkte zu bezahlen. Wie könnte Timon an seine ersten Hüttenpunkte kommen (wie macht er das ganz konkret, mit wem muss er reden etc.)? Trage die nötige(n) Transaktion(en) in die Tabelle ein.

Wir gehen außerdem davon aus, dass die Gruppe sich darauf geeinigt hat, **keine neuen Hüttenpunkte** zu erschaffen. 💡

Erinerrung: Vergiss nicht, dass auch Timon nicht mit seinem Klarnamen im Hauptbuch auftauchen möchte.

3.3

Aufgabe 3.3:

Inwiefern wurde durch Timons Beitritt die Anonymität einiger Pseudonyme gefährdet? 💡

3.4

Aufgabe 3.4:

Bitcoin verwendet ein ähnliches System wie die Pseudonyme der Hüttenpunkte. Vervollständige die Tabelle auf der nächsten Seite, indem du kurz zu den beschriebenen Unterschieden recherchierst: 💡

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

	Hüttenpunkte	Bitcoin
Wie werden die Einträge anonymisiert?	Teilnehmer*innen erscheinen nicht mit Klarnamen, sondern mit Pseudonymen.	
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>

3.5

Aufgabe 3.5:

Schaue dir deine Ergebnisse dazu an, wie du deine ersten Bitcoin erwerben könntest: Inwiefern sind Transaktionen, die du jetzt mit deinen gekauften Bitcoin tätigst, wirklich anonym? Wer könnte deine Personendaten deinem „Pseudonym“ (Also der digitalen Signatur) zuordnen?

3.6

Aufgabe 3.6:

Wie unterscheidet sich die Privatsphäre deiner Transaktion, wenn du stattdessen eine klassische Bank für deine Transaktion verwendest? 💡

3

Abschlussaufgabe 3:

Gehe zurück zur Tabelle aus E.2 und fülle die letzte Spalte zum Aspekt der Anonymität aus.

Du solltest jetzt verstanden haben, wie das Prinzip eines Hauptbuchs mit der Anonymität von Transaktionen zusammenhängt. In den nächsten Abschnitten widmen wir uns einigen technischen Grundlagen, damit wir die eigentlich besondere Idee von Bitcoin erklären können.

Abschnitt 4: Technische Grundlage: Kryptographische Hashfunktionen

Grundlage für Abschnitt 5

In den nächsten zwei Abschnitten soll es darum gehen, wie Bitcoin technisch die Idee des dezentralen Hauptbuches umsetzt, sodass keiner Drittpartei vertraut werden muss.

Um den Mechanismus dafür zu erklären, brauchen wir jedoch ein wenig Vorwissen zum Thema kryptographische Hashfunktionen:

Begriff: Hashfunktion

Eine Hashfunktion nimmt einen beliebigen Eingabewert und berechnet daraus einen Wert aus einem festen Wertebereich (Bspw. könnte das Ergebnis immer zwei Ziffern haben). Dabei ergibt die gleiche Eingabe immer das gleiche Ergebnis.

Bevor wir uns mit der komplexeren Hashfunktion beschäftigen, die von Bitcoin verwendet wird, betrachten wir folgende einfachere Hashfunktion:

Hashfunktion Beispiel: Die Quadrat-Mitte-Methode

Berechnung:

1. Nehme die Eingabezahl und berechne ihr **Quadrat**.
2. Hat das Quadrat eine **gerade** Anzahl von Ziffern: nimm die **beiden mittleren Ziffern** als Hash.
3. Hat das Quadrat eine **ungerade** Anzahl von Ziffern: nimm die **mittlere Ziffer + die Ziffer links davon** als Hash.

Diese Funktion nennen wir im Folgenden Hashq().

Visualisierung — die markierten Ziffern ergeben den Hash:

Eingabezahl 57: $57^2 = 3[24]9 \rightarrow \text{Hashq}(57) = 24$

Eingabezahl 23: $23^2 = [52]9 \rightarrow \text{Hashq}(23) = 52$

Anmerkung: Zur Vereinfachung gehen wir davon aus, dass die Eingabezahl größer als 3 ist.

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

4.1

Aufgabe 4.1 Begründe, weshalb die Eingabezahl größer als 3 sein sollte.

4.2

Aufgabe 4.2 Berechne den Hash der folgenden Zahlen mit der Quadrat-Mitte-Methode.

Eingabezahl	Quadrat	Hashwert
42		
99		
13		

4.3

Aufgabe 4.3 Können zwei Zahlen den gleichen Hashwert besitzen? Finde ein Beispiel:

4.4

Aufgabe 4.4 Berechne eine mögliche Eingabezahl, sodass der Hashwert passend ist.

Eingabezahl	Quadrat	Hashwert
		22
		77

Beschreibe stichpunktartig, wie du vorgegangen bist:

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Bitcoin verwendet die Hashfunktion „SHA-256“, welche eine kryptographische Hashfunktion ist. Genau wie die *Quadrat-Mitte-Methode*, bekommt auch *SHA-256* eine beliebig lange Eingabezahl. Wie genau SHA-256 daraus dann den Hashwert berechnet müssen wir nicht genau nachvollziehen. Die Berechnung ist so komplex, dass die Berechnung eines einzigen Hashwerts schriftlich mehrere Seiten in Anspruch nehmen würde.

Begriff: Kryptographische Hashfunktion

Eine kryptographische Hashfunktion ist eine besondere Art von Hashfunktion. Um Bitcoin zu verstehen, reicht es für uns zu wissen, dass es bei einer kryptographischen Hashfunktion unmöglich ist, aus einem Hashwert eine passende Eingabezahl zu berechnen, ohne einfach alle Möglichkeiten auszuprobieren.

Begriff: SHA-256

Eine kryptographische Hashfunktion, welche 2001 von der amerikanischen National Security Agency (NSA) veröffentlicht wurde. Die 256 steht dafür, dass der berechnete Hashwert immer genau 256 Bit lang ist.

4.5

Aufgabe 4.5 Folgendes Onlinetool kann für dich SHA-256 Hashwerte Berechnen:
<https://emn178.github.io/online-tools/sha256.html>

Probiere einige Berechnungen aus und beantworte folgende Fragen: 💡

a) Dir ist wahrscheinlich aufgefallen, dass nicht nur Zahlen, sondern auch Texte als Eingabe verwendet werden können. Wieso geht das?

b) Warum sind in der Ausgabe(Output) Buchstaben und Zahlen gemischt?

c) Was fällt dir auf, wenn du für zwei sehr ähnliche Eingabewerte die Hashwerte berechnen lässt?
(Bspw. „Informatik“ und „informatik“)

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

4.6

Aufgabe 4.6 SHA-256 ist eine kryptographische Hashfunktion, daher ist es nur durch Ausprobieren möglich einen Eingabewert zu finden, der einen gegebenen Hashwert erzeugt.

Wie viele mögliche verschiedene Hashwerte können dabei durch die 256 Bit erzeugt werden? 💡

4

Abschlussaufgabe 4: Benutzt das Onlinetool, um einen Eingabewert zu finden, dessen Hashwert mit einer Null beginnt.

Eingabewert:

Wie viel länger würdest du wahrscheinlich brauchen, um einen Eingabewert zu finden, dessen Hashwert mit zwei Nullen beginnt und wieso geht das nicht schneller?

Du solltest jetzt verstanden haben, was eine Hashfunktion ist und dass es bei kryptographischen Hashfunktionen nicht möglich ist effizient, den Eingabewert eines zugehörigen Hashwerts zu berechnen. Die einzige Möglichkeit bleibt das Ausprobieren. Im nächsten Abschnitt benutzen wir dieses Wissen um Bitcoins technische Innovation zu erklären.

Abschnitt 5: Technische Grundlage: Proof-of-work

Was Bitcoin so besonders macht

*Die Freundesgruppe hat sich nun dazu entschieden, dass jede*r Teilnehmer*in eine Kopie des Hauptbuches erhält:*

Aufgabe 5.1:

5.1

Stell dir nun vor, Anna (Krümelmonster im Hauptbuch) möchte, dass Tom (Bert im Hauptbuch) für sie den Abwasch macht und Tom dafür 4 HP geben. Laut Toms Hauptbuch hat Anna (Krümelmonster) jedoch gar keine Hüttenpunkte mehr die sie ausgeben könnte.

Anna hat jedoch in ihrem Hauptbuch heimlich die Transaktionen gelöscht, bei denen sie Hüttenpunkte bezahlt hat und hat in ihrem Hauptbuch damit 10 HP.

a)

Beschreibe das entstehende Problem:

b) Fällt dir eine weitere Situation ein, in der die Regelung mit den Kopien problematisch ist?

5.2

Aufgabe 5.2: Solche Situationen bilden die Kernproblematik, die dabei entsteht, wenn das Hauptbuch dezentral gespeichert wird. Fallen dir eigene Vorschläge ein, wie die Gruppe mit der Problematik umgehen kann?

In diesem Abschnitt geht es darum, genau dieses Problem der dezentralen Speicherung zu lösen: Wie schaffen wir es, dass das Hauptbuch auf der einen Seite nicht zentral von einer Drittpartei (Bspw. Tom als Hüttenpunktwächter) gespeichert wird, auf der anderen Seite jedoch sichergestellt wird, dass nicht komplett verschiedene Versionen des Hauptbuchs entstehen? Die grundlegende Idee ist hierfür der sogenannte Proof-of-Work.

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Konzept: Proof-of-work Idee

Sollte es mehrere unterschiedliche Versionen des Hauptbuchs geben, dann ist das Hauptbuch gültig, in welchem die meiste Arbeit (Rechenleistung) steckt. Der Proof-of-Work bietet einen Mechanismus, zu beweisen, dass in einem Hauptbuch viel Arbeit bzw. Rechenleistung steckt.

Zu verstehen, wie das funktioniert und was genau mit der Arbeit bzw. Rechenleistung gemeint ist, ist das Ziel dieses Abschnitts.

Für den Proof-of-work Mechanismus gibt es kein einfaches Gegenstück wie beispielsweise die Pseudonyme aus Abschnitt 3 für die Walletadressen, welches die Gruppe sinnvoll in ihrem physischen Hauptbuch verwenden kann. Daher erweitern wir das Hauptbuch der Hüttenpunkte um den gleichen Mechanismus den auch Bitcoin benutzt. Das führt allerdings dazu, dass die Freundesgruppe mit unrealistisch hohen Zahlen komplexe Rechnungen anstellen muss. Für unser Beispiel gehen wir davon aus, dass sie damit kein Problem haben:

*Die erste Änderung besteht darin, dass nun nicht alle Transaktionen in ein Buch geschrieben werden, sondern die Transaktionen in Blöcke aufgeteilt werden. Die Freundesgruppe entscheidet sich dafür, dass jeder Block maximal zwei Transaktionen enthält. Du kannst dir die Blöcke vorstellen wie einzelne Seiten Papier. Durch die Aufteilung in Blöcke hat sich erstmal noch nicht viel verändert: Jeder Teilnehmer*in hat jetzt zwar kein Buch mehr, aber dafür eine Menge von Seiten, die gemeinsam das Buch ergeben.*

Damit besteht das Hauptbuch aus Abschnitt 2, aus vier Blöcken wie folgt:

Hauptbuch Hüttenpunkte Block #1

#	Von	An	HP
00	Krümelmonster, Elmo, Oskar und Bert bekommen jeweils 10 Hüttenpunkte (HP)		
01	Krümelmonster	Elmo	4

Hauptbuch Hüttenpunkte Block #2

#	Von	An	HP
02	Elmo	Oskar	6
03	Oskar	Bert	2

Hauptbuch Hüttenpunkte Block #3

#	Von	An	HP
04	Krümelmonster	Bert	5
05	Krümelmonster	Oskar	1

Hauptbuch Hüttenpunkte Block #4

#	Von	An	HP
06	Bert	Elmo	12

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

5.3

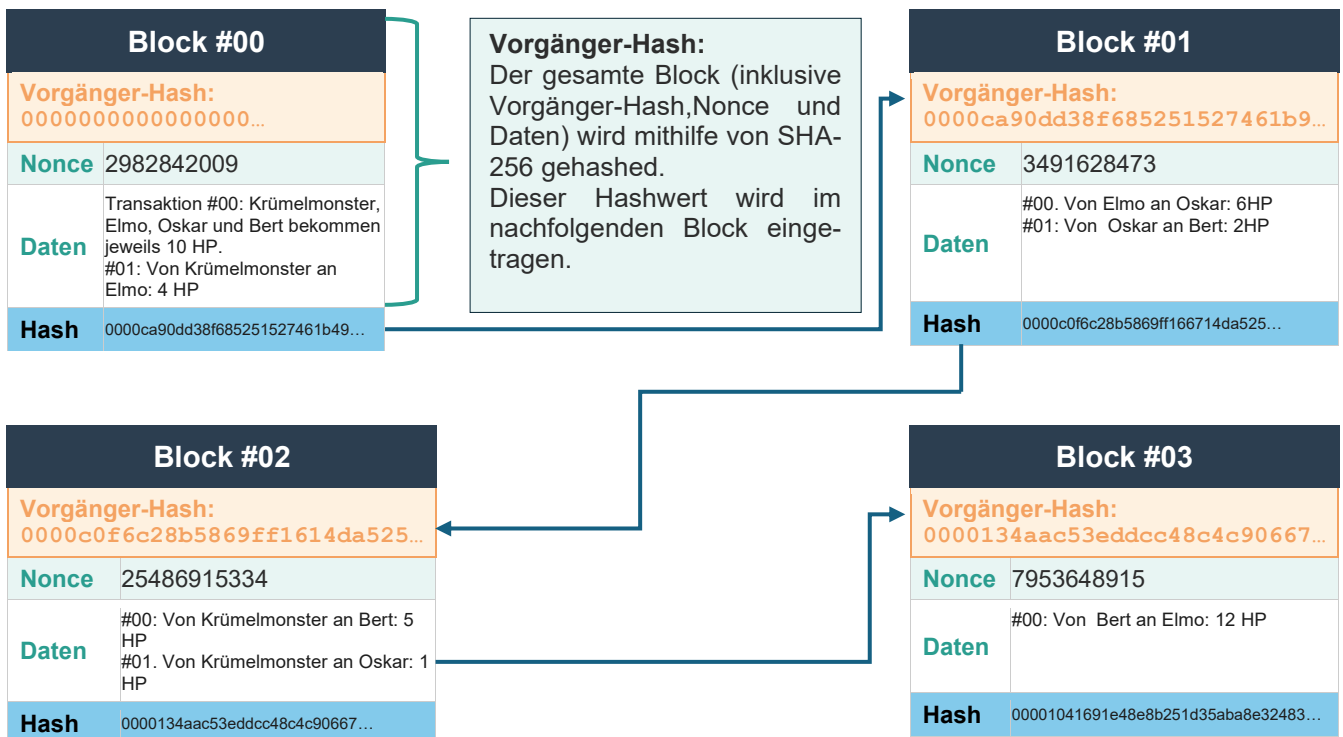
Aufgabe 5.3: Die Anzahl der Transaktionen pro Block muss nicht wie in unserem Beispiel zwei sein. Recherchiere, wie viele Transaktionen ungefähr in einen Bitcoin Block passen:

Diese Aufteilung löst allerdings noch nicht das Problem, wie die Seiten/Blöcke jetzt so gespeichert werden, dass dabei keiner Drittpartei vertraut werden muss.

Dafür strukturiert die Freundesgruppe um, was auf einer Seite/Block von Transaktionen alles stehen muss.

jede Seite/Block muss von nun an die Folgenden Einträge haben:

- Der Hash des vorherigen Blocks (Siehe Abbildung).
- Die Transaktionen (Maximal zwei Transaktionen pro Seite).
- Die Nonce (Was das genau ist, betrachten wir später).



Begriff: Blockchain

Die entstehende Kette von Blöcken nennen wir Blockchain (Übersetzt: Blockkette).

5.4

Aufgabe 5.4: Warum ist bei Block #00 der Wert des Vorgänger-Hashes „0000...“?

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Wie bereits angesprochen, ist es das Ziel, irgendwie zu beweisen, wie viel Arbeit in einem Hauptbuch (bzw. einer Blockchain) steckt. Dafür verwenden wir die Nonce:

Begriff: Nonce

Die Nonce ist ein frei veränderbarer Wert, der keinen Unterschied für den Block macht, abgesehen davon, dass er den resultierenden Hashwert des Blocks verändert.

*Nun führt die Gruppe eine zusätzliche Regel ein: **Dass Seiten/Blöcke nur dann gültig sind, wenn ihr Hashwert mit vier Nullen beginnt.***

5.5

Aufgabe 5.5: Öffne die folgende Webseite und beantworte die Fragen **a-d**:
<https://andersbrownworth.com/blockchain/blockchain>

a) Warum kannst du bei jedem Block lediglich die Nonce und die Daten verändern, nicht jedoch die Felder „Vorgänger“ und „Hash“?

b) Was passiert mit den Feldern „Vorgänger“ und „Hash“, wenn du die Nonce oder die Daten veränderst? Welche anderen Blöcke werden auch beeinflusst und warum?

c) Als du die Daten verändert hast, haben wahrscheinlich einige Blöcke ihre Farbe geändert. Erläutere was die Farbe der Blöcke signalisiert.
(**Hinweis:** Achte darauf, was sich außer der Farbe verändert, wenn du auf „Mine“ klickst. Was könnte das mit der Farbe zu tun haben?)

d) Übertrage einige der Transaktionen aus dem Hüttenpunkte Beispiel auf die Webseite und drücke die Schaltfläche „Mine“. Beschreibe in eigenen Worten was hierbei passiert. (Die Auflösung ist auf der nächsten Seite).

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

Was du gerade ausprobiert hast, ist das sogenannte „Mining“:

Begriff: Mining

Das Herausfinden einer passenden Nonce, sodass der entstehende Block einen SHA-256 Hashwert besitzt, welcher mit vier Nullen (In unserem Beispiel vier, bei Bitcoin ist diese Zahl später anders) beginnt.

5.6

Aufgabe 5.6: Was hat das Mining mit der Abschlusssaufgabe des letzten Abschnitts(Abschlusssaufgabe 4) zu tun?

5.7

Aufgabe 5.7: Trage die ersten sieben Transaktionen der Hüttenpunkte in die ersten vier Blöcke der Blockchain Simulation ein (<https://andersbrownworth.com/blockchain/blockchain>).

a) Was passiert jetzt, wenn du im ersten Block eine Transaktion veränderst?

b) Was musst du tun, damit wieder alle Blöcke die Regel erfüllen?

c) Blöcke werden genau dann gültig, wenn der Hashwert mit vier Nullen beginnt. Wie viele Hashwerte müssen dafür im Durchschnitt ausprobiert werden?

Erinnern wir uns jetzt zurück an Anna am Anfang des Kapitels: „*Anna hat jedoch in ihrem Hauptbuch heimlich die Transaktionen gelöscht, bei denen sie Hüttenpunkte bezahlt hat und hat in ihrem Hauptbuch damit 10 HP.*“

Wieso wird es nun mit den neuen Regeln zu den **Hashwerten** und **Noncen** schwerer für Anna, bestimmte Transaktionen aus ihrem Hauptbuch zu löschen?

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

*Unsere Analogie zu Bitcoin fällt hier ein bisschen zusammen, da der Rechenaufwand, selbst einen einzigen SHA-256 Hash zu berechnen, für Menschen schlichtweg zu hoch ist. In der Realität funktioniert das durch Computerprogramme. Um die Idee bildlich zu veranschaulichen, stellen wir uns trotzdem vor, die Teilnehmer*innen könnten diesen absurden Rechenaufwand leisten:*

Im Durchschnitt müssen pro Block ca. 65000 verschiedene Noncen ausprobiert werden (5.7c).

*Stellen wir uns trotz der realen Probleme einfach vor, dass jede*r Teilnehmer*in am Tag ca. 40000 Noncen ausprobieren kann.*

5.8

Aufgabe 5.8: Wie viele neue Seiten könnte die Freundesgruppe um Anna, Lukas, Sarah und Tom im Durchschnitt pro Tag mit diesen Annahmen verifizieren/minen?

5.9

Aufgabe 5.9: Warum kann hier nur ein Durchschnittswert angegeben werden?

*Das Ziel der Gruppe war es ursprünglich, dass es kein zentrales Hauptbuch mehr gibt, sondern dieses dezentral gespeichert werden kann (indem jede*r Teilnehmer*in eine Kopie besitzt). Um zu klären, welche Version des Hauptbuchs, als richtige zählt stellen sie nun folgende Regel auf:*

„Das Hauptbuch, welches am meisten Seiten hat, ist das legitime Hauptbuch der Hüttenpunkte.“

5.10

Aufgabe 5.10: Wieso können Teilnehmer*innen nicht einfach ein möglichst langes (viele Seiten) Hauptbuch mit Transaktionen ihrer Wahl erstellen?

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

5.11

Aufgabe 5.11: Erinnere dich an die Situation aus 5.1 a) zurück: Anna hat versucht einfach alle Transaktionen, in denen sie (als Krümelmonster), HP ausgegeben hat in ihrem Hauptbuch zu löschen. Erläutere, warum Anna nun nicht mehr so leicht vergangene Transaktionen ändern/löschen kann:

Damit hast du die Grundlegende Idee von Bitcoin verstanden: Wenn es aufwändig genug ist, einen Block zu verifizieren (weil das Mining viel Zeit und Rechenleistung braucht), dann kann ein früherer Block nicht einfach *gefälscht* werden, da dadurch auch alle folgenden Blöcke neu verifiziert werden müssten. Wenn ein Block also genügend Folgeblöcke hat, kannst du dir ziemlich sicher sein, dass niemand diesen Block mehr ändern kann.

5

Abschlussaufgabe 5: Ein bekannter Angriff, auf das Bitcoin System ist der sogenannte 51%-Angriff.

a) Stelle Vermutungen auf, was mit einem 51%-Angriff gemeint sein könnte:

b) Recherchiere im Internet und überprüfe deine Vermutung aus **a)**. Erläutere, wie ein 51%-Angriff funktioniert:

Dieser Abschnitt war der technisch anspruchsvollste Abschnitt des Arbeitshefts. Du solltest verstanden haben, wie Bitcoins Proof-of-work Idee funktioniert und welches Problem dadurch gelöst wird. Insbesondere solltest du verstanden haben, wieso ein Eintrag in der Blockchain nicht mehr im Nachhinein verändert werden kann.

Im nächsten Abschnitt betrachten wir eine negative Seite der Proof-of-work Idee, von der du vielleicht bereits gehört hast:

Die mit dem Mining verbundenen hohen Energiekosten.

Abschnitt 6: Mining

und die Kosten für unseren Planeten

6.1

Aufgabe 6.1: Auf der folgenden Webseite kannst du dir alle Blöcke der Bitcoin Blockchain anschauen: <https://btcscan.org/blocks/recent>

a) Welche Nummer hat der aktuelle Block? Mit wie vielen Nullen beginnt der Hashwert des Blocks?

b) Suche nach dem allerersten Block (auch **Genesis Block** genannt). Welche Transaktionen findest du in diesem Block und mit wie vielen Nullen beginnt der Hashwert des Blocks?

Begriff: Mining-Reward

Was du hier gefunden hast, ist der Mining-Reward, oder die Belohnung für das Mining, also das Finden der richtigen Nonce.

6.2

Aufgabe 6.2: Wie hoch war die Blockbelohnung im aktuellsten Block?

 **Hinweis:** „Coinbase“ ist nicht nur der Name eines Kryptoanbieters, sondern auch der Name für die Herkunft der Blockbelohnungen im Bitcoin Protokoll (der Anbieter hat sich hiernach benannt).

b) Recherchiere warum sich diese Belohnung von der des Genesisblocks unterscheidet und wie zukünftige Blockbelohnungen aussehen werden:

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

c) Recherchiere warum die Belohnung des neusten Blocks wahrscheinlich nicht genau 3.125 BTC beträgt:

6.3

Aufgabe 6.3: Erläutere wieso eine Belohnung für das Mining notwendig ist:

Um Bitcoins zu minen müssen möglichst viele Noncen ausprobiert und der SHA-256 Hashwert jeweils neu berechnet werden. Dabei wird viel Rechenleistung verwendet:

6.4

Aufgabe 6.4: Während 2020-2021 verbrauchte Bitcoin Mining ca. 173 Terrawattstunden an Strom. Dabei wurden ca. 86 Megatonnen Co2 und 1.65 km^3 Wasser verbraucht. Recherchiere zu diesen Mengenangaben und finde Vergleiche (Bspw. entspricht eine Stunde Fernsehen (je nach Fernseher) ca. 0.1 Kilowattstunden):

a) 173 Terrawattstunden Strom (173 TWh) entsprechen:

b) 86 Megatonnen Co2 entsprechen:

c) 1.65 km^3 Wasser entsprechen:

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

6.5

Aufgabe 6.5: In Aufgabe 6.1 hast du herausgefunden, dass der Genesisblock und der aktuellste Bitcoinblock unterschiedlich viele Nullen zu Beginn ihres Hashwertes hatten. Dies liegt daran, dass das Bitcoin Protokoll vorsieht, dass ein neuer Block ca. alle 10 Minuten „gemined“ wird. Je nachdem wie viele Miner momentan versuchen einen Block zu minen/lösen wird die benötigte Anzahl an Nullen erhöht bzw. verringert.

a) Erläutere was das Problem wäre, wenn Bitcoin bei der geforderten Anzahl von Nullen des Genesisblocks geblieben wäre:

b) Erläutere wie sich die Anzahl an geforderten Nullen verändern werden, wenn Bitcoin an Popularität gewinnt:

c) Erläutere welchen Einfluss dies auf die Energiekosten von Bitcoin haben wird:

6.6

Aufgabe 6.6: Da durchschnittlich ein Block (mit ca. 4000 Transaktionen) alle 10 Minuten gemined wird, ist die Anzahl der Transaktionen limitiert. Zum Vergleich: VISA kann ca. 65000 Transaktionen pro **Sekunde** durchführen

a) Wie viele Transaktionen pro Sekunde können über Bitcoin durchgeführt werden?

b) Erläutere inwiefern das problematisch ist:

6.7

Aufgabe 6.7: Gehe zurück zur Tabelle aus E.2 und fülle die letzte Spalte zum Aspekt der Schnelligkeit aus.

Bitcoin, die Währung der Zukunft? ₿

Blockchain — Arbeitsheft

6.8

Aufgabe 6.8: Du kennst den jährlichen Stromverbrauch von Bitcoin: ca. 173 Terawattstunden und weißt, dass ca. alle 10 Minuten 4000 Transaktionen durchgeführt werden:

a) Berechne, wie hoch dann der Stromverbrauch für eine einzelne Transaktion ungefähr ist:

b) Das entspricht folgendem Vergleichswert aus dem alltäglichen Leben:

c) Recherchiere, wie hoch stattdessen die Stromkosten einer klassischen Onlinezahlung/Überweisung sind (Bspw. VISA oder Paypal):

6

Abschlussaufgabe 6: Nach allem, was du bisher über Bitcoin gelernt hast: Gehe zurück zur Tabelle aus E.2 und schaue welche freien Felder der letzten Spalte du mit deinem jetzigen Wissen noch ausfüllen kannst.

Bewerte danach, inwiefern du die Energiekosten von Bitcoin gerechtfertigt findest. Nimm dabei Bezug auf die Aspekte der Tabelle aus E.2.

i Zusammenfassung: In diesem Arbeitsheft hast du gelernt, wie Bitcoin technisch funktioniert, inwiefern es überhaupt sinnvoll ist, wie es in der realen Welt angewendet wird, und hast dir Gedanken darüber gemacht, inwiefern wir Bitcoin aufgrund der hohen Ressourcenkosten überhaupt verwenden sollten.

Ausblick: Bitcoin ist hier allerdings nur ein Beispiel für verschiedene Technologien, die auf der Idee der Blockchain basieren. Meist sind dies andere Kryptowährungen, es gibt jedoch auch andere Gebiete, in denen die Blockchain-Technologie verwendet wurde (Bspw. NFTs). Das in diesem Arbeitsheft erlernte Grundprinzip bleibt jedoch bei all diesen Technologien sehr ähnlich.