TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

anderes logo

Technische Universität
Kaiserslautern
Fachbereich Mathematik

Masterarbeit
Im Studiengang Master of Education

Cryptowährungen

Und deren Einsatz im schulischen Kontext

Cryptocurrencies

And their Deployment in a School Environment

Autor:
Marcel Schütz

Erstgutachter:	Prof. Dr. Claus Fieker
Zweitgutachter:	StD Thilo Vollrath
Prüfungssemester:	Sommersemester 2019
Prüfungszeitraum:	XX.03.2019 bis 02.09.2019

Zusammenfassung

Die mediale Präsenz von Kryptowährungen hat im letzten Jahrzehnt stark zugenommen. Trotzdem besitzen viele, auch jüngere Generationen, nicht das Wissen über die Funktionsweise der elektronischen Währungen. Um einen sicheren Umgang mit der Thematik, sowie die Bildung einer eigenen, fundierten Meinung zu fördern, werden im ersten Teil dieser Arbeit fachliche Grundlagen verschiedener Arten von Kryptowährungen untersucht. Im Zuge dessen wird ein allgemeines Grundgerüst der für Central Authority eCash benutzten algebraischen Strukturen vorgestellt, welches sich durch einen hohen Grad an Individualisierbarkeit auszeichnet. Im zweiten, didaktischen Teil dieses Werks wird die Frage nach der Umsetzbarkeit dieser Thematik in einem schulischen Kontext durch eine vollständig geplante, durchgeführte und reflektierte Unterrichtseinheit erörtert.

Abstract

Media presence of crypto currencies has increased strongly in the last decade. Nevertheless, many, even younger generations, do not possess knowledge about the functionality of electronic currencies. In order to promote a safe handling of the topic, as well as the formation of an own, founded opinion, in the first part of this work the basic principles of different types of crypto currencies are examined. In the course of this, a general, basic, yet customizable framework of algebraic structures used in Central Authority eCash systems is presented. In the second, didactic part of this work the question regarding this topic's feasibility in a school environment is discussed by presenting a fully planned, executed and reflected teaching unit.

Inhaltsverzeichnis

1 Fachliche Grundlagen **1**
- 1.1 Algebraische Grundlagen . . . 1
  - 1.1.1 Elliptische Kurven . . . 2
  - 1.1.2 Der diskrete Logarithmus . . . 6
- 1.2 Informatische Grundlagen . . . 7
  - 1.2.1 Merkle Bäume . . . 8

2 Kryptowährungen **11**
- 2.1 Ziele von Kryptowährungen . . . 11
- 2.2 Central Authority eCash . . . 12
  - 2.2.1 Hauptanwendungen des Systems . . . 14
  - 2.2.2 Implementationen des CA-Systems . . . 18
- 2.3 Peer-to-peer eCash . . . 24

3 Vereinfachte Kryptowährungen **29**
- 3.1 Erste Iteration des Systems . . . 29
  - 3.1.1 Hauptanwendungen des Systems . . . 30
- 3.2 Analyse der Schwachpunkte . . . 31

4 Didaktischer Teil **33**
- 4.1 Die Modellierungstage 2019 . . . 33
- 4.2 Verlaufsplan . . . 34
- 4.3 Lernziele . . . 36
- 4.4 Besondere Voraussetzungen . . . 37
- 4.5 Eigene Voraussetzungen . . . 38
- 4.6 Fachwissenschaftliche Bemerkungen . . . 38
- 4.7 Didaktische Analyse . . . 39
  - 4.7.1 Einordnung in den Lehrplan . . . 39
  - 4.7.2 Fachliche Voraussetzungen des Kurses . . . 41
  - 4.7.3 Begründung und Bedeutung des Lerngegenstands . . . 42
  - 4.7.4 Unterrichtsverfahren . . . 43
  - 4.7.5 Didaktische Konzeption . . . 44
  - 4.7.6 Methodische Überlegungen . . . 47
- 4.8 Reflexion der Lerneinheit . . . 50
  - 4.8.1 Reflexion der Vorstellungspräsentation . . . 50
  - 4.8.2 Reflexion der interaktiven Einführungspräsentation . . . 50
  - 4.8.3 Reflexion der Projektarbeit . . . 52
- 4.9 Feedback . . . 53

5 Fazit **55**

6 Danksagung **57**

7 Anhang **59**
7.1 Handout Modellierungstage 59
7.2 Skript Modellierungstage 61
7.3 Präsentationsfolie für das Thema 75
7.4 Interaktive Präsentation 75
7.5 Beispielrechnung 87
7.6 Schüler*innenergebnis 88
7.7 Feedback der Schülerinnen und Schüler 89

Abbildungsverzeichnis

1 Merkle Baum zur Datei 8
2 Die Geradenchallenge im Reellen 22
3 Verhindern des Double Spending im Reellen 23
4 Transaktion im Bitcoinsystem 26
5 Die Folie der Einleitungspräsentation 75
6 Eine Beispielrechnung zur Bestimmung der Dauer des Ausprobierens 87
7 Die Grundschritte der Schüler*innen-Kryptowährung 88
8 Das Feedback der Schülerinnen und Schüler 89

Tabellenverzeichnis

1 Zeitplan des ersten Tages 33
2 Zeitplan des zweiten Tages 34
3 Bedeutungen der Abkürzungen 34
4 Verlaufsplan Teil 1 35
5 Verlaufsplan Teil 2 36
6 Verwendete Unterrichtsmittel, Medien und deren Funktion 49

1 Fachliche Grundlagen

In diesem Abschnitt werden die benötigten mathematischen, sowie informatischen Grundlagen, welche für diese Arbeit benötigt werden, vorgestellt. Die angebrachten Definitionen und Sätze sind größtenteils aus dem Buch „Lineare Algebra“ von Siegfried Bosch [Bos14] und dem Vorlesungsskript zur „Einführung in die Kryptographie“ von Prof. Dr. Christian Eder [EBH18] extrahiert.

1.1 Algebraische Grundlagen

Im Folgenden beschäftigen wir uns mit den algebraischen Grundlagen dieser Arbeit. Sie bilden das theoretische Grundgerüst für Kryptowährungen und sind somit essentiell für spätere Abschnitte.
Es wird davon ausgegangen, dass der Leser schon mit grundlegenden algebraischen Strukturen, wie *Gruppen* und *Ringen*, vertraut ist. Des Weiteren soll die folgende Vereinbarung gelten.

{box:ringMit1

Kommutative Ringe mit Eins werden im Folgenden als *Ring* bezeichnet.

Definition 1.1: Modul [Bos14]

{def:modul

Sei $\mathcal{S}$ ein Ring. Ein $\mathcal{S}$-Modul ist eine Menge M mit einer inneren Verknüpfung $M \times M \to M$, $(a, b) \mapsto a+b$, genannt **Addition**, und einer äußeren Verknüpfung $\mathcal{S} \times M \to M$, $(s, m) \mapsto s \cdot m$, genannt **skalare Multiplikation**, so dass gilt:

1. M ist eine abelsche Gruppe bezüglich der Addition '+'.
2. $\forall s_1, s_2 \in \mathcal{S} \wedge \forall m \in M : (s_1 + s_2) \cdot m = s_1 \cdot m + s_2 \cdot m$.
3. $\forall s \in \mathcal{S} \wedge \forall m_1, m_2 \in M : s \cdot (m_1 + m_2) = s \cdot m_1 + s \cdot m_2$.
4. $\forall s_1, s_2 \in \mathcal{S} \wedge \forall m \in M : (s_1 \cdot s_2) \cdot m = s_1 \cdot (s_2 \cdot m)$.
5. $\forall m \in M \wedge 1 \in \mathcal{S} : 1 \cdot m = m$

Die erste Definition, welche eingeführt wird, ist die eines *Moduls*. In dieser Arbeit wird es dafür benutzt die vorgestellte Kryptowährung in [KM16] zu verallgemeinern. Weiterhin ist anzumerken, dass Moduln als eine Art Verallgemeinerung von Vektorräumen betrachtet werden können: Die Eigenschaften 2. und 3. bedeuten, dass sich die Addition und skalare Multiplikation distributiv verhalten, während 4. die Assoziativität der skalaren Multiplikation beschreibt ([Bos14], S.204-205).
Das folgende Beispiel dient nicht nur zur Verdeutlichung, sondern ist auch die Grundlage für eine modifizierte Implementation der von Koblitz und Menezes [KM16] vorgestellten Währung.

Beispiel 1.2. *([Bos14])* {bsp:ZModul}
Sei $\mathcal{G}$ eine abelsche Gruppe. Vermöge der äußeren Verknüpfung

$$\mathbb{Z} \times \mathcal{G} \to \mathcal{G}, (z, g) \mapsto \begin{cases} \sum_{i=1}^{z} g, & z \geq 0 \\ -\sum_{i=1}^{z} g & z < 0 \end{cases}$$

ist $\mathcal{G}$ ein $\mathbb{Z}$-Modul.

1.1.1 Elliptische Kurven

{sec:ECC}

Wie schon erwähnt, ist die in dieser Arbeit untersuchte Kryptowährung eine Verallgemeinerung der Implementation, welche in [KM16] vorgestellt ist. Da diese originale Version auf Basis von elliptischen Kurven definiert und auch im späteren Verlauf als Beispiel angeführt ist, wird eine Einführung darin in diesem Abschnitt gegeben. Die Vorgehensweise ist dabei aus dem Vorlesungsskript zu der „Einführung in die Kryptographie “ [EBH18] von Prof. Dr. Christian Eder übernommen.

Definition 1.3: Projektiver Raum ([EBH18])
Sei K ein Körper.

1. Wir bezeichnen die Menge

   $$\mathbb{A}^n(K) = K^n = \{(x_1, \ldots, x_n) | x_i \in K\}$$

   als den **affinen Raum** der Dimension n über K.

2. Zwei Punkte $P, Q \in \mathbb{A}^n(K), P \neq Q$ bestimmen eine eindeutige **(affine) Gerade**

   $$\overline{PQ} \coloneqq P + K \cdot (Q - P) \coloneqq \{P + k(Q - P) | k \in K\}$$

   . Es gilt $P, Q \in \overline{PQ}$.

3. Die Menge

   $$\mathbb{P}^n(K) \coloneqq (K^{n+1} \backslash \{0\})/K^* \coloneqq \{K^* \cdot x | x \in K^{n+1} \backslash \{0\}\}$$

   bezeichnen wir als den **projektiven Raum** der Dimension n über K.

Definition 1.4: Homogene Koordinaten ([EBH18])
Sei $x = (x_0, \ldots, x_n) \in K^{n+1} \backslash \{0\}$. Für den Punkt $P = K^* \cdot x$ schreiben wir

$$P = (x_0 : \ldots : x_n).$$

Wir bezeichnen $x_0, \ldots, x_n \in K$ als **homogene Koordinaten** von P. Diese sind bis auf einen Faktor $k \in K^*, k \neq 0$ eindeutig bestimmt. Diese Eigenschaft wird in der folgenden Äquivalenzrelation beschrieben:

$$(x_0 : \ldots : x_n) \sim (y_0 : \ldots : y_n) \Leftrightarrow (y_0, \ldots, y_n) = k \cdot (x_0, \ldots x_n)$$

Nachdem nun grundlegende Strukturen der algebraischen Geometrie definiert sind, widmen wir uns nun algebraischen Mengen, sowie dem Prinzip der Homogenisierung. Beides benötigen wir für die genauere Untersuchung der Weiherstrass-Gleichungen, welche für die Definition von elliptischen Kurven essentiell sind.

Definition 1.5: Homogenisierung ([EBH18])
Sei K ein Körper. Ein Polynom $F \in K[x_0, \ldots, x_n]$ des Grades n heißt **homogen**, falls alle Monome von F auch vom Grad d sind. Es folgt, dass $F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n)$.
Weiterhin bezeichnen wir

$$F^*(x, y, z) \coloneqq z^d F(\frac{x}{z}, \frac{y}{z}) \in K[x, y, z]$$

als die **Homogenisierung** eines Polynoms $F \in K[x, y]$, $\deg F = d$.

Definition 1.6: Algebraische Mengen ([EBH18])
Sei K ein Körper.

1. Sei $\mathbb{A}^n(K)$ der affine Raum der Dimension n über K und $F \in K[x_1, \ldots, x_n]$ ein Polynom über K in n Unbekannten. Wir interpretieren F als eine K-wertige Funktion über $\mathbb{A}^n(K)$ und sei S eine Menge solcher Polynome F. Wir definieren die **affine algebraische Menge** von S als

$$V(S) \coloneqq \{x \in \mathbb{A}^n(K) | F(x) = 0 \text{ für alle } F \in S\} \subset \mathbb{A}^n(K)$$

2. Sei $\mathbb{P}^n(K)$ der projektive Raum der Dimension n über K und $F \in K[x_0, \ldots, x_n]$ ein homogenes Polynom über K in $n+1$ Unbekannten.Wir interpretieren F als eine K-wertige Funktion über $\mathbb{P}^n(K)$ und sei S eine Menge solcher Polynome F. Wir definieren die **projektive algebraische Menge** von S als

$$V(S) \coloneqq \{x \in \mathbb{P}^n(K) | F(x) = 0 \text{ für alle } F \in S\} \subset \mathbb{P}^n(K)$$

Mit Hilfe der vorangegangenen Definitionen können wir nun letztendlich elliptische Kurven einführen und ihren Nutzen unter einem gruppentheoretischen Aspekt untersuchen.

Definition 1.7: Elliptische Kurven ([EBH18])
Sei K ein Körper und $\bar{K}$ der algebraische Abschluss von K. {def:EC}

1. Wir bezeichnen die Gleichung

$$E^* : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, a_i \in K$$

als die **(homogene) Weierstrass-Gleichung**. Sie ist die Homogenisierung der **(affinen) Weierstrass-Gleichung**

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K.$$

Wir schreiben

$$E(K) \coloneqq V(E^*) \subset \mathbb{P}^2(K)$$

für die **Verschwindungsmenge** von E^*.

2. Falls $E(K)$ glatt ist, also keine singulären Punkte besitzt, heißt $E(K)$ **elliptische Kurve**.

3. Wir definieren $O = (0 : 1 : 0) \in E(\bar{K})$.

4. Für $P, Q \in E(\bar{K})$ definieren wir $P \star Q$ via der Schnittmenge $E(\bar{K}) \cap L = \{P, Q, P \star Q\}$, wobei

$$L \coloneqq \begin{cases} \overline{PQ}, & P \neq Q \\ T_p, & P = Q, \end{cases}$$

mit $T_p \coloneqq \{(u : v : w) \in \mathbb{P}^2(K) | \nabla F^*(P) \cdot (u, v, w)^T = 0\}$.

5. Die Verknüpfung $+$ definieren wir als

$$P + Q \coloneqq (P \star Q) \star O,$$

wobei $P, Q \in E(\bar{K})$.

Um letztendlich zeigen zu können, dass $E(\bar{K})$ vermöge der definierten Abbildungen Gruppeneigenschaften erlangt, wird das folgende Lemma benötigt, welches einen Spezialfall von *Bézouts Theorem* (siehe [Hul12], S.151) darstellt:

Lemma 1.8. *([EBH18])*
Sei $L \subset \mathbb{P}^2(K)$ eine Gerade, dann gilt

$$|L \cap E(\bar{K})| = 3$$

(gezählt mit Vielfachheit).

Beweis. Sei $L = \{(x : y : z) | ax + by + cz = 0\} \subset \mathbb{P}^2(K)$, mit $(a, b, c) \neq (0, 0, 0)$. Wir unterscheiden die folgenden Fälle:

1. $\underline{a = b = 0:}$ $L = \{(x : y : 0) \subset \mathbb{P}^2(K)\}$ ist die Gerade im Unendlichen. Um $L \cap E(\bar{K})$ zu berechnen, setzen wir $z = 0$ in E und bekommen so $x^3 = 0$. Der unendlich weit entfernte Punkt $(0 : 1 : 0)$ stellt eine Lösung der Vielfachheit 3 dar.

2. $\underline{a \neq 0 \vee b \neq 0:}$ $L = \{(x : y : 1) | ax + by = -c\} \cup \{(b : -a : 0)\}$.

   (a) $\underline{b \neq 0:}$ $(b : -a : 0) \neq (0 : 1 : 0)$, somit ist $(b : -a : 0) \notin E(\bar{K})$, da $(0 : 1 : 0)$ der einzige unendlich weit entfernte Punkt von $E(\bar{K})$ ist, nämlich bei $z = 0$. (Des Weiteren hat er Vielfachheit 3, da $E^*(x, y, 0) : x^3 = 0$). Durch die Substitution $y = -\frac{ax+c}{b}$ in E erhalten wir ein kubisches Polynom mit 3 Nullstellen in $\bar{K}$ (gezählt mit Vielfachheit).

(b) $\underline{b = 0, a \neq 0:}$ $(0 : 1 : 0) \in E(\bar{K}) \cap L$. Wir substituieren $x = -\frac{c}{a}$ in E und erhalten so ein quadratisches Polynom mit 2 Nullstellen (affine Punkte) in $\bar{K}$ (gezählt mit Vielfachheit). Insgesamt haben wir so also 3 Punkte gezählt.

□

Lemma 1.9. *([EBH18])*
Seien P, Q, R Punkte auf $E(\bar{K})$. Dann gilt: {lem:ECGrup

1. *$\star$ und $+$ sind kommutativ.*
2. *$(P \star Q) \star P = Q$.*
3. *$O \star O = O$.*
4. *Sei $L \in \mathbb{P}^2(\bar{K})$ eine Gerade und $E(\bar{K}) \cap L = \{P, Q, R\}$, dann gilt: $(P + Q) + R = O$.*
5. *$P + O = P$.*
6. *$P + Q = O \Leftrightarrow P \star Q = O$.*
7. *$+$ ist assoziativ.*
8. *$(E(\bar{K}), +)$ ist eine abelsche Gruppe mit neutralem Element O und $-P = P \star O$.*
9. *$E(K)$ ist eine Untergruppe von $E(\bar{K})$.*

Beweis.

1. Gilt nach Konstruktion von $+$ und $\star$.
2. Gilt nach der Definition von $\star$ mit $L = \{P, Q, P \star Q\}$.
3. Es gilt, dass $\nabla F^*(O) = (0, 0, 1)$. Daraus folgt, dass $(0 : 1 : 0) \in T_P = \{(u : v : w) | w = 0\}$ (der Gerade im Unendlichen).
4. $(P + Q) + R \coloneqq (((P \star Q) \star O) \star R) \star O \overset{(2)}{=} O \star O \overset{(3)}{=} O$.
5. $P + O = (P \star O) \star O = (O \star P) \star O \overset{(2)}{=} P$.
6. Falls $P \star Q = O$, dann ist $P + Q = (P \star Q) \star O = O \star O \overset{(2)}{=} O$. Falls $P + Q = O$, dann ist $P \star Q \overset{(5)}{=} (P \star Q) + O = ((P \star Q) \star O) \star O = (P + Q) \star O = O \star O \overset{(2)}{=} O$.
7. Siehe [Har77], Kapitel IV, Abschnitt 4.
8. Folgt aus 1., 5., 6. und 7..

9. Sei E definiert über K und $P, Q \in E(K)$. Dann sind L und $L \cap E$ auch über K definiert. Weiterhin liegt $P \star Q$, als die dritte Nullstelle von $L \cap E(\bar{K})$, auch in K. Letzteres beruht auf der folgenden Tatsache: Falls $f \in K[x]$, $\deg f = r$, und falls $r - 1$ Nullstellen schon in K liegen, so muss dies auch für die Letzte gelten.

□

Lemma 1.9 zeigt nun letztlich, dass die Punkte auf elliptischen Kurven mehr als nur die Verschwindungsmenge einer Weiherstrass-Gleichung sind. In der Kryptographie werden sie oft als Verschlüsselungsgrundlage benutzt, da es bei geeigneter Wahl eines zugrundeliegenden Körpers sehr schwer ist das folgende Problem zu lösen:

$$xP = Q \implies x = ?$$

Dieses Phänomen werden wir im nächsten Abschnitt in allgemeinerer Form genauer untersuchen.

1.1.2 Der diskrete Logarithmus

Wie schon im vorherigen Abschnitt angeklungen ist, beschäftigen wir uns nun mit dem Problem des „Logarithmierens“ im diskreten Fall. *Diskret* bedeutet hierbei, dass *endliche* algebraische Strukturen als Basen, sowie $\mathbb{Z}/n\mathbb{Z}$ als Exponenten solch einer Potenz der Fokus unserer Definitionen sein werden. Eine erste, konventionelle Definition des diskreten Logarithmus lautet wie folgt.

Definition 1.10: Diskreter Logarithmus ([EBH18])

ef:discLog}

Sei $\mathcal{G} = \langle g \rangle$ eine endliche zyklische Gruppe. Dann gibt es für jedes $y \in \mathcal{G}$ genau ein minimales $a \in \mathbb{N}_0$, mit $g^a = y$. Wir bezeichnen a als den **diskreten Logarithmus** (kurz: **DL**) von y zur **Basis** g. Das Berechnen a „$= log_g y$“ des diskreten Logarithmus (mit bekannten g und y) bezeichnen wir als das **diskrete Logarithmusproblem**, oder kurz: **DLP**.

Es ist anzumerken, dass es im Allgemeinen wichtig ist, dass $\mathcal{G}$ eine zyklische Gruppe ist, da dies bedeutet, dass sie einen Erzeuger g besitzt. Wie schon in Definition 1.10 festgehalten, kann man mit Hilfe wiederholter Verknüpfung von g mit sich selbst alle Elemente von $\mathcal{G}$ erzeugen, was für einen **naiven** Angreifer bedeutet, dass er im schlimmsten Fall **alle** Potenzen von g ($\widehat{=} \#\mathcal{G}$) berechnen müsste. Genau diese Eigenschaft ginge verloren, wenn g kein Erzeuger wäre, denn $\langle g \rangle$ würde so nur eine **kleinere** Untergruppe erzeugen, was den naiven Angriff potenziell um ein Vielfaches vereinfachen, beziehungsweise beschleunigen kann.

{box:DLAssumption}

Bemerkung

In dieser Arbeit gehen wir von der **DL Assumption** aus. Dies bedeutet, dass $DLP \notin BPP$, also diskrete Logarithmen im Allgemeinen nicht durch eine probabilistische Turingmaschine in polynomieller Zeit berechenbar sind [EBH18].

Passend zu Abschnitt 1.1.1 kann das DLP auch für elliptische Kurven definiert werden:

Definition 1.11: DL mit elliptischen Kurven ([EBH18])
Sei K ein Körper und $\mathcal{G} = \langle P \rangle$, wobei $P \in E(K)$. Falls {def:ECDLP}

$$xP = \underbrace{P + \ldots + P}_{\text{x-mal}} = Q$$

gilt, bezeichnen wir, analog zu Definition 1.10, x als den **diskreten Logarithmus** (kurz: **DL**) von Q zur **Basis** P. Das Berechnen x „$= log_P Q$“ des diskreten Logarithmus (mit bekannten P und Q) bezeichnen wir als das **elliptische Kurven diskrete Logarithmusproblem**, oder kurz: **ECDLP**.

Um im nächsten Kapitel die Verallgemeinerung der in [KM16] vorgestellten Kryptowährung einführen zu können, definieren wir uns mit Hilfe von Moduln in 1.12 eine neue Version des DLP.

Definition 1.12: Verallgemeinerter diskreter Logarithmus
Sei $\mathcal{S}$ ein Ring, $\mathcal{G}$ eine Gruppe und $f : \mathcal{S} \times \mathcal{G} \to \mathcal{G}, (s, g) \mapsto s \times g$ eine Abbildung, vermöge derer $\mathcal{G}$ ein $\mathcal{S}$-Modul ist. Falls {def:VDLP}

$$y = s \times g$$

bezeichnen wir s als den **verallgemeinerten diskreten Logarithmus** von y zur **Basis** g. Das Berechnen s „$= log_g y$“ des verallgemeinerten diskreten Logarithmus (mit bekannten g und y) bezeichnen wir als das **verallgemeinerte diskrete Logarithmusproblem**, oder kurz: **VDLP**.

Bemerkung: Diese Definition setzt, genauso wie 1.10 und 1.11, **keine** kryptographische Sicherheit in Form von schwieriger Berechenbarkeit der diskreten Logarithmen voraus. Ähnlich wie in der Bemerkung nach Definition 1.10, muss davon ausgegangen werden, dass ein potenzieller Nutzer geeignete Strukturen $\mathcal{G}, \mathcal{S}$, sowie Abbildung f so wählt, sodass $\text{VDLP}(\mathcal{G}, \mathcal{S}, f) \notin BPP$.

1.2 Informatische Grundlagen

In diesem Abschnitt führen wir Begriffe ein, welche sich eher der Informatik als Fachrichtung zuordnen lassen. Sie werden hauptsächlich in der Definition von Peer-2-Peer-Währungen in Abschnitt 2.3 benötigt.

1.2.1 Merkle Bäume

Merkle Bäume, oder auch Hash Bäume genannt, dienen dazu die Integrität von Datensätzen effizient überprüfen zu können. Sie sind eine spezielle Art Baum mit den folgenden Eigenschaften:

Definition 1.13: Merkle/Hash Baum ([Mer80])
Ein (binärer) Merkle Baum (Hash Baum) der Tiefe n ist ein binärer Out-Tree der Tiefe n mit einer Wurzel $\mathcal{R}$, einer Menge von inneren Knoten T und Blättern T_B. Er hat die folgenden Eigenschaften:

- Alle Blätter $t_i, i \in \{0,1\}^n$ sind Hashwerte (zum Beispiel von Datensätzen).
- Für innere Knoten t_j der Tiefe k mit Kindern $t_{i'=j||0}, t_{i''=j||1}$, $j \in \{0,1\}^k$, $i', i'' \in \{0,1\}^{k+1}$ gilt:
$$t_j = \mathcal{H}(t_{i'}||t_{i''})$$
- Für die Wurzel gilt:
$$\mathcal{R} = \mathcal{H}(t_0||t_1)$$

Wobei $\mathcal{H}(\cdot)$ eine beliebige kryptographische Hashfunktion ist.

In Beispiel 1.14 wird der Nutzen von Merkle Bäumen verdeutlicht.

Beispiel 1.14. *Angenommen ein Nutzer möchte in einem P2P-Netzwerk eine in mehrere Teile D_i gespaltene Datei herunterladen. Abbildung 1 zeigt, wie ein zugehöriger Merkle Baum aussehen könnte:*

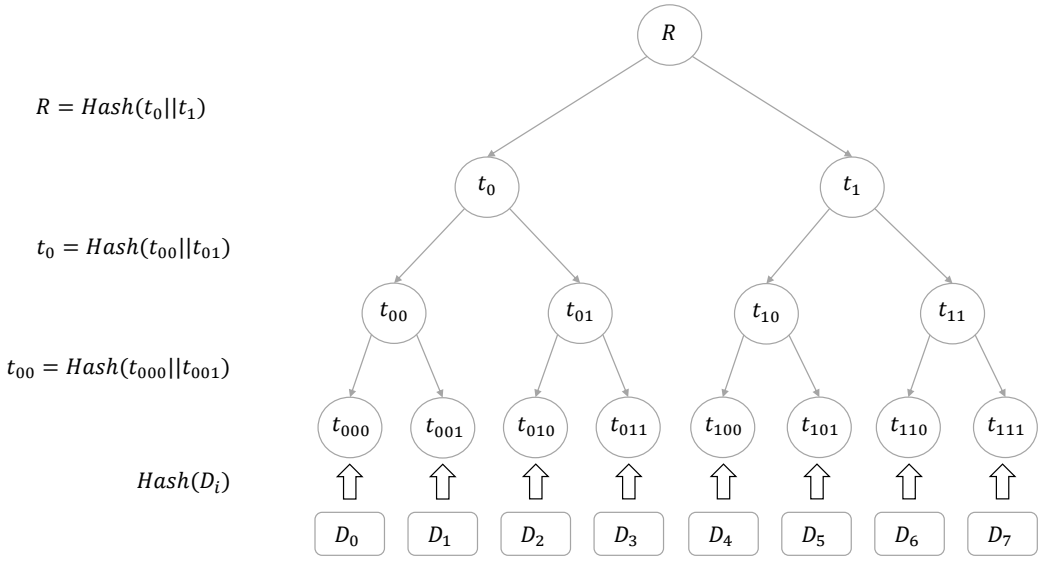


Abbildung 1: Merkle Baum zur Datei

Nachdem der User bei einer Quelle, der er vertraut, die Merkle-Wurzel (Merkle Root) $\mathcal{R}$ bezogen hat, können die übrigen Knoten und Blätter auch von nicht

vertrauenswürdigen Peers bezogen werden, da diese immer gegen $\mathcal{R}$ prüfbar sind. Wenn der Nutzer nun beispielsweise Paket D_3 bezogen hat und dieses aufgrund potentieller Übertragungsfehler oder nicht vertrauenswürdigen Peers auf Integrität (Fehlerfreiheit) überprüfen möchte, so benötigt er weder die ganze Datei, noch den ganzen Baum. Er muss nur t_{010}, t_{00} und t_1 anfordern, denn er kann mit Hilfe seines t_{011} und dem angeforderten t_{010} selbst $t_{01} = \mathcal{H}(t_{011}||t_{010})$ berechnen. Er fährt analog für die Berechnung von t_0, sowie das Gegenprüfen von $\mathcal{R} = \mathcal{H}(t_0||t_1)$ fort.

2 Kryptowährungen

{sec:CC}

In diesem Abschnitt werden die drei gewünschten Ziele von Kryptowährungen, sowie zwei Möglichkeiten der Implementierung einer solchen vorgestellt. Die erste Option ist eine zentralisierte Version, welche auf eine obligatorische Bank-Ebene zurückgreift. Die Zweite hingegen setzt auf ein Peer-to-Peer-Netzwerk aus Knoten, in welchem die Transaktionen verarbeitet werden.

2.1 Ziele von Kryptowährungen

Schon immer war Bargeld eine gute Art anonym, schnell und sicher Transaktionen abzuwickeln: Nur anhand des physischen Geldes ist nicht zurückzuverfolgen, wer die (Vor-)Besitzer waren/sind, die Münzen und Scheine wechseln durch einfaches Aushändigen den Besitzer und –unter der Annahme, dass Bargeld nur sehr schwer zu fälschen ist– kann man sicher sein, dass die Transaktion auch irreversibel korrekt abgeschlossen wurde.
Nachteile des klassischen Bargelds sind jedoch auch relativ offensichtlich. So ist es zum Beispiel sehr schwer mit einer großen Menge an Bargeld in einem entfernten Land eine Transaktion abzuschließen, je nachdem wie groß die Summe ist, kann der Transport auch schon auf kurzen Distanzen umständlich werden und man kann im Allgemeinen keine Zahlungen für Geschäfte im Internet damit tätigen.

Nun gibt es natürlich schon Lösungen, um Transaktionen elektronisch abzuschließen, beispielsweise Kreditkarten, Überweisungen oder Online-Bezahldienste wie PayPal [Pay19]. Nachteile dieser Methoden beinhalten jedoch fehlende Anonymität, Weiterverkauf der Transaktionsdaten an Dritte, (hohe) Transaktionsgebühren oder eine langsame Geschwindigkeit im Generellen. Ein weiterer Minuspunkt bei allen genannten Optionen ist, dass auch Transaktionen zwischen zwei Nutzern des Systems über eine zentrale Anlaufstelle geleitet und nicht einfach *nur* zwischen den beiden Parteien des Handels abgewickelt werden, was beispielsweise dazu führen kann, dass durch politischen Druck Zentralen dazu gezwungen werden können gewisse Nutzer vom System auszuschließen (siehe die Banking-Blockade der USA gegen Spenden an Wiki-Leaks [Syn17]).

Die Herausforderung ist also eine elektronische Möglichkeit zu schaffen, welche den Komfort von Kreditkarten oder Online-Bezahldiensten mit den Verzügen des Bargeldes kombiniert: *eCash*. Im Folgenden werden die Einheiten dieser Währungen vereinfachend als „Coins“ bezeichnet. Die zuvor genannten Punkte fassen Koblitz & Menezes [KM16, S.88] zu den drei Zielen von eCash zusammen.

Definition 2.1: Ziele von eCash {def:zieleE

- **Sicherheit:** Es ist nicht möglich Coins zu fälschen oder eine Coin doppelt auszugeben („Double-Spending“)

- **Geheimhaltung:** Durch eine Zahlung kann die Identität der am Handel teilnehmenden Personen nicht aufgedeckt werden.

- **Effizienz:** Die Benutzung des eCash-Systems sollte schnell und einfach sein. Des Weiteren sollten, abgesehen von einem PC, keine weiteren Hilfsmittel benötigt werden.

Für eCash haben sich in den letzten Jahren zwei große Paradigmen herausgestellt, nämlich die *Central Authority*-Systeme, welche eine Art zentrale Bank besitzen, bei der man seine Coins Einzahlen und Abheben kann, sowie die *Peer-to-Peer*-Systeme, die auf solch eine Instanz verzichten und eine Bearbeitung der Transaktionen innerhalb eines Netzwerkes implementieren.

2.2 Central Authority eCash

ec:CAeCash}

In diesem Abschnitt wird eine verallgemeinerte Möglichkeit der Implementierung von eCash nach [KM16, S.88-94] beschrieben. Die im Werk von Koblitz und Menezes vorgestellte Version basiert auf einem RSA gestützten Verfahren von Chaum [Cha83], welches abgewandelt wurde, sodass die Verschlüsselung durch ECC geschieht. Die hier vorgestellte Implementation ist eine Verallgemeinerung, die von den explizit verwendeten algebraischen Strukturen in [KM16] abstrahiert.

Damit das System konstruiert werden kann, sind einige Voraussetzungen und Definitionen nötig. Im Folgenden gilt:

vereinbarung}

Vereinbarung

- $(\mathcal{S}, +, \cdot)$ ist ein Ring, abkürzend mit $\mathcal{S}$ bezeichnet.
- $(\mathcal{G}, \circ)$ ist eine Gruppe, abkürzend mit $\mathcal{G}$ bezeichnet.
- e ist das neutrale Element in $\mathcal{G}$.
- $\mathcal{G}$ wird vermöge der Abbildung $f : \mathcal{S} \times \mathcal{G} \to \mathcal{G}, (s, g) \mapsto s \times g$ ein $\mathcal{S}$-Modul (siehe Def. 1.1).

  $\to$ $s \times g$ soll im Folgenden verkürzt als sg geschrieben sein.
- Das VDLP (siehe Def. 1.12) ist schwer mit $\mathcal{G}$, $\mathcal{S}$ und f.
- $\mathcal{H} : \{0,1\}^* \to \mathcal{S}$, ist eine Hashfunktion, die beliebige Bitstrings nach $\mathcal{S}$ abbildet.

Nachdem nun die mathematischen Grundlagen dargelegt wurden, stellt sich natürlich die Frage, wie man diese in eine Währung verpacken kann. Analog zu dem Beispiel von Koblitz & Menezes [KM16] wird die folgende Definition vorgeschlagen.

Definition 2.2: Coinsignaturen und Coins

ureCentral}

Seien $A, B \in \mathcal{G}$ beliebig gewählt. Eine Signatur auf dem Tupel (A, B) besteht aus dem Tripel $(C', R, S) \in \mathcal{G}^3$ und einem $y \in \mathcal{S}$, welche die folgenden Gleichungen

erfüllen.

{eqn:signEqn1}
$$yP = hQ \circ R \tag{1}$$

$$yA = hC' \circ S \tag{2}$$ {eqn:signEq

mit $h = \mathcal{H}(A, B, C', R, S)$.

Eine Coin ist definiert als das 6-Tupel (A, B, C', R, S, y).

Die Grundidee einer Interaktion zwischen zwei Nutzern Alice und Bob beruht auf einer recht simplen Idee, welche sich die Schwere des VDLP zunutze macht. Dazu sei $P \in \mathcal{G}, P \neq e$ fest gewählt und beiden Parteien bekannt. Zuerst muss sich Alice eine Steigung s, sowie einen y-Achsenabschnitt t einer Geraden aus $\mathcal{S}$ wählen. Sie schickt Bob $A = sP$ und $B = tP$, welche s und t implizit bestimmen. Auch hier ist wieder anzumerken, dass es Bob aufgrund der Schwere (siehe Bemerkung nach Definition 1.12) des verallgemeinerten diskreten Logarithmusproblems nicht möglich ist die beiden Parameter zu bestimmen. Die Idee ist nun, dass Alice ihren Handelspartner Bob davon überzeugen will, dass sie s und t kennt, ohne dabei einen davon an Bob übermitteln zu müssen, was in folgendem Protokoll geschieht:

Geradenprotokoll {box:Geradenp

1. Bob wählt ein beliebiges $x \in \mathcal{S}$, seine *Challenge*.
2. Alice bestimmt $y = s \cdot x + t$, sodass (x, y) ein Punkt auf ihrer Geraden ist.
3. Bob verifiziert y, indem er die Gleichung $yP = xA \circ B$ verifiziert.

Der dritte Schritt ist hierbei durch das folgende Lemma gegeben.

{lem:gerade

Lemma 2.3.
Seien $s, t, x \in \mathcal{S}$ bel., $A = sP \in \mathcal{G}$ und $B = tP \in \mathcal{G}$ gegeben. So gilt:

$$y = s \cdot x + t \tag{3}$$
$$\Leftrightarrow$$
$$yP = xA \circ B \tag{4}$$

Beweis. Seien s, t, x, A, B wie in Lemma 2.3 gegeben.
Da $\mathcal{G}$ ein $\mathcal{S}$-Modul ist, gilt nun also, dass

$$\begin{aligned} y &= s \cdot x + t \\ \Leftrightarrow yP &= (s \cdot x + t)P \\ \Leftrightarrow yP &= x(sP) \circ tP \\ \Leftrightarrow yP &= xA \circ B \end{aligned}$$

□

2.2.1 Hauptanwendungen des Systems

Im Folgenden werden –nach einem Set-Up-Schritt– die drei Hauptanwendungen des Systems gezeigt: Abheben, Bezahlen und Einzahlen. Wir beginnen nun mit dem Set-Up, welches benötigt wird, um einige Vorbereitungen zu treffen.

Definition 2.4: Set-Up

tUpCentral} Bezeichne folgend $\mathcal{B}$ die Bank, $\mathcal{U}$ einen User und $\mathcal{M}$ einen Händler. Der Set-Up-Schritt läuft wie folgt ab.

Die **Bank**:

1. veröffentlicht drei beliebige, nicht-neutrale Elemente $P, P_1, P_2 \in \mathcal{G}$.
2. wählt ein geheimes $z \in \mathcal{S}$ als ihren *private Key*.
3. veröffentlicht $Q = zP$, $Q_1 = zP_1$, $Q_2 = zP_2$ als ihren *public Key*.

Es ist anzumerken, dass der private Key, sowie der public Key der Bank permanent gewählt sind, also für die ganze Bestehensdauer des Systems gleich bleiben.

Der **User**:

1. wählt einen geheimen Exponenten $u_1 \in \mathcal{S}$.
2. berechnet seine Kontonummer $I = I_{\mathcal{U}} = u_1 P_1$.
3. berechnet seine modifizierte Kontonummer $\tilde{I} = I \circ P_2$.
4. registriert sich bei $\mathcal{B}$ mit seiner Kontonummer I.

Danach berechnet $\mathcal{B}$ einen geteilten Key C als $C = z\tilde{I}$. $\mathcal{U}$ berechnet C als $C = u_1 Q_1 \circ Q_2$.

Nachdem das Set-Up abgeschlossen ist, hat $\mathcal{U}$ mehrere Möglichkeiten. Er kann entweder Coins von der Bank abheben, eine Transaktion mit $\mathcal{M}$ tätigen oder Coins in die Bank einzahlen. Da für eine Transaktion Coins benötigt werden, beginnen wir mit dem Abheben.

Definition 2.5: Abheben

benCentral} $\mathcal{U}$ will von $\mathcal{B}$ Coins abheben. Die Auszahlung kann auch wieder in einen Set-Up-Schritt und das eigentliche Abheben aufgeteilt werden.

Das **Set-Up**:

1. $\mathcal{B}$ wählt zufällig ein $w \in \mathcal{S}$.
2. $\mathcal{B}$ schickt $R = wP$ und $S = w\tilde{I}$ an $\mathcal{U}$.
3. $\mathcal{U}$ wählt zufällig $s, t_1, t_2, u, v \in \mathcal{S}$.
4. $\mathcal{U}$ berechnet $A = s\tilde{I}$, $B = t_1 P_1 \circ t_2 P_2$, $C' = sC$, $R' = uR \circ vP$, $S' = (s \cdot u)S \circ vA$, $r = u^{-1} \cdot \mathcal{H}(A, B, C', R', S')$.

5. $\mathcal{U}$ schickt r an $\mathcal{B}$.

Die **Auszahlung**:

1. $\mathcal{B}$ schickt $y = r \cdot z + w$ an $\mathcal{U}$.
2. $\mathcal{U}$ verifiziert $yP = rQ \circ R$ und $y\tilde{I} = rC \circ S$.
3. $\mathcal{U}$ berechnet $y' = u \cdot y + v$.

Nach diesen Schritten hat $\mathcal{U}$ eine Coin (A, B, C', R', S', y') „abgehoben“, wie in Lemma 2.6 gezeigt ist.

{lem:coinS

Lemma 2.6.
Seien $A, B, C', R', S' \in \mathcal{G}$ und $s, t_1, t_2, u, v \in \mathcal{S}$ wie in Definition 2.5 gewählt.
Das Sechs-Tupel

$$(A, B, C', R', S', y')$$

definiert eine Coin, welche die Coin-Signatur Gleichungen 2.2 erfüllt.

Beweis. Nach den Definitionen von R', y' und der Gleichung $yP = rQ \circ R$ aus dem zweiten Schritt der Auszahlung in 2.5 gilt folgende Gleichung:

$$\begin{aligned} y'P &= (u \cdot y)P \circ vP \\ &= (u \cdot r)Q \circ uR \circ vP \\ &= hQ \circ R' \end{aligned}$$

Des Weiteren gilt wegen den Definitionen von y', A, C', S' und der Gleichung $y\tilde{I} = rC \circ S$ aus dem zweiten Schritt der Auszahlung in 2.5 die Gleichung

$$\begin{aligned} y'A &= (u \cdot y + v)s\tilde{I} \\ &= (u \cdot s)(rC \circ S) \circ vA \\ &= (u \cdot r \cdot s)C \circ (s \cdot u)S \circ vA \\ &= hC' \circ S' \end{aligned}$$

□

Durch den Umweg im vierten Schritt des Set-Ups in 2.4 wird erreicht, dass die Bank, obwohl sie Wissen über R, S, C, I und y besitzt, keine Informationen über die „ausgezahlte“ Coin (A, B, C', R', S', y') hat.

Bevor wir uns den Bezahlvorgang näher betrachten können, wird das folgende Lemma benötigt, welches das Geradenprotokoll etwas verallgemeinert.

{lem:Bezahl

Lemma 2.7.
Sei $\mathcal{U}$ ein User mit Kontonummer I.
Seien $u_1, s, t_1, t_2 \in \mathcal{S}$ beliebig gewählt und $A, B \in \mathcal{G}$ somit wie in Definition 2.5 als Teil einer Coin c gegeben, welche von $\mathcal{U}$ besessen wird.

Für ein beliebiges $x \in \mathcal{S}$ gilt die Gleichung

$$y_1 P_1 \circ y_2 P_2 = xA \circ B$$

wobei $y_1 = (u_1 \cdot s) \cdot x + t_1$ (1) und $y_2 = s \cdot h_0 + t_2$ (2) gelten.

Beweis. Nach Definition 2.4 ist $\tilde{I}$ definiert als $\tilde{I} = I \circ P_2 = u_1 P_1 \circ P_2$ (3).
Damit gilt also:

$$\begin{aligned} y_1 P_1 \circ y_2 P_2 &\overset{(1)\&(2)}{=} (u_1 \cdot s \cdot h_0) P_1 \circ t_1 P_1 \circ (s \cdot h_0) P_2 \circ t_2 P_2 \\ &= (u_1 \cdot s \cdot h_0) P_1 \circ (s \cdot h_0) P_2 \circ t_1 P_1 \circ t_2 P_2 \\ &\overset{\text{Def. B}}{=} (u_1 \cdot s \cdot h_0) P_1 \circ (s \cdot h_0) P_2 \circ B \\ &= h_0((s \cdot u_1) P_1 \circ s P_2) \circ B \\ &\overset{(3)}{=} h_0 A \circ B \end{aligned}$$

□

Lemma 2.7 kann als Verallgemeinerung betrachtet werden, da man als User nun die Möglichkeit hat sein Wissen über vier Parameter zu beweisen, anstatt nur zwei, was im Bezahlvorgang 2.8 essentiell wichtig ist.

Definition 2.8: Bezahlen

enCentral} Bei dem Bezahlvorgang werden folgende Schritte abgehandelt:

1. $\mathcal{U}$ schickt $\mathcal{M}$ die Coin (A, B, C', R', S', y').
2. $\mathcal{M}$ verifiziert die Coin-Signaturen in 2.2.
3. Beide berechnen eine Bitfolge d, welche Zeit und Datum repräsentiert.
4. Beide berechnen $h_0 = \mathcal{H}(A, B, I', d)$, wobei $I' = I_{\mathcal{M}}$ ist, die Kontonummer von $\mathcal{M}$.
5. $\mathcal{M}$ wählt sich h_0 als seine Challenge für das verallgemeinerte Geradenprotokoll.
6. $\mathcal{U}$ schickt $y_1 = (u_1 \cdot s) \cdot h_0 + t_1$ und $y_2 = s \cdot h_0 + t_2$ an $\mathcal{M}$.
7. $\mathcal{M}$ verifiziert die Gleichung $y_1 P_1 \circ y_2 P_2 = h_0 A \circ B$.

Falls die Gleichung in Schritt 7 verifiziert werden konnte, akzeptiert $\mathcal{M}$ die Bezahlung.

Nachdem der Händler $\mathcal{M}$ eine Transaktion abgeschlossen hat, mit einer Coin (A, B, C', R', S', y') als Bezahlung, kann er diese (auch nach einiger Zeit erst) bei der Bank $\mathcal{B}$ einzahlen. Das Einzahlungsprotokoll ist im Folgenden erklärt.

enCentral} **Definition 2.9: Einzahlen**

1. $\mathcal{M}$ schickt $\mathcal{B}$ die Coin $c = (A, B, C', R', S', y')$, zusammen mit y_1, y_2 und d (siehe 2.8)

2. $\mathcal{B}$ verifiziert die Coin-Signaturen in 2.2.

3. $\mathcal{B}$ berechnet $h_0 = \mathcal{H}(A, B, I_{\mathcal{M}}, d)$.

4. $\mathcal{B}$ verifiziert die verallgemeinerte Geradenprotokollgleichung in 2.7.

Falls Schritt 2 **und** 4 des Einzahlungsprotokolls erfolgreich durchgeführt wurden, akzeptiert $\mathcal{B}$ die Einzahlung der Coin c von $\mathcal{M}$ *vorläufig*. Um die Einzahlung –und somit auch in einem gewissen Sinn die ganze Transaktion– komplett abzuschließen, muss $\mathcal{B}$ noch überprüfen, ob an einer Stelle der Transaktion *Double Spending*, also das doppelte Ausgeben oder Einzahlen einer Coin, aufgetreten ist. Die Schritte, die $\mathcal{B}$ dazu durchführen muss sind in der nächsten Definition aufgeführt.

Definition 2.10: Verhindern des Double Spending

{def:Double

Bei einer Einzahlung überprüft die Bank, wie schon in Definition 2.9 erwähnt, noch einmal, ob eine Coin (A, B, C', R', S', y') schon mal eingezahlt wurde. Das Ereignis des Double-Spendings wird also spätestens beim Einzahlen erkannt. Nun ist es aber natürlich nicht nur von Interesse, dass eine doppelte Einzahlung vorkam, sondern auch, wer der Schuldige ist. Denn nur weil der Händler $\mathcal{M}$ versucht hat die Münze doppelt einzuzahlen, heißt das noch lange nicht, dass er auch der Gesuchte ist.

Falls nun also $\mathcal{B}$ bemerkt, dass es schon einen Eintrag für eine einzuzahlende Coin gibt, lassen sich zwei Möglichkeiten aufführen:

> h_0 **ist verschieden**: Dieser Fall bedeutet, dass die Coin schon in einer früheren Transaktion –oder besser gesagt: einer Transaktion, die früher mit einer Einzahlung an die Bank abgeschlossen wurde– als Zahlungsmittel benutzt wurde, was bedeutet, dass der Besitzer der Coin, $\mathcal{U}$, der Schuldige ist. Um nun herauszufinden, wer genau der Besitzer der Coin war, benutzt $\mathcal{B}$ eine simple Eigenschaft der Geradenchallenge aus: Im Falle einer doppelten Nutzung der Parameter u_1, s, t_1, t_2 mit verschiedenen Challenges, können diese berechnet werden, da nun $(h_0, y_1), (h_0', y_1'), (h_0, y_2), (h_0', y_2')$ bekannt sind. Die ersten beiden liegen auf einer Geraden $y = u_1 \cdot s \cdot x + t_1$, die zweiten auf $y = s \cdot x + t_2$. Da für eine Gerade immer nur zwei verschiedene Punkte, die darauf liegen, notwendig sind, um sie eindeutig zu bestimmen, ist der Besitzer der Coin nun nicht mehr anonym, da die Bank mit Hilfe von $I_{\mathcal{U}} = u_1 P_1$ eindeutig den Täter bestimmen kann.
>
> h_0 **ist gleich**: Unter der Annahme, dass $\mathcal{H}$ nur mit vernachlässigbar kleiner Wahrscheinlichkeit gleiche Hashwerte für verschiedene Eingabeparameter berechnet, geht $\mathcal{B}$ davon aus, dass das Quadrupel (A, B, I', d) in beiden Fällen zur Berechnung von $h_0 = \mathcal{H}(A, B, I', d)$ benutzt wurde, was bedeutet, dass der Händler $\mathcal{M}$ versucht eine Coin doppelt einzubezahlen.

2.2.2 Implementationen des CA-Systems

Elliptische Kurven:
Wie schon erwähnt, ist die vorgeschlagene Implementation von Koblitz & Menezes [KM16] die Grundlage für die hier vorgestellte allgemeinere Variante. Diese, auf elliptischen Kurven basierende Version, soll nun kurz als Beispiel für eine Umsetzung präsentiert werden. Die benötigten Definitionen sind die folgenden:

einbarungECC}

Vereinbarung: ECC

- $\mathbb{F}_q$ ist der endliche Körper mit q Elementen.
- $E(\mathbb{F}_q)$ ist die Verschwindungsmenge einer elliptischen Kurve E über $\mathbb{F}_q$.
- $(E(\mathbb{F}_q), +)$ ist eine Gruppe, die abkürzend mit $E(\mathbb{F}_q)$bezeichnet wird.
- $e \in E(\mathbb{F}_q)$ ist das neutrale Element von $E(\mathbb{F}_q)$.
- $p \mid \#(E(\mathbb{F}_q))$, mit $p \in \mathbb{P}$.
- p hat eine ähnlich große Bitlänge wie q.
- $\mathcal{G} = \langle P \rangle \leq E(\mathbb{F}_q)$ ist die Untergruppe von $E(\mathbb{F}_q)$ mit Ordnung p.
- $\mathcal{S} = \mathbb{Z}/p\mathbb{Z}$ ist ein Ring mit Verknüpfungen + und $\cdot$
- $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}/p\mathbb{Z}$, ist eine Hashfunktion, die beliebige Bitstrings nach $\mathbb{Z}/p\mathbb{Z}$ abbildet.

Natürlich fällt auf, dass $\mathcal{G}$ nur vermöge einer passenden Abbildung zum $\mathcal{S}$-Modul wird. Diese ist jedoch recht intuitiv in der folgenden Definition beschrieben.

Definition 2.11: Die Modulstruktur für ECC

dStruktECC} Wir definieren:

$$f : \mathbb{Z}/p\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q), (z, P) \mapsto zP \coloneqq \underbrace{P + \cdots + P}_{\text{z-mal}}$$

Die Definition von f in 2.11 ist sinnvoll, da $\mathcal{G}$ automatisch ein $\mathbb{Z}$-Modul ist (siehe Bsp. 1.2). Da $\#\mathcal{G} = p$, ist es somit auch ein $\mathbb{Z}/p\mathbb{Z}$-Modul.

Die folgenden Definitionen sind aufgrund der spezifisch gewählten Struktur, den elliptischen Kurven interessant, da sie noch etwas mehr Aufschluss über die kryptographische Sicherheit des Systems geben.

Definition 2.12: Exponentenraum

Seien $\mathcal{G}$ und $\mathcal{S}$ wie oben gegeben, so nennen wir $\mathcal{S} = \mathbb{Z}/p\mathbb{Z}$ den *Exponentenraum* von $\mathcal{G}$.

Beispiel 2.13. ***Exponenten***

Seien $E(\mathbb{F}_q)$ und $\mathcal{G}$ wie oben gegeben und $Q, P \in \mathcal{G}$, mit $Q = \underbrace{P + P + \cdots + P}_{x} =$ xP, so nennen wir $x \in \mathbb{Z}/p\mathbb{Z}$ einen Exponenten.

Die Bezeichnung als Exponenten geschieht hier nur in Anlehnung an die multiplikative Gruppe über einem endlichen Körper $\mathbb{F}_q$. Die Gruppenverknüpfung bleibt natürlich die Addition (siehe Definition 1.7).

Definition 2.14: Implizit bestimmte Exponenten
Sei $P \in \mathcal{G}$ bel. mit $P \neq e$ und $Q = xP \in E(\mathbb{F}_q)$ für ein bel. $x \in \mathbb{Z}/p\mathbb{Z}$. Wir sagen:

$$Q \textit{ bestimmt } x \textit{ implizit.}$$

Implizit bestimmte Exponenten müssen im Allgemeinen nicht eindeutig sein. Die Vereinbarung für die ECC-Version, genauer, $\mathcal{G} \leq E(\mathbb{F}_q)$, $(\#\mathcal{G} = p)$, sichert dies jedoch.

Definition 2.15: Repräsentation von Punkten
Seien $P_1, P_2 \in \mathcal{G}$ bel. und $Q = t_1P_1 + t_2P_2 \in E(\mathbb{F}_q)$, so nennen wir

$$t_1P_1 + t_2P_2$$

eine *Repräsentation* von Q.

Jeder Punkt $Q \in E(\mathbb{F}_q)$definiert also implizit eine Menge

$$\mathcal{R}_Q = \{(t_1, t_2) | t_1, t_2 \in \mathbb{Z}/p\mathbb{Z}, Q = t_1P_1 + t_2P_2\}.$$

Mit Hilfe dieser Definitionen behaupten Koblitz & Menezes [KM16] nun, dass das Problem eine Repräsentation eines Punktes Q zu finden genauso schwer ist wie das ECDLP selbst zu lösen.

Multiplikative Gruppen:
Ein weiteres Beispiel und gleichzeitig auch wichtiger Zwischenschritt für die Definition einer vereinfachten Kryptowährung in Unterrichtssituationen ist der folgende Ansatz, welcher, anstatt mit elliptischen Kurven, mit Restklassen in $(\mathbb{Z}/p\mathbb{Z})^\times$ operiert. Ähnlich zur ECC-Version wird auch in dieser die Schwere des diskreten Logarithmusproblems –für geeignete p – ausgenutzt.

Die Vereinbarungen für diese Version ist im Folgenden zu sehen:

Vereinbarung: Multiplikative Gruppen

{box:vereinbarungMult

- p ist eine Primzahl.
- $\mathcal{R} = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Restklassenring.
- $\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})^\times$ ist die multiplikative Gruppe von $\mathcal{R}$.
- $\#\mathcal{G} = p - 1$.
- $e \in \mathcal{G}$ ist das neutrale Element von $\mathcal{G}$.
- p ist so gewählt, dass das DLP in $\mathcal{G}$ schwer ist.
- $\mathcal{S} = \mathbb{Z}/(p-1)\mathbb{Z}$ ist ein Ring mit Verknüpfungen + und $\cdot$
- $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}/(p-1)\mathbb{Z}$, ist eine Hashfunktion, die beliebige Bitstrings nach $\mathbb{Z}/(p-1)\mathbb{Z}$ abbildet.

Auch hier muss wieder eine passende Abbildung gewählt werden, sodass $\mathcal{G}$ vermöge dieser zum $\mathcal{S}$-Modul wird. Wir definieren sie ähnlich zur ECC-Version:

Definition 2.16: Die Modulstruktur für multiplikative Gruppen

ltGruppen} Wir definieren:

$$f : \mathbb{Z}/(p-1)\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, (z, g) \mapsto zg \coloneqq g^z = \underbrace{g \cdot \ldots \cdot g}_{\text{z-mal}}$$

Um einen Einblick in die Implementation zu bekommen, ist in Lemma (2.17) eines der wichtigsten Protokolle der Central Authority Kryptowährung als Beispiel aufgeführt:

ltCentral}

Lemma 2.17.
Sei $\mathcal{U}$ ein Nutzer mit Kontonummer $I_\mathcal{U}$.
Seien $u_1, s, t_1, t_2 \in \mathbb{Z}/(p-1)\mathbb{Z}$ beliebig gewählt und $A, B \in \mathbb{Z}/p\mathbb{Z})^\times$ somit als Teil einer Coin c gegeben, welche von $\mathcal{U}$ besessen wird.
Für ein beliebiges $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ gilt die Gleichung

$$y_1 P \cdot y_2 P = xA \cdot B$$

wobei $y_1 = (u_1 \cdot s) \cdot x + t_1$ (1) und $y_2 = s \cdot x + t_2$ (2) gelten.

Beweis. Es gilt: $\tilde{I} = I \cdot P_2 = u_1 P_1 \cdot P_2$ (3).

Damit gilt also:

$$\begin{aligned} y_1P_1 \cdot y_2P_2 &\overset{(1)\ \&\ (2)}{=} (u_1 \cdot s \cdot x + t_1)P_1 \cdot (s \cdot x + t_2)P_2 \\ &= (u_1 \cdot s \cdot x)P_1 \cdot t_1P_1 \cdot (s \cdot x)P_2 \cdot t_2P_2 \\ &\overset{\text{Def.}B}{=} (u_1 \cdot s \cdot x)P_1 \cdot (s \cdot x)P_2 \cdot B \\ &= x((u_1 \cdot s)P_1 \cdot sP_2) \cdot B \\ &\overset{(3)}{=} x(s((u_1)P_1 \cdot P_2)) \cdot B \\ &= x(s\tilde{I}) \cdot B \\ &= xA \cdot B \end{aligned}$$

□

Reelle Zahlen:
Eine der denkbar einfachsten, aber leider auch unsichersten Versionen arbeitet auf den reellen Zahlen. Werden die in Abschnitt 2.2 eingeführten Definitionen und Protokolle ohne Veränderungen für die Menge der reellen Zahlen übernommen, so ist leicht erkennbar, dass sich die Berechnungen zu simplen Potenzierungen reeller Zahlen vereinfacht, was wiederum keinerlei kryptographische Sicherheit hervorbringt. Ein großer Vorteil dieser Implementation ist jedoch, dass sich das wichtigste Protokoll des Systems, die Geradenchallenge, sehr schön visualisieren lässt.

Beginnen wir jedoch zuerst mit den Vereinbarungen dieser Version:

Vereinbarung: Reelle Zahlen {box:vereinba

- $\mathcal{G} = (\mathbb{R}_{>0}, \cdot)$ ist die Gruppe über den reellen Zahlen mit der Verknüpfung $\cdot$.
- $e \in \mathcal{G}$ ist das neutrale Element von $\mathcal{G}$.
- $\mathcal{S} = \mathbb{R}$ ist ein Ring mit Verknüpfungen $+$ und $\cdot$.
- $\mathcal{H} : \{0,1\}^* \to \mathbb{R}$, ist eine Hashfunktion, die beliebige Bitstrings nach $\mathbb{R}$ abbildet.

Wie auch in den anderen Versionen wird eine Abbildung in Definition 2.18 präsentiert, vermöge derer $\mathcal{G}$ zu einem $\mathcal{S}$-Modul wird.

Definition 2.18: Die Modulstruktur für reelle Zahlen
Wir definieren: {def:modSt

$$f : \mathbb{R} \times \mathbb{R}_{>0} \to \mathbb{R}_{>0}, (z, g) \mapsto zg \coloneqq g^z = \underbrace{g \cdot \ldots \cdot g}_{\text{z-mal}}$$

Wie schon erwähnt, lässt sich f als Potenzierung einer reellen Zahl g mit einem Exponenten z auffassen.

Beispiel 2.19. ***Visualisierung der Geradenchallenge***
Wir rufen uns die grundlegende Definition der Geradenchallenge 2.2 ins Gedächtnis. Ein Nutzer $\mathcal{U}$ will sein Wissen über s und t einem Händler $\mathcal{M}$ beweisen, ohne ihm diese zu übermitteln. Die beiden Parameter werden als Steigung und y-Achsenabschnitt einer Geraden in $S = \mathbb{R}$ aufgefasst. Ein Beispiel könnte wie folgt aussehen.

- *$P = 2$ und ist sowohl $\mathcal{U}$ als auch $\mathcal{M}$ bekannt.*
- *$\mathcal{U}$ wählt sich $s = 2$ und $t = 3$.*
- *$\mathcal{M}$ gibt $x = 1$ als seine Challenge vor.*

Diese Situation ist in Abbildung 2 dargestellt.

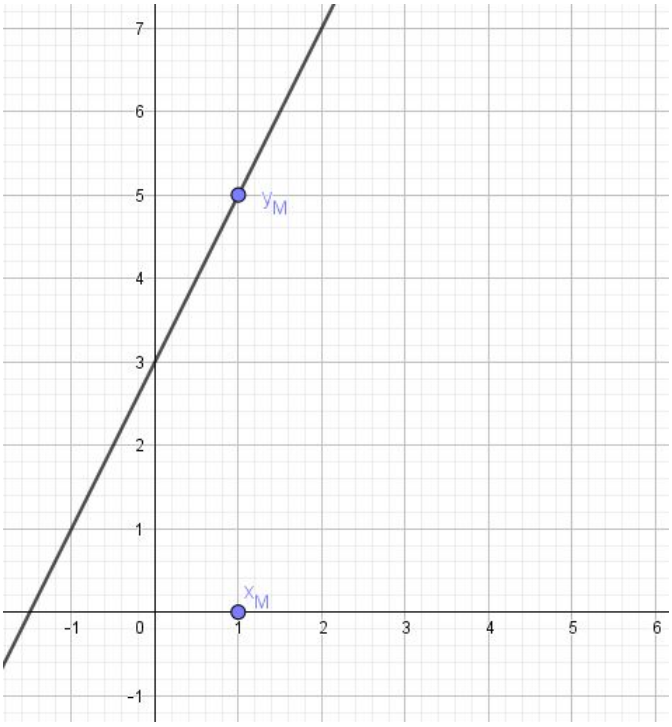


Abbildung 2: Die Geradenchallenge im Reellen

ge_reell_1}

Wie schon erwähnt, ist das Berechnen von s und t im Reellen keine Herausforderung. Theoretisch müsste sich ein Betrüger noch nicht einmal diese Arbeit machen, da er y auch einfach als $y = log_P(A^x \cdot B)$ berechnen könnte. Da diese Version nur zur grafischen Veranschaulichung dient, müssen wir für dieses Beispiel annehmen, dass das Logarithmieren auch in den reellen Zahlen schwer ist, was bedeutet, dass die einzige Möglichkeit, die einem Betrüger bleiben würde, das Raten der Parameter ist. Bei einer unendlichen großen Anzahl von Wahlmöglichkeiten ist es jedoch aussichtslos zu einem $x_{\mathcal{M}}$, welches beliebig von $\mathcal{M}$ (!) gewählt wird, eine Gerade $y = s_1 x + t_1$ zu finden, welche auch durch den Punkt $(x_{\mathcal{M}} | s x_{\mathcal{M}} + t)$ verläuft.

Doch nicht nur die Basics der Geradenchallenge können visualisiert werden, sondern auch, wie das Double Spending von Coins verhindert wird. Dazu betrachten wir uns die folgende Situation:

- $P, s, t, x_{\mathcal{M}}$ *seien so gewählt wie oben.*
- $\mathcal{U}$ *tätigt eine zweite Transaktion der Coin an einen weiteren Händler* $\mathcal{M}_2$.
- $x_{\mathcal{M}_2} = 4$.

Dem normalen Protokoll nach, würde $\mathcal{U}$ *nun* $y_{\mathcal{M}_2} = 11$ *berechnen, was bedeutet, dass er einen zweiten Punkt auf seiner Geraden preisgibt. Offensichtlich hat* $\mathcal{U}$ *auch nicht die Möglichkeit eine schneidende Gerade zur Berechnung von* y *zu verwenden, da der entstehende Punkt sowieso auf der ursprünglichen Gerade liegen muss. Diese Situation ist in Abbildung 3 zu sehen:*

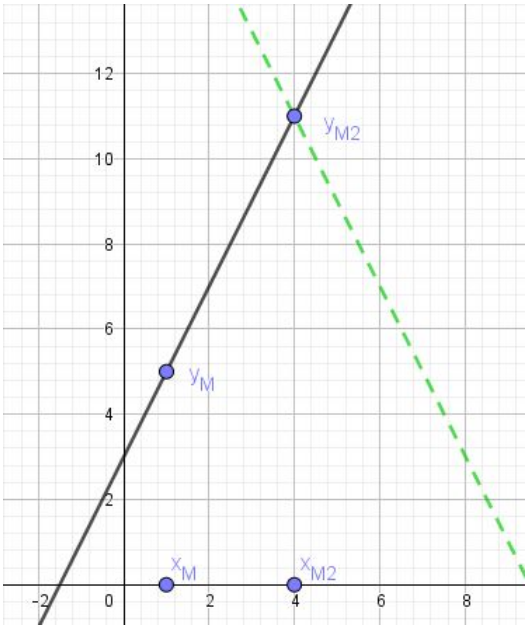


Abbildung 3: Verhindern des Double Spending im Reellen {fig:Gerade

Nicht nur können jetzt s *und* t *bestimmt werden, sondern im Falle der verallgemeinerten Geradenchallenge 2.7 auch die Identität* $I_{\mathcal{U}}$ *des Täters, was der Bank erlaubt entsprechende Maßnahmen gegen diesen einzuleiten.*

2.3 Peer-to-peer eCash

c:p2pECash}

In diesem Abschnitt werden wir uns mit einer dezentralisierten Version des eCash, **Bitcoin** [N+08], beschäftigen. Wie schon impliziert, handelt es sich hierbei um ein Netzwerk, dass sich um die verschiedenen Transaktionen der Nutzer kümmert. Der Erfinder von Bitcoin, Satoshi Nakamoto, hat also eine gänzlich neue Währung erschaffen, die komplett unabhängig von gängigen Währungen wie dem Dollar ist.

Auch für diese Version des eCash werden wir uns in den nächsten Abschnitten mit den mathematischen Grundlagen, sowie der Funktionsweise der Hauptanwendungen des Systems beschäftigen, wie von Koblitz, Menezes [KM16] und Nakamoto [N+08] beschrieben.

rung_bitcoin}

Vereinbarung

- $\mathbb{F}_q$ist der endliche Körper mit q Elementen.
- $E(\mathbb{F}_q)$ist die Verschwindungsmenge einer elliptischen Kurve E über $\mathbb{F}_q$.
- $(E(\mathbb{F}_q), +)$ ist eine Gruppe, die abkürzend mit $E(\mathbb{F}_q)$bezeichnet wird.
- $e \in E(\mathbb{F}_q)$ist das neutrale Element von $E(\mathbb{F}_q)$.
- $p \mid \#(E(\mathbb{F}_q))$, mit $p \in \mathbb{P}$.
- p hat eine ähnlich große Bitlänge wie q.
- $\mathcal{G} \leq E(\mathbb{F}_q)$ist die Untergruppe von $E(\mathbb{F}_q)$mit Ordnung p.
- $\mathcal{H} : \{0,1\}^* \to \{0,1\}^{256}$, ist eine Hashfunktion, die beliebige Bitstrings nach $\{0,1\}^{256}$ abbildet.
- Es ist schwer $x, y \in \{0,1\}^*$ zu finden, sodass $\mathcal{H}(x) = \mathcal{H}(y)$.
- Das Wissen über $\mathcal{H}(a)$ und $\mathcal{H}(b)$ gibt keine Aufschlüsse über $\mathcal{H}(x \; op \; y)$, wobei *op* eine beliebige binäre Operation auf $\{0,1\}^*$ ist.
- Die iterative Berechnung der Funktionswerte von $\mathcal{H}$ in $\{0,1\}^{256}$ gleicht einer Gleichverteilung über $\{0,1\}^{256}$.
- $\mathcal{H}' : \{0,1\}^* \to \mathbb{Z}/p\mathbb{Z}$, $b \mapsto \mathcal{H}(b) \bmod p$

Mit diesen Vorbedingungen können wir uns nun den zwei Hauptbestandteilen des Bitcoinsystems zuwenden: der *Rechenaufgabe*, sowie der *Signatur*. Letztere benötigt das folgende Lemma:

ur_bitcoin}

Lemma 2.20.

Sei $P \in \mathcal{G}$ ein beliebiger nicht-neutraler Punkt, $z, k \in \mathbb{Z}/p\mathbb{Z}$ beliebig und dadurch ein $Q = zP \in \mathcal{G}$ gegeben. Dann gilt:

$$\pi_x(kP) \equiv \pi_x(s^{-1}\mathcal{H}'(M)P + s^{-1}rQ) \bmod p \tag{5}$$

Mit $s = k^{-1}(\mathcal{H}'(M) + zr) \bmod p$

Beweis. Seien die Variablen wie im Lemma gegeben. Es gilt:

$$s = k^{-1}(\mathcal{H}'(M) + zr) \bmod p \Rightarrow s^{-1} = k(\mathcal{H}'(M) + zr)^{-1} \bmod p$$

Des Weiteren gilt:

$$\begin{aligned} s^{-1}\mathcal{H}'(M)P + s^{-1}rQ &= k(\mathcal{H}'(M) + zr)^{-1}\mathcal{H}'(M)P + k(\mathcal{H}'(M) + zr)^{-1}rQ \\ &= k(\mathcal{H}'(M) + zr)^{-1}\mathcal{H}'(M)P + k(\mathcal{H}'(M) + zr)^{-1}rzP \\ &= k(\mathcal{H}'(M) + zr)^{-1}P(\mathcal{H}'(M) + rz) \\ &= kP \end{aligned}$$

□

Definition 2.21: Signatur

{def:Signat

Angenommen ein Nutzer $\mathcal{U}$ möchte eine Nachricht M signieren, welche eine Zahlung an einen Händler $\mathcal{M}$ enthält. Dies geschieht nach dem folgenden Schema:

1. $\mathcal{U}$ wählt sich einen permanenten *private key* $z \in \mathbb{Z}/p\mathbb{Z}$, sowie einen permanenten *public key* $Q = zP \in \mathcal{G}$.
2. $\mathcal{U}$ wählt sich ein geheimes $k \in \mathbb{Z}/p\mathbb{Z}$ und berechnet kP, sowie $r = \pi_x(kP)$.
3. $\mathcal{U}$ wählt (r, s) als Signatur, mit $s = k^{-1}(\mathcal{H}'(M) + zr) \bmod p$.
4. $\mathcal{U}$ schickt M zusammen mit (r, s) an $\mathcal{M}$.

Der Händler kann nun die Signatur verifizieren, indem er wie in Lemma 2.20 beschrieben, die x-Koordinaten der beiden Punkte überprüft.

Schritt 1 der Definition 2.21 gleicht dem Erzeugen eines key-Paares mit Hilfe der ECDSA-Signatur [JMV01], wobei die Schritte 2 bis 4 das Signieren in der ECDSA-Signatur darstellen. Um die Herkunft einer Nachricht zu verifizieren, benötigen andere Nutzer nur den public key aus Schritt 1 [KM16].

Definition 2.22: Rechenaufgabe

{def:Recher

Die Rechenaufgabe, welche in der späteren Erklärung des Systems wichtig wird, besteht daraus eine Bitfolge l zu finden, sodass

$$\mathcal{H}(u||l) < b \tag{6}$$

{eqn:Recher

Wobei u eine gegebene Bitfolge, $\cdot||\cdot$ die Konkatenation zweier Bitfolgen darstellt und b die Bitfolgendarstellung einer ganzen Zahl $B \in \mathbb{Z}, 0 \leq B \leq 2^{256} - 1$ ist.

Beispiel 2.23. *Sei* $B = 2^{250}$ *und ein beliebiges* $u \in \{0,1\}^*$ *gegeben. Das Ziel der Rechenaufgabe ist es nun eine Bitfolge* $l \in \{0,1\}^*$ *zu finden, sodass* $\mathcal{H}(u||l) < b$*.Da die Bitfolgendarstellung*

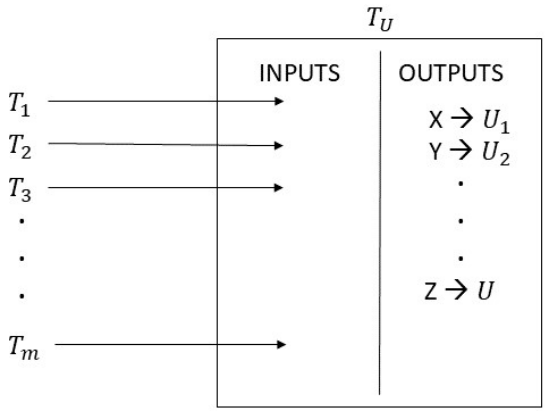
$$b = \underbrace{000000}_{6}\,1\,\underbrace{0\cdots0}_{249}$$

sechs führende Nullen hat, muss man, weil die Werte von $\mathcal{H}$ gleichmäßig auf $[0, 2^{256} - 1]$ verteilt sind, solange l erhöhen, bis $\mathcal{H}(u||l)$ einen Wert ergibt, der auch mindestens sechs führende Nullen hat.

Ein l, das die Ungleichung der Rechenaufgabe 2.22 erfüllt, wird auch ***proof-of-work*** *genannt.*

Definition 2.24: Transaktionen

henBitcoin} Transaktionen und „Coins“ sind bei dem Bitcoinsystem nicht ganz trennbar, da zu keinem Zeitpunkt weder physisch, noch in Form einer Datei auf einem Datenträger, wirklich eine Bitcoin „existiert“. So verschieden Bitcoin und das klassische Bankensystem auch sind, so haben sie gemeinsam, dass das Geld auf dem Konto nur eine Wertanzeige ist, die von ein- und ausgehenden Überweisungen/Transaktionen bestimmt ist. In einem gewissen Sinne führt Bitcoin diese Vorgehensweise mit dem folgenden Transaktionssystem noch weiter:



onBitcoin} Abbildung 4: Transaktion im Bitcoinsystem

Abbildung 4 zeigt eine allgemeine Transaktion eines Users $\mathcal{U}$. Die Empfänger dieser Transaktion sind auf der *Output*-Seite zu sehen $(\mathcal{U}_1, ..., \mathcal{U}_n, \mathcal{U})$. Die *Input*-Seite akzeptiert Hashwerte von Transaktionen, T_i, in denen $\mathcal{U}$ ein Rezipient (also in der Outputliste) war und somit einen gewissen Wert an Bitcoins überwiesen bekommen hat. Da eine Transaktion, mehrere Outputs haben kann, bezeichnen wir mit $c_i \in \mathbb{N}$ den Index, an dem $\mathcal{U}$ als Output in T_i vorkam. Wie auch in der Abbildung zu erkennen ist, kann sich ein User auch selbst in die Outputliste schreiben, was damit zusammenhängt, dass die Summe der Werte in den Input-Transaktionen natürlich nicht immer genau dem zu bezahlenden Preis gleicht, sondern ihn auch übersteigen kann. Damit $\mathcal{U}$ in einem solchen Fall nicht zu viel bezahlen muss, gibt er sich selbst als Output an, um so sein „Wechselgeld“ zu bekommen. Falls die Werte der Output-Transaktionen (auch das Wechselgeld) sich nicht zur Input-Summe aufsummieren, so wird der Rest automatisch als *Anreizlohn* (englisch: *Incentive*) gesehen, welcher in der nächsten Definition genauer beschrieben wird.

Will $\mathcal{U}$ nun also eine Transaktion tätigen, so schickt er die folgende Nachricht ins

Bitcoinnetzwerk:

$$c_1, T_1, ..., c_m, T_m, X, \mathcal{U}_1, Y, \mathcal{U}_2, ..., Z, \mathcal{U}, sign(\mathcal{U})$$

Wobei $sign(\mathcal{U})$ die ECDSA-Signatur des Users ist, welche dann im Netzwerk durch den *public key* von $\mathcal{U}$ verifiziert werden kann. Letzteres ist der Grund, warum andere User Transaktionen nicht einfach für sich behaupten und mit ihnen bezahlen können.

Nachdem geklärt ist, wie Nutzer valide Transaktionen im Bitcoinnetzwerk „in Auftrag“ geben können, fehlt nur noch ein wichtiger Teil des Systems: die **Blockchain**. Diese kommt durch die Anordnung von Transaktionen in Blöcken, die jeweils auf einen vorhergehenden Block verweisen, zu ihrem Namen. Nutzer, die solche Blöcke nach bestimmten Regeln zusammenstellen, werden *Miner* genannt. Die Regeln lauten, dass eine Transaktion nicht doppelt vorkommen darf, also weder innerhalb des Blocks, noch in einem Anderen und dass die Transaktionen valide sind. Durch diese Anordnung kann also auch von anderen Minern überprüft werden, ob eine Transaktion schon einmal „ausgegeben“ wurde oder ob ein Nutzer wirklich dazu berechtigt ist, die Transaktion als seine eigene zu behaupten.

Die **Blöcke** bestehen aus zwei Teilen: einem *Header* ($H||l$), sowie einem Merkle-Baum, der aus den Hashwerten der enthaltenen Transaktionen aufgebaut ist. Ersterer wird nach dem folgenden Schema konstruiert:

1. Der Miner berechnet die Hashwerte aller Transaktionen im Block.
2. Der Miner baut einen Merkle-Baum aus diesen Hashwerten auf.
3. Der Miner fügt die Merkle-Wurzel, sowie den Hashwert des vorangehenden Blocks zu H zusammen.
4. Der Miner löst die Rechenaufgabe 2.22, mit $u = H$, zu einem systemgegebenen B.
5. Der Miner nutzt $H||l$ als Header des neuen Blocks.

Falls ein Miner Glück hatte und als erster die Rechenaufgabe in Schritt 4 gelöst hat, so publiziert er seinen Block im Netzerk, sodass die anderen Knoten seine Validität überprüfen können. Falls nun zwei Miner zu fast gleicher Zeit einen Proof-of-Work errechnet haben, tritt der Fall ein, dass sich die Blöcke unterschiedlich schnell im Netzwerk über die Knoten verbreiten, was bedeutet, dass verschiedene Knoten die Blöcke zu verschiedenen Zeitpunkten (aber immer noch zeitlich nah beieinander) erhalten. Jeder Knoten rechnet mit dem zuerst angekommenen Block als letztes Glied in der Kette weiter, was dazu führt, dass sich **Gabelungen** (englisch: *Forks*) in der Blockchain bilden können. Nach einiger Zeit wird ein Pfad jedoch länger als alle anderen und somit als gültiger Hauptpfad in der Kette angesehen. Nur wenn neu gefundene Blöcke auch Teil dieses Hauptpfades werden, führt das System eine Überweisung im Wert von (im Moment) 12.5 Bitcoin an den Miner durch, was auch gleichzeitig die einzige Möglichkeit ist neue Bitcoins zu generieren.

3 Vereinfachte Kryptowährungen

{sec:ezCC}

Im folgenden Abschnitt wird eine vereinfachte Form des bereits vorgestellten Central Authority eCash eingeführt. Dies ist im Hinblick auf den didaktischen Teil dieser Arbeit wichtig, da man Schülerinnen und Schülern, auch in der Oberstufe, das Prinzip der ECC aufgrund fehlender algebraischer Grundlagen eher schlecht innerhalb eines kurzen Zeitraums beibringen kann.

Der Aufbau dieses Abschnitts sieht die Beschreibung einer ersten, sehr vereinfachten Form des Systems vor, gefolgt von einer Analyse seiner Schwachpunkte.

3.1 Erste Iteration des Systems

Um eine sehr vereinfachte Version des Central Authority eCash-Systems zu schaffen, muss man sich zuerst die wichtigsten Aspekte beziehungsweise Schritte verdeutlichen, damit diese auch im zugänglicheren System als Grundpfeiler bestehen bleiben. Diese grundlegenden Aktionen sind das *Abheben*, das *Bezahlen* und das *Einzahlen* von Coins. Nicht zu vergessen ist auch die Geradengleichung, welche besonders bei dem Bezahlen eine essentielle Rolle spielt und vor allem das Double Spending einer Coin verhindert. Die essentiellen Aspekte, zusammen mit den zugehörigen Ideen, werden nun vorgestellt.

Grundgedanke:
Die Quintessenz des Systems ist die Geradengleichung, welche in dieser Version nicht mit der Einführung zweier weiterer Variablen verallgemeinert wird. Unser Ziel ist es das Grundgerüst des Central Authority eCashs beizubehalten, damit spätere Schritte zur erweiterten Version einfacher sind.

Abheben:
Beim Abheben fordert ein Nutzer $\mathcal{U}$ Coin-Daten von der Bank $\mathcal{B}$ an. Diese Daten müssen, ähnlich wie im Original, etwas mit der Kontonummer des Nutzers zu tun haben. Des Weiteren sollten die Variablen der Geradengleichung einfließen, damit $\mathcal{U}$ später auch sein Wissen darüber (also seinen rechtmäßigen Besitz der Coin) einem Händler $\mathcal{M}$ beweisen kann.

Bezahlen:
Bei der „Übergabe“ überprüft $\mathcal{M}$ zuerst, ob $\mathcal{U}$ wirklich der Besitzer der Coin ist, indem er eine Challenge mit Hilfe der Geradengleichung erstellt. Sollte $\mathcal{U}$ diese bestehen, so gibt er implizit sein Wissen über die Variablen an $\mathcal{M}$ weiter. Weiterhin erstellen beide einen „Beweis“ , dass diese Transaktion wirklich stattgefunden hat. Eine Gleichung, die den Beweis und die Challenge enthält kann nun gebildet werden.

Einzahlen:
Das Einzahlen geschieht durch die Übergabe der Transaktionsdaten von $\mathcal{M}$ an $\mathcal{B}$. Die Bank muss nun die Beweisgleichung verifizieren und überprüfen, ob die Challenge schon einmal verwendet wurde, um letztendlich ein Double Spending zu verhindern.

3.1.1 Hauptanwendungen des Systems

Es werden nun, nach dem gleichen Schema wie zuvor, die einzelnen Hauptanwendungen des Systems vorgestellt.

Definition 3.1: Set-Up

bEzCentral} Das Set-Up ist im Vergleich zur ECC-Version denkbar einfach:
Bezeichne folgend $\mathcal{B}$ die Bank, $\mathcal{U}$ einen User und $\mathcal{M}$ einen Händler. Der Set-Up-Schritt läuft wie folgt ab:
Die **Bank** händigt $\mathcal{U}$ eine eindeutige Kontonummer $I_{\mathcal{U}} \in \mathbb{R}$ aus.

Definition 3.2: Abheben

hEzCentral} $\mathcal{U}$ will von $\mathcal{B}$ Coins abheben. Der Auszahlungsvorgang kann in einen Set-Up-Schritt und das eigentliche Abheben aufgeteilt werden.

Das **Set-Up**:

1. $\mathcal{U}$ wählt $s, t \in \mathbb{R}$ beliebig und geheim.
2. $\mathcal{B}$ wählt $r \in \mathbb{R}$ beliebig und speichert es.
3. $\mathcal{B}$ schickt r an $\mathcal{U}$.

Die **Auszahlung**:

1. $\mathcal{U}$ berechnet $A = I_{\mathcal{U}}^s$ und $B = I_{\mathcal{U}}^t$.

Nun besitzt $\mathcal{U}$ eine Coin $c = (A, B, r)$.

Um das Bezahlen zu ermöglichen benötigen wir noch eine Möglichkeit das Datum, die Händler-Kontonummer und die Coin-Daten ohne eine explizite Hashfunktion zu einer eindeutigen „Transaktions-ID“ zu verarbeiten. Die nächste Definition stellt solch eine Option vor.

Definition 3.3: Ersatz für Hashfunktionen

zEzCentral} Sei $d \in \mathbb{N}^{14}$ die Ziffernfolge, die entsteht, wenn man das Datum (TT/MoMo/JJJJ) und die Uhrzeit (HH/MiMi/SS) der Transaktion in der folgenden Form schreibt: $d = TTMoMoJJJJHHMiMiSS$.
Wir benutzen die Vorschrift

$$\begin{aligned} \mathcal{H} : \mathbb{N}^{14} \times \mathbb{R} \times \mathbb{R}^3 &\longrightarrow \mathbb{R} \\ (d, I_{\mathcal{M}}, c) &\mapsto 1.d * I_{\mathcal{M}} * A * B * r \end{aligned}$$

als eine Art Hashfunktionenersatz.

Nachdem wir nun die essentiellen Daten einer Transaktion in eine einzelne Zahl verrechnen können, läuft das Bezahlen sehr ähnlich zu 2.8 ab.

Definition 3.4: Bezahlen

{bezahlenEzCentral} Der Bezahlvorgang besteht aus den folgenden Schritten:

1. $\mathcal{U}$ schickt c an $\mathcal{M}$.
2. $\mathcal{M}$ schickt $\mathcal{U}$ seine Challenge $h_0 = \mathcal{H}(d, I_{\mathcal{M}}, c)$.
3. $\mathcal{U}$ berechnet $y = s * h_0 + t$.
4. $\mathcal{M}$ verifiziert $I_{\mathcal{U}}^{y} = I_{\mathcal{U}}^{s*h_0} * I_{\mathcal{U}}^{t} = A^{h_0} * B$.

Definition 3.5: Einzahlen

Das Einzahlen erfolgt mit diesen Schritten: {def:einzah

1. $\mathcal{M}$ schickt c, y und d an $\mathcal{B}$.
2. $\mathcal{B}$ verifiziert $I_{\mathcal{U}}^{y} = I_{\mathcal{U}}^{s*h_0} * I_{\mathcal{U}}^{t} = A^{h_0} * B$.
3. $\mathcal{B}$ überprüft mit den selben Methoden wie in 2.10, ob Double Spending der Coin c stattgefunden hat.

3.2 Analyse der Schwachpunkte

In diesem Abschnitt widmen wir uns den Schwachpunkten der ersten Iteration, indem wir systematisch alle Hauptanwendungen des Systems nacheinander analysieren.

Wir beginnen mit dem *Set-Up*: In dieser einfachen Version geschieht hier außer der Vergabe von Kontonummern nichts. Vergleicht man diesen Schritt mit der Originalversion, fällt auf, dass hauptsächlich das Setzen von öffentlichen und privaten Schlüsseln/Exponenten fehlt, was aber, je nachdem wie die folgenden Schritte definiert sind, erst einmal kein Sicherheitsrisiko per se darstellt. Das einzige Problem besteht darin, dass der Nutzer nicht wie im Original noch einen geheimen Exponenten u_1 wählen kann, welcher in späteren Schritten (zum Beispiel bei der Berechnung von C in Definition 2.4) zur impliziten Verifizierung der Identität genutzt werden kann. Des Weiteren will ein Nutzer natürlich immer noch, wie in den Zielen von eCash (Definition 2.1) schon angedeutet, so anonym wie möglich bleiben. Das Fehlen einer weiteren Anonymitätsebene (in Form eines geheimen Exponenten u_1) behindert dieses Vorhaben jedoch.

Das *Abheben* hat aufgrund seiner Simplizität einige Schwachpunkte hinzugewonnen. Der Vorgang besteht nur noch aus den rudimentären Schritten des Originals: $\mathcal{U}$ wählt die essentiellen Parameter der Coin s und t, während die Bank ein r speichert, um einerseits die Auszahlung einer Coin zu authentifizieren, aber auch, um später (ähnlich den Coin-Signaturgleichungen) die „Echtheit“ der besagten Coin überprüfen zu können. Zumindest wäre dies der Fall, wenn keine Angriffe auf A und B möglich wären. In Definition 2.5 kann man leicht erkennen, dass der Kommunikationskanal zwischen U und B abhörbar sein kann, da alle Werte, die

zwischen beiden Parteien ausgetauscht werden, durch die Unlösbarkeit des DLP, sowie der *Onewayness* von $\mathcal{H}$ gesichert sind. In Definition 3.2 kann ein Angreifer $\mathcal{A}$ durch einfaches Abhören des Kanals schnell Wissen über r erlangen. Da $\mathcal{B}$ keine Verbindung zwischen A, B und r gespeichert hat, kann sich der Angreifer selbst eine Coin $c' = (A' = I_{A'}^{s'}, B' = I_{A'}^{t'}, r)$ fälschen (sogenanntes *Coin Forging*). Zu diesem Zeitpunkt existieren nun zwei Coins, die von der Bank nach einem Handel zur Einzahlung angenommen würden. Der Angreifer muss also nur noch c' an einen Händler (am besten einen Komplizen) weitergeben, der dann die gefälschte Coin wieder einzahlt. Zu diesem Zeitpunkt nimmt die Bank an, dass c' die echte Coin ist, markiert r in ihrem System als ausgegeben und akzeptiert keine weiteren Einzahlungen von Coins, welche die gleiche „Signatur“ aufweisen. Selbst wenn $c = (A, B, r)$ bei der Bank als „abgehoben“ markiert wäre, könnte ein Angreifer mit Leichtigkeit die relevanten Variablen s und t berechnen, da die Potenzierung von $I_{\mathcal{U}}$ mit s und t in $\mathbb{R}$ leicht mit Hilfe des Logarithmus zu invertieren ist.

Der dritte Schritt, das *Bezahlen*, hat durch mehrere Einflussfaktoren sehr an Sicherheit verloren. Beim ersten Szenario gehen wir wieder davon aus, dass der Übertragungskanal nicht sicher und somit abhörbar ist. Sollte ein Angreifer $\mathcal{A}$ die Coin c in Schritt 1 von Definition 3.4 auslesen, kann er c mit folgenden Schritten auf sein Konto überweisen: Zuerst berechnet er sich selbst eine Challenge $h_0' = \mathcal{H}(d, I_{\mathcal{A}}, c)$, wobei er für den Datumsstring d sogar eine beliebige Bitfolge benutzen kann. Da s und t in $\mathbb{R}$ sehr leicht zu berechnen sind, kann der Angreifer $y = s * h_0' + t$ berechnen und hat somit alle Daten, die er braucht, um c bei der Bank einzahlen zu können.
Das zweite Szenario ergibt sich daraus, dass auch der Händler $\mathcal{M}$ ein potenzieller Angreifer sein könnte. Selbst wenn der Übertragungskanal gesichert wäre, kann solch ein Betrüger mit Leichtigkeit den Nutzer bestehlen: Nachdem $\mathcal{U}$ die Coin c verschickt hat, berechnet $\mathcal{M}$ eine neue Coin $c' = (A' = I_{\mathcal{U}}^{s'}, B' = I_{\mathcal{U}}^{t'}, r)$, wobei s' und t' beliebig aus $\mathbb{R}$ gewählt sein können. Dies wird getan, damit er nach dem Einzahlen von c' behaupten kann, dass $\mathcal{U}$ derjenige war, der die Coin doppelt ausgeben wollte und somit keine Ware verschicken oder Dienstleistungen erbringen muss. Nachdem $\mathcal{M}$ nun c' gefälscht hat, kann er nach dem gleichen Prinzip wie oben beschrieben vorgehen und c' bei der Bank einzahlen.

4 Didaktischer Teil

In diesem Abschnitt werden wir uns mit der Planung und Durchführung, sowie den Materialien, welche für die Modellierungstage 2019 erstellt wurden, von einem didaktischen und methodischen Standpunkt aus beschäftigen. Des Weiteren werden im Feedback-Abschnitt dieses Kapitels die Rückmeldungen der Schülerinnen und Schüler, sowie ihrer Lehrerin, dargestellt und diskutiert.

Bemerkung: Im Folgenden werden die Modellierungstage 2019 der Einfachheit wegen als „Lerneinheit“ bezeichnet.

4.1 Die Modellierungstage 2019

Um einen ersten Eindruck über die Umstände der Lerneinheit zu bekommen, muss geklärt werden, was die Modellierungstage sind und was deren Ziel ist: Das KOMMS („Kompetenzzentrum für mathematische Modellierung in MINT-Projekten in der Schule“) [KOM19] der Technischen Universität Kaiserslautern bietet im Rahmen des Projekts „Schulentwicklung für mathematische Modellierung in MINT-Fächern“ (SchuMaMoMINT), die Möglichkeit, dass Kurs- und Klassenverbände verschiedene Projektthemen bearbeiten. Der Zeitraum ist flexibel zwischen einem und drei Tagen wählbar, wobei in unserem Fall der zeitliche Rahmen auf zwei Tage begrenzt war.

Die Projektthemen werden klassischerweise vom KOMMS gestellt und sollen die Schülerinnen und Schüler mit authentischen, realen und modernen Fragestellungen konfrontieren, welche in Gruppenarbeit nach den Grundschritten der Modellierung, die noch in 4.7.4 vorgestellt werden, bearbeitet werden. Freundlicherweise wurde mir die Möglichkeit gegeben ein eigenes Projekt mit dem Titel „Erstellung einer Kryptowährung“ mit einzubringen, welches zusammen mit einem Standortproblem für Gepäckausgaben am Flughafen und dem Finden einer optimalen Besichtigungstour durch Berlin, welche ausnahmsweise auch von anderen Studenten erdacht waren, das Angebot an Themen bildete.

In den folgenden Tabellen kann man einen groben Überblick über den zeitlichen Rahmen der Veranstaltung erhalten:

Uhrzeit	**Dauer [min]**	**Phase**
10:30 Uhr	20	Vorstellung der Themen & Gruppenbildung
10:50 Uhr	130	Erste Arbeitsphase
13:00 Uhr	60	Essenspause
14:00 Uhr	120	Zweite Arbeitsphase

Tabelle 1: Zeitplan des ersten Tages {tab:Zeitpl

Der Offizielle Beginn ist um 10:30 Uhr angesetzt, wobei die Schülerinnen und Schüler ab 09:30 Uhr eine Stunde lang eine Ralley über den Universitätscampus durchführen. Man kann erkennen, dass es am ersten Tag zwei Arbeitsphasen für die Teilnehmenden gibt, welche durch eine Essenspause von 60 Minuten Länge

Uhrzeit	Dauer [min]	Phase
09:00 Uhr	150	Arbeitsphase & Präsentationserstellung
11:30 Uhr	60	Essenspause
12:30 Uhr	30	Feinschliff der Präsentationen
13:00 Uhr	60	Vorstellung der Präsentationen

Tabelle 2: Zeitplan des zweiten Tages

geteilt sind. Am zweiten Tag beginnt die Lerneinheit schon um 09:00 Uhr, wobei hier die Schülerinnen und Schüler einen Großteil ihrer Arbeitsphase für die Vorbereitung und das Üben der Präsentationen nutzen. Nach einer einstündigen Essenspause haben sie noch einmal 30 Minuten Zeit, um etwaige Verbesserungen an ihren Präsentationen durchzuführen, welche schließlich ab 13:00 Uhr vor allen Teilnehmenden, Betreuern und interessierten Professorinnen und Professoren vorgestellt werden.

4.2 Verlaufsplan

In den Tabellen 4 und 5 ist der Verlaufsplan der Lerneinheit einsehbar, damit der Leser eine Vorstellung von Inhalt und zeitlichem Rahmen bekommt. Der Start des Plans beginnt mit der ersten Arbeitsphase aus Tabelle 1.

Folgende Abkürzungen wurden benutzt:

Abkürzung	Bedeutung
UF	Unterrichtsform
LV	Lehrervortrag
UG	Unterrichtsgespräch
SD	Schüler*innendiskussion
SV	Schüler*innenvortrag
EA	Einzelarbeit
PA	Partnerarbeit

Tabelle 3: Bedeutungen der Abkürzungen

deutungAbk}

Phase	Inhalt	UF	Dauer
Einstieg	• Begrüßung + Vorstellung der Inhalte und Ziele • SuS analysieren „Kreislauf einer Coin“ • SuS erarbeiten Akteure und Grundlagen • Frage: *Überweisung oder Bargeld: Was passt besser dazu?* ⇒ SuS erkennen Anonymität des Bargelds ⇒ **Wie kann Bargeld simuliert werden?**	LV UG + SD	9 Min
Erarbeitung SetUp & Abheben	• Frage: *Was kommt an die Pfeile?* ⇒ SuS erkennen, dass Personalien und Kontonummer eng verbunden sind • Lehrerbehauptung: Coins „nur“ 3 reelle Zahlen! • Fragen sammeln ⇒ SuS klarmachen, dass diese Fragen die Grundlagen unserer Überlegungen bilden • Erklären des Abhebens ⇒ SuS lernen gleichzeitig Diagrammform • Genaue Erklärung was *geheim, beliebig* und *speichern* bedeutet!	UG SD LV + UG	6 Min
Sicherung SetUp & Abheben	• Durch Abheben-Step: *Was steckt alles in einer Coin?* • TIPP: Rückgriff auf Fragen: *Was ist Besitzbeweis?/Hat Bank wirklich ausgezahlt?* • SuS sammeln Antworten in Notizen ⇒ Danach auf Folie sammeln	SD + UG	3 Min
Erarbeitung Bezahlen	• Frage: *Was ist der nächste Schritt im Diagramm?* ⇒ *Bezahlen* • Frage: *Was heißt Bezahlen in unserem Kontext?* ⇒ SuS diskutieren Lösungsansätze • ⇒ Nutzer muss Wissen über s und t beweisen, ohne sie weiterzugeben! • Lehrereinwand: *Sind in mathematischer Modellierung: Benutzen also mathematische Objekte. Welches ganz einfache Objekt ist durch 2 Variablen eindeutig bestimmt?* ⇒ **Geraden!** • SuS bearbeiten Aufgabe	UG + SD SD GA/PA	12 Min

Tabelle 4: Verlaufsplan Teil 1 {tab:Verlau

Phase	Inhalt	UF	Dauer
Sicherung Bezahlen	• Besprechung der Aufgabe: SuS stellen kurz an Tafel vor & Erklären ihre Meinung ⇒ Wie kann $A^x \cdot B$ verwendet werden?	SV	5 Min
Erarbeitung Geradenchallenge & Sicherheitsprobleme	• Lehrer: Stellt Geradenchallenge an Tafel vor • Frage: *Warum funktioniert dieses Protokoll?* ⇒ SuS analysieren. • Frage: *Welche Sicherheitslücken sind aufgefallen?* ⇒ Logarithmus in $\mathbb{R}$ zu leicht! ⇒ Ist Motivation für Restklassenarithmetik	UG	9 Min
Sicherung Geradenchallenge & Sicherheitsprobleme	• SuS notieren sich in eigenen Worten, wie Geradenchallenge funktioniert • SuS notieren sich das Sicherheitsproblem mit reellen Logarithmen	EA	4 Min
Erarbeitung Restklassenarithmetik	• Lehrer: Erklärung Einordnungsschema von Zahlen in Eimern • SuS führen Bsp. fort und beantworten weiterführende Fragen: *Wie viele Zahlen gibt es in einem Eimer? Was ist mit dem Eimer mit der 5 oder 6?* • SuS formulieren anhand des Schemas die Definition von Restklassen in $\mathbb{Z}$ • SuS bearbeiten Aufgaben zu Restklassen ⇒ SuS entdecken eigenständig das DLP • Lehrer: Zeigt Excel-Script zur Veranschaulichung des DLP	LV + UG SD EA/PA LV	15 Min
Sicherung Restklassenarithmetik	• SuS notieren sich die Rechenregeln der Restklassenarithmetik • SuS formulieren eigenständig das DLP	EA SD	2 Min

Tabelle 5: Verlaufsplan Teil 2 {tab:Verlaufsplan2

4.3 Lernziele

Die Lernziele für diese Lerneinheit lassen sich wie folgt in Grob- und Feinlernziele unterteilen:

Groblernziel:

- Die Schülerinnen und Schüler erstellen eine eigene Kryptowährung.

Dieses Groblernziel lässt sich nun in mehrere Feinlernziele unterteilen, durch welche die Lerneinheit eine Grundstruktur erhält. Diese granularen Ziele sind im

Folgenden aufgelistet:

Feinlernziele: Die Schülerinnen und Schüler...

- ... nennen die Ziele einer Kryptowährung (Definition 2.1).
- ... nennen die Grundschritte einer Central Authority Kryptowährung.
- ... analysieren die Geradenchallenge (Definition 2.2) und begründen, warum diese als *Zero Knowledge Beweis* [Bar07] in einer Kryptowährung genutzt werden kann.
- ... analysieren die Sicherheit einer Beispielswährung hinsichtlich einfachen Angriffsszenarien.
- ... formulieren die Definition von Restklassen in $\mathbb{Z}/n\mathbb{Z}$ anhand eines Beispiels.
- ... rechnen mit Restklassen in $\mathbb{Z}/n\mathbb{Z}$.
- ... begründen, warum das DLP (siehe Def. 1.10) schwer ist.
- ... verschlüsseln Informationen mit Hilfe von Restklassenarithmetik, sowie des DLP.

4.4 Besondere Voraussetzungen

{sec:besVo

Die organisatorischen, sowie technischen Voraussetzungen der Lerneinheit lassen sich nach dem Kriterium aufteilen, ob sie während der Planungsphase bekannt waren oder nicht. Im Vorfeld waren die folgenden Informationen zugänglich: Die teilnehmenden Schülerinnen und Schüler besuchen alle den gleichen Mathematik-Leistungskurs in der elften Klassenstufe. Die Gesamtgruppengröße beläuft sich auf 15 Schülerinnen und Schüler, welche auch gleichzeitig die Gesamtgröße des Kurses ist. Die Schülerinnen und Schüler sollen sich eigenständig auf die Projektthemen in Gruppen aufteilen, die alle im gleichen Raum arbeiten. Weiterhin war bekannt, dass der zur Verfügung stehende Raum ungefähr 35-38 Personen fassen kann, in ihm eine große Tafel (vier gleich große Abschnitte) verbaut ist, es einen Beamer mit HDMI-Anschluss, sowie für alle Beteiligten der Lerneinheit kostenlosen Internetzugang gibt. Der zeitliche Rahmen für die interaktive Einarbeitungsphase sollte 60 bis 70 Minuten nicht überschreiten. Als besondere Voraussetzung sollten die Teilnehmer, wie in früheren Iterationen, sehr viel Modellierungsarbeit selbst übernehmen, was bedeutete, dass die Anzahl an Hilfen, wie zum Beispiel Arbeitsblätter mit Aufgaben als Denk- und Strukturierhilfe oder Stationen mit nach Schwierigkeit gestaffelten Hilfskärtchen, außerhalb der interaktiven Einarbeitungsphase gering gehalten werden sollten. Hierbei ist jedoch auch anzumerken, dass es ausdrücklich erlaubt war die Schülerinnen und Schüler bei Unklarheiten und drohendem Arbeitsstillstand durch Tipps oder hilfreichen Fragestellungen zu unterstützen.

Unbekannt war, wie viele Schülerinnen und Schüler jeweils an den einzelnen Projektthemen arbeiten, da sie, wie schon erwähnt, die Gruppen selbstständig bilden. Weiterhin hatte diese Tatsache zur Folge, dass es nicht sicher war, ob die Benutzung des Beamers oder der Tafel für die Einarbeitungsphase zur Verfügung stehen, da durch ihre ausgiebige Nutzung die anderen Gruppen gestört werden würden. Schließlich, die am schwierigsten zu überkommende unbekannte Voraussetzung, ist das fehlende Wissen über die Kurszusammenstellung. Es gab leider keine Informationen über das Leistungsprofil, den Grad der Heterogenität, besondere Umstände bei einzelnen Schülerinnen und Schülern oder den aktuellen Wissensstand beziehungsweise das Vorwissen.

4.5 Eigene Voraussetzungen

sec:eigVor}

Um die Planung der Lerneinheit noch besser nachvollziehen zu können, ist es wichtig, dass der Leser auch über die persönlichen Voraussetzungen der Lehrperson Bescheid weiß.
Mein eigenes Interesse an dem Fachgegenstand ist sehr hoch, da er größtenteils im Gebiet der Algebra anzusiedeln ist, aber auch einige Aspekte der Stochastik, einem weiteren meiner Interessensgebiete, widerspiegelt. Da „Kryptographie“ mein Vertiefungsgebiet im Studium darstellt und diese Lerneinheit im Zuge meiner Masterarbeit entsteht, schätze ich meine Sachkenntnis über die Erstellung von Kryptowährungen als fundiert ein. Lediglich die Grundschritte der mathematischen Modellierung, wie sie vom KOMMS vorgeschlagen sind, waren mir in dieser Genauigkeit nicht bekannt, weshalb ich mich damit auch im Abschnitt 4.7.4 des Unterrichtsverfahrens näher beschäftige.

Als *Fazit* lässt sich durch die Voraussetzungen 4.4 und 4.5 also zusammenfassen, dass die Planung und Durchführung dieser Lerneinheit von Anpassungsfähigkeit und Flexibilität geprägt sind, da vor allem über die Schülerinnen und Schüler im Vorfeld fast keine Informationen existieren. Es muss so geplant werden, dass schwächere Schülerinnen und Schüler eine solide Basis an Wissen und Kompetenzen aufbauen, damit sie zumindest ein *„minimal working example“* einer Kryptowährung erstellen, aber gleichzeitig ihre stärkeren Mitschüler gefordert werden und auch weiterführende Ideen in ihr eigenständig erdachtes System einbringen können. Die Lehrperson muss sich während der Durchführung flexibel an die Gruppenzusammenstellung und etwaige Fragen der Teilnehmer einstellen, somit die richtigen didaktischen, sowie auch methodischen Möglichkeiten auswählen und passende Antworten in verschiedenen Szenarios, welche durch die freie Arbeit der Teilnehmer entstehen können, finden.

4.6 Fachwissenschaftliche Bemerkungen

Eine detaillierte, fachliche Analyse des in der Lerneinheit vorkommenden Stoffes lässt sich in Kapitel 2: *Kryptowährungen* und Kapitel 3: *Vereinfachte Kryptowährungen* finden.

4.7 Didaktische Analyse

In diesem Abschnitt werden die Entscheidungen, welche die didaktische Planung bestimmen, konkret dargelegt und durch verschiedene Aspekte, wie zum Beispiel der Curricularen Forderungen oder auch der Bedeutung des Lerngegenstandes, begründet. Besonderes Augenmerk wird hierbei auch auf die didaktische Reduktion gelegt, da sie einen großen Teil der Planung dieser Lerneinheit ausmacht.

4.7.1 Einordnung in den Lehrplan

Die hier vorgestellte Lerneinheit „Erstellen einer Kryptowährung“ ist als eigenes Thema weder im Rahmenlehrplan der Sekundarstufe I [Min07], noch im Lehrplan der Sekundarstufe II [Min98] vorzufinden, was aber bei Exkursen und Projektthemen nicht verwunderlich ist. Leider ist jedoch auch das übergeordnete Thema „Kryptographie“ nicht direkt in den mathematischen Lehrplänen des Gymnasiums zu finden. Trotz diesen Aspekten findet sich eine Erwähnung der Wissenschaft über die Verschlüsselung von Informationen in den *Anregungen zur Umsetzung des Rahmenlehrplans Mathematik Rheinland-Pfalz* [Pä07]. Für die Klassenstufe 6 wird hier beim Schwerpunktthema **L5: Daten und Zufall** ein Projekt „Geheimschriften“ vorgeschlagen, in welchem Schülerinnen und Schüler einfache Chiffren wie die Cäsarverschlüsselung lernen, eigene Verschlüsselungen erstellen und diese dann mit Hilfe von Häufigkeitsanalysen brechen. Natürlich gibt es noch viel mehr Verbindungspunkte der Kryptographie mit Themen des Lehrplans: Die schon angesprochenen Häufigkeitsanalysen können auch in der Oberstufe während des Themas **Stochastik** vertiefend behandelt und deren Effektivität zu einem gewissen Teil bewiesen werden. Auch die selbst erstellten Chiffren können in der Oberstufe unter verschiedenen Gesichtspunkten untersucht werden. In der **Kombinatorik** können sich die Schülerinnen und Schüler beispielsweise die Frage stellen, wie viele Möglichkeiten der Chiffrierung eines Klartextes mit Hilfe einer Verschlüsselungsmethode es gibt.
Doch nicht nur die Kryptographie im Allgemeinen lässt sich zu Teilen in den rheinland-pfälzischen Lehrplänen finden, sondern auch Kryptowährungen im Speziellen sind bei Weitem nicht losgelöst davon zu betrachten: Die Zuordnung einer individuellen Kontonummer (*und wie dies im Genauen bei der eigenen Kryptowährung geschehen soll*) zu einem Nutzer spiegelt **Leitidee 4: Funktionaler Zusammenhang** wieder. Oftmals wird diese Eindeutigkeit sogar als erklärendes Beispiel bei der Einführung von Funktionen genutzt. Äquivalenzklassen im Allgemeinen, sowie Restklassen können in **Leitidee 1: Zahl und Zahlbereiche** verortet werden, da sie beispielsweise zur Definition der rationalen Zahlen $\mathbb{Q}$ genutzt werden, was sich als Exkurs in der Oberstufe anbietet. Restklassen in $\mathbb{Z}/n\mathbb{Z}$ sind über die Definition der Division mit Rest, welche schon in der Grundschule bearbeitet wird, so leicht zu verstehen, dass man sie auch in der Mittelstufe erarbeiten kann. Über die Behandlung von Restklassen als Beispiel eines anderen Zahlsystems in der Orientierungsstufe ist meiner Meinung nach abzusehen, da die Schülerinnen und Schüler erst ein solides Verständnis für „normale“ Stellensysteme wie das Dezimalsystem bekommen müssen. Das Diskrete Logarithmusproblem

könnte, vorausgesetzt Restklassen in $\mathbb{Z}/n\mathbb{Z}$ wurden behandelt, an mehreren Stellen des Lehrplans eingesetzt werden. Der Logarithmus in $\mathbb{R}$ ist in Klassenstufe 9/10 zu verorten. Hier könnte das DLP als Beispiel angebracht werden, dass eben nicht jedes mathematische Problem, obwohl es einfach aussehen mag, momentan eine schnelle Lösung besitzt und somit auch die Grenzen der modernen Mathematik aufgezeigt werden. Auch in der Oberstufe kann das DLP als Anwendungsbeispiel gebracht werden. Die scheinbare Zufälligkeit des Ergebnisses einer Potenzierung von Restklassen in $\mathbb{Z}/n\mathbb{Z}$ liegt in der Natur des Problems und ist auch ein Hauptgrund dafür, dass es so schwer ist. Genau diese Eigenschaft kann im Themenbereich **Simulation von Zufallsexperimenten** (in Leistungskursen verbindlich, im Grundkurs ein Wahlpflichtbereich) und somit auch **Pseudozufallszahlen** thematisiert werden.

Da mein zweites Studienfach Informatik ist und diese Lerneinheit nicht gänzlich als „Mathematikunterricht“ gewertet werden kann, ist es meines Erachtens nach auch interessant zu sehen, wo die angesprochenen Themen in den Informatiklehrplänen zu verorten sind. Im Lehrplan der Sekundarstufe I kann man einen ersten Grundstein für die Kryptographie erkennen, da im Themengebiet **Grundlagen der Kommunikation in Rechnernetzen beschreiben** der verbindliche Inhalt **Verschlüsselung von Daten** vorgeschrieben ist. Hierbei sollten aber zunächst ein mal, wie auch schon oben erwähnt, grundlegende Verfahren wie das Cäsarverfahren thematisiert werden. Als Exkurs oder Zusatzprojekt bei Pufferzeit kann man jedoch, da Informatik an Gymnasien erst ab der achten (Wahlpflichtfach) oder neunten (Wahlfach) Klasse angeboten wird, das DLP mit Restklassen in $\mathbb{Z}/n\mathbb{Z}$ anbieten.
In der Oberstufe hat man bessere Möglichkeiten Kryptowährungen in den Unterricht einzubeziehen. So ist im Themengebiet **Kommunikation in Rechnernetzen** der verbindliche Inhalt **Moderne Verfahren zur Verschlüsselung und Signierung** zu finden. Neben RSA kann hier auch die Verschlüsselung von Daten mit Hilfe des DLP behandelt werden. Des Weiteren sollen die Schülerinnen und Schüler auch Kommunikationssysteme und Protokolle im Allgemeinen analysieren und beschreiben können, wozu auch ein Central Authority Kryptowährungssystem mit seinen verschiedenen Grundschritten (SetUp, Abheben, Handeln, Einzahlen) zählen kann.

Fazit: Kryptographie und vor Allem Kryptowährungen lassen sich, wie zu erwarten war, in Mathematik oft nicht direkt und als ganzes Thema in den Unterrichtsfluss einbinden, sondern stellen eher eine gute Option für Projektwochen und Referate dar. Nichtsdestotrotz kann man an vielen Stellen im Mathematikunterricht Aspekte der beiden Themen als Beispiele oder weiterführende Inhalte darbringen. Für Informatik hingegen sind solche Kryptowährungssysteme relativ leicht auch in den normalen Unterrichtsverlauf einzubinden, da man sie als eine Art Kommunikationssystem auf Sicherheit hin überprüfen oder auch die *Grenzen von Algorithmen* durch das DLP erkennen kann.

4.7.2 Fachliche Voraussetzungen des Kurses

Da in dieser Lerneinheit ein mir unbekannter Kurs unterrichtet wird, habe ich mich dazu entschieden die fachlichen Voraussetzungen aus dem Unterricht auf das Nötigste zu reduzieren: Die Schülerinnen und Schüler...

- ... rechnen mit reellen Zahlen.
- ... benutzen die Potenzschreibweise, um eine mehrfache Multiplikation einer Zahl mit sich selbst vereinfachend darzustellen.
- ... nennen die allgemeine Geradengleichung.
- ... vereinfachen Terme mit Hilfe der Potenzregeln.
- ... vereinfachen Terme, welche ausschließlich Variablen beinhalten.
- ... berechnen den Rest einer ganzzahligen Division zweier Zahlen.
- ... benutzen einen Taschenrechner um große Zahlen schnell miteinander zu verrechnen.
- ... benutzen die Logarithmusfunktion um gesuchte Exponenten zu bestimmen.

Da es mir bekannt ist, dass die Teilnehmenden die elfte Klassenstufe besuchen, habe ich die folgenden Vorkenntnisse und Kompetenzen vorausgesetzt: Die Schülerinnen und Schüler...

- ... beschreiben und analysieren einfache Schaubilder.
- ... gehen in ihrem täglichen Leben mit Geld um.
- ... nennen in groben Zügen die Funktionsweise einer klassischen Bank.
- ... nutzen algorithmisches Vorgehen, um geordnete Abläufe zu generieren.

Weiteres Vorwissen oder auch Vorurteile der Schülerinnen und Schüler aus Medien und anderen Fächern sind zu vermuten, da Kryptowährungen und Sicherheit im Internet in der letzten Zeit ein oft angesprochenes Thema sind. Ich gehe davon aus, dass es einige technisch affine Teilnehmenden geben wird, welche sich entweder schon teilweise oder gänzlich mit bekannten Währungen wie Bitcoin [N$^+$08] oder Ethereum [B$^+$14] beschäftigt haben. Des Weiteren ist zu vermuten, dass manche Schülerinnen und Schüler ein eher negativ konnotiertes Bild von Kryptowährungen haben, da diese auf Grund der Anonymität oft in Verbindung mit illegalen Handlungen stehen.

4.7.3 Begründung und Bedeutung des Lerngegenstands

Warum gerade Kryptowährungen? Diese Frage ist berechtigt und soll hier kurz beantwortet werden. Laut einem Bericht der Zeit [Sch18] hatte die us-amerikanische Handelsplattform *Coinbase* im Jahre 2018 eine Nutzerzahl von 13,3 Millionen, welche sich zum Vorjahr aus von 5,5 Millionen mehr als verdoppelte. Obwohl der Hype um das digitale Bargeld etwas abgeflacht ist, hat man mit Kryptowährungen ein sehr aktuelles Thema, von dem viele Menschen schon gehört haben, aber trotzdem keine fundierte Meinung besitzen. Dieses schon bestehende Interesse nutzen wir aus, um das Basiskonzept von Central Authority Kryptowährungen einzuführen und somit einen ersten Einblick in die „Blackbox Kryptowährung“ und kryptographische Arbeitsweisen zu geben. Doch nicht nur Kryptowährungen im Speziellen, sondern auch die in ihnen verwendeten kryptographischen Methoden sollen so anhand dieses motivierenden Beispiels den Schülerinnen und Schülern nahegebracht werden, damit diese verschiedene Kompetenzen entwickeln. Dazu gehört, dass sie **die vorgestellten Protokolle in einem passenden Kontext korrekt anwenden** und diese auch **anpassen, um sie kompatibel mit wechselnden Grundlagen von Kryptowährungen zu machen**. Natürlich werden auch viele mathematische Kompetenzen gefordert. Die Teilnehmenden müssen beispielsweise **mathematisch argumentieren**, um sich klar zu machen, warum das DLP für geeignete n in $\mathbb{Z}/n\mathbb{Z}$ schwer zu lösen ist. Da die einführende Präsentation nicht alle Grundschritte einer Central Authority Kryptowährung abdeckt und vor allem nur in rudimentären Zügen, müssen die Schülerinnen und Schüler dieses **Problem mathematisch lösen**. Das bedeutet, dass sie sich in ihren Gruppenarbeitsphasen, welche das **Kommunizieren** durch Diskussion und Zusammenarbeit fördern, selbstständig neue Fragestellungen erarbeiten müssen, um Schritt für Schritt ihre eigene Kryptowährung zu verbessern. Weiterhin wird durch den engen Zusammenhang zwischen Geraden, der allgemeinen Geradengleichung und linearen Funktionen die Kompetenz geschult **mathematische Darstellungen zu verwenden**, da die Schülerinnen und Schüler Aspekte von allen diesen Darstellungsmöglichkeiten betrachten müssen, um das Geradenprotokoll zu verstehen. Einen großen Einfluss hat auch das **Umgehen mit symbolischen, formalen und technischen Elementen der Mathematik**, da die Planung einer Kryptowährung stark vom kreativen Einsatz von Variablen, Termen und Gleichungen bestimmt ist. Hinter vielen dieser Gleichungen liegt jedoch eine Idee, welche so von der natürlichen in eine symbolisch-formale Sprache transferiert wurde. Letztlich fehlt nur noch die Kompetenz, welche auch Hauptsächlich von den Modellierungstagen verbessert werden soll: das **mathematische Modellieren**. Wie schon erwähnt müssen reale Probleme, wie zum Beispiel der „Transfer“ einer Coin von einem Nutzer zum Nächsten oder auch der Aufbau einer Währungseinheit an sich, in mathematische Modelle übersetzt und anhand deren Eigenschaften dann passend in den verschiedenen Gleichungen benutzt werden.

errichtsverfahren}

4.7.4 Unterrichtsverfahren

Die Lerneinheit ist stark problemorientiert angelegt: Am Anfang jeder Phase der interaktiven Präsentation steht eine Fragestellung, beziehungsweise ein Problem, welche sich automatisch aus den vorhergehenden Abschnitten ableitet. Das Ausgangsproblem „Erstellung einer Kryptowährung“ ist dadurch motiviert, dass man einen Weg dafür finden will auf elektronischem Wege wie mit Bargeld und all seinen Vorteilen, zum Beispiel Anonymität und Nicht-Zurückverfolgbarkeit von Transaktionen, bezahlen zu können.

Wie schon erwähnt, ist der Verlauf der Lerneinheit nicht nur problemorientiert angelegt, sondern folgt auch den Grundschritten der Modellierung, wie sie vom KOMMS vorgeschlagen werden:

1. **Problem des Anwenders:** Ein (oftmals nicht mathematisch versierter) Anwender hat ein Problem, welches er in „normaler“ Sprache formuliert. (Hier: *Ich würde gerne online wie mit Bargeld bezahlen können.*)

2. **Exakte Erfassung (Definition) des Problems:** Was ist die Ausgangssituation? Was ist das Ziel? Gibt es (potenziell vom Anwender gegebene) Einschränkungen? (Hier: *Was sind die Grundschritte des Systems und wie sollen sie funktionieren?*)

3. **Mathematische Modellbildung:**

   (a) **Analyse des Problems:** Welche besonderen Eigenschaften hat das Problem?

   (b) **Mathematische Beschreibung des Problems:** Wie kann man das Problem in Gleichungen, Terme oder mathematische Objekte fassen?

   (c) **Suche nach geeigneten mathematischen Verfahren:** Welche Vorgehensweisen sind schon bekannt? Welche müssen erarbeitet werden?

   (d) **Lösung des mathematischen Problems:** Wie genau sollen die erarbeiteten Verfahren angewandt werden? (Kann man Computer einsetzen?)

4. **Interpretation der Lösung:** (Im Hinblick auf das anfängliche Problem des Anwenders) Kann dieses spezielle Problem nun gelöst werden? Wie gut ist die gefundene Lösung?

5. **Beschreibung der Lösung in Sprache des Anwenders:** Wie beschreibe ich dem (oftmals nicht mathematisch versierten) Anwender die Lösung? Wie bricht man die (potentiell komplexen) mathematischen Ergebnisse auf ein verständliches Level herunter? Gibt es wichtige Punkte, die unbedingt genannt werden müssen? (Hier: *Präsentation vor der Klasse.*)

4.7.5 Didaktische Konzeption

Inhaltliche Schwerpunkte: Da der zeitliche Rahmen sehr klein ist, wird der inhaltliche Fokus der Lerneinheit auf zwei Aspekten von Kryptowährungen liegen, den Grundschritten (vor allem die Geradenchallenge) eines solchen Systems, sowie die Verschlüsselung von Daten mit Hilfe des diskreten Logarithmusproblems in $\mathbb{Z}/n\mathbb{Z}$. Als größerer inhaltlicher Zusammenhang sind hier Kryptowährungen im Allgemeinen und natürlich auch Kryptographie anzubringen.

Alternative Stoffauswahl: Passend zu den zwei inhaltlichen Schwerpunkten betrachtet man hier auch verschiedene Wege, welche aber nicht immer unabhängig voneinander gegangen werden können. Entscheidet man sich beispielsweise dafür eine Peer-to-Peer Kryptowährung und deren Grundschritte zu erarbeiten, kann es vorkommen, dass nicht das Verschlüsseln der Daten im Vordergrund steht, sondern größtenteils nur das Berechnen des Proof-of-Work (vergleiche Definition 2.22). Das bedeutet also, dass mit verschiedenen Kryptowährungen oftmals andere kryptographische Methoden in den Vordergrund rücken. Dies ist wiederum der Grund, warum in der Lerneinheit ein relativ allgemeines System (mit einer Bank) vorgestellt wird, denn die Schülerinnen und Schüler sollen meiner Meinung nach nicht durch spezielle Eigenheiten, welche oft durch die komplexeren kryptographischen Methoden als Nebenprodukt entstehen, abgelenkt werden.
Fazit: Da schon bestehende Central-Authority Kryptowährungen zu spezifische Eigenheiten mit sich bringen und netzwerkgestützte Alternativen wie zum Beispiel Bitcoin nicht das Feinlernziel „*Die Schülerinnen und Schüler nennen die Grundschritte einer Central Authority Kryptowährung*“ erfüllen können, habe ich mich dafür entschieden ein leichtes, aber trotzdem allgemeines System zu behandeln.

Teilaspekte des Lerngegenstands: Der behandelte Lerngegenstand kann in mehrere immanente Teilaspekte zerlegt werden, die in diesem Abschnitt durch *Kursivschreibweise* kenntlich gemacht sind.
Bei Betrachtung von Central Authority Kryptowährungen fällt auf, dass diese hauptsächlich von drei Themengebieten (den *Grundschritten*, der *Definition einer Coin*, sowie den *kryptographischen Methoden*) bestimmt sind, welche auch wiederum in mehrere Aspekte unterteilt werden können. Die Grundschritte bestehen aus dem *Abheben-*, *Bezahl-* und *Einzahlenschritt*, welche eng miteinander verflochten sind. Nicht nur die drei grundlegenden Schritte des Systems bedingen sich gegenseitig, sondern auch die *Definition einer Coin*, die widerspiegelt welche Informationen, die *zu Variablen modelliert wurden*, hauptsächlich in die *aufgestellten Gleichungen* der Grundschritte einfließen. Schließlich werden *kryptographische Methoden* benötigt, um Informationen auch über unsichere Kanäle verschicken, oder Zero Knowledge Beweise durchführen zu können. Ersteres wird in dieser Lerneinheit durch das *Problem des diskreten Logarithmus* mit *Restklassen in* $\mathbb{Z}/n\mathbb{Z}$ erreicht. Sein Wissen über Informationen zu beweisen, ohne dass man diese jemandem verrät wird hier mit Hilfe der *Geradenchallenge* vollbracht. Man erkennt, dass auch die großen Aspekte nicht exklusiv voneinander betrachtet werden können, da das Bezahlen auch in der vereinfachten Version grundlegend

durch die Geradenchallenge definiert ist.

Alternative Strukturierung: Wie schon in „Teilaspekte des Lerngegenstandes ersichtlich“ sind die einzelnen Aspekte so stark miteinander verwoben und bauen aufeinander auf, dass sich nicht viele natürliche Möglichkeiten ergeben wie sie strukturiert werden können. So ist es beispielsweise nicht möglich die Grundschritte genauer als auf genereller Ebene als ersten Schritt zu betrachten, da die Protokolle –und die darin enthaltenen Berechnungen– die Daten aus den Coins benötigen.
Es gibt jedoch auch gewisse Freiheitsgrade bei der Strukturierung des Lerngegenstandes. Man könnte mit dem Bezahlen beginnen, die ersten Überlegungen zur Geradenchallenge anstellen und somit die zentrale Idee dieser Kryptowährung als erste Erkenntnis gewinnen. Dies hat jedoch den Nachteil, dass von den Schülerinnen und Schülern ein hohes Maß an Abstraktionsvermögen abverlangt wird, da sie noch keine Coins definiert haben und diese somit *komplett* als „ungreifbare Daten“ behandeln müssen. Mit Hilfe von Lemma 2.7 kann man die Geradenchallenge erweitern, sodass der Umfang der Coindaten erst einmal nicht relevant ist und so erst später die Definition einer Coin einbringen. Obwohl Zero Knowledge Beweise für Schülerinnen und Schüler interessant sein mögen, ist es doch eher unmotivierend das Bezahlen ohne die explizite Währung zu betrachten und auf später vertröstet zu werden.
Führt man die Coins jedoch vor den Grundschritten eingeführt, hat man zumindest die Wahl, ob das Bezahlen oder Abheben als erster Aspekt betrachtet wird. Lediglich das Einzahlen sollte der zuletzt betrachtete Schritt sein, da die Hauptidee bei diesem aus dem Übertragen und Verifizieren der Handelsdaten besteht. Die größte Freiheit hat man bei der Wahl, ob die Restklassenarithmetik und das DLP vor oder nach den Grundschritten behandelt werden sollen. Meiner Meinung nach ist es auch eine valide Entscheidung diese *vor* den Grundschritten zu behandeln. Die Schülerinnen und Schüler sehen solch ein Kryptowährungssystem dann eher als reines Anwendungsbeispiel an. Obwohl der Lehrplan eine wissenschaftspropädeutische Vorgehensweise und somit auch innermathematische Motivationen für den Leistungskurs akzeptiert, bin ich der Meinung, dass man oft einen problemorientierten Ansatz vorziehen kann, was sich auch in meiner Entscheidung – zuerst eine Version einer Kryptowährung vorzustellen, die versucht ohne Restklassenarithmetik auszukommen– widerspiegelt, denn diese Vorgehensweise zeigt den Nutzen und die Notwendigkeit der Restklassenarithmetik nämlich ganz natürlich als *Lösung eines Problems* (hier: Der Logarithmus in $\mathbb{R}$ ist zu leicht zu berechnen.)

Zugänge und Interessen: Da es im Zeitraum der Planung dieser Lerneinheit keine aktuellen Nachrichtenbeiträge oder andere Vorfälle, die mit Kryptowährungen in Verbindung stehen, gab, fiel diese Option leider weg. Sie ist wegen des starken Realitäts- sowie Gegenwartsbezugs eigentlich einer meiner bevorzugten Zugänge. Für diese Lerneinheit fällt die Wahl auf den Alltagsbezug, denn schon in der Themenpräsentation (siehe Anhang 7.1) sind Probleme angesprochen, die bestimmt jeder, der schon einmal eine Rechnung per Überweisung bezahlt (oder auch hat bezahlen lassen) hat, kennt: Wir leben im Jahr 2019 und das

Bezahlen via Überweisungsträger dauert immer noch mehrere Tage, da die Transaktion über die Zwischenstation Bank ausgeführt werden muss. Meiner Meinung nach kann man mit dem Thema der Lerneinheit auch gut die Interessen vieler Schülerinnen und Schüler im Leistungskurs ansprechen, denn Kryptowährungen sind geheimnisvoll, ein für die Teilnehmenden bisher eher unbekanntes Anwendungsgebiet der Mathematik und standen schon oft im Rampenlicht der Medien, in denen sie oftmals in Verruf geraten sind, was sie meines Erachtens nach nur noch interessanter macht. Diese Tatsachen gepaart mit der Möglichkeit *selbst* eine *eigene* Kryptowährung erstellen zu können erscheint mir als sehr motivierend für Schülerinnen und Schüler eines Mathematik-Leistungskurses. Schließlich habe ich mich noch dazu entschlossen keine Informatik- oder Computerkenntnisse vorauszusetzen, damit auch weniger technikaffine Teilnehmende nicht abgeschreckt werden.

Vermutete Schwierigkeiten: Meiner Meinung nach könnte es bei der Durchführung mehrere Schwierigkeiten geben, die es gilt zu überwinden. Die erste ist die potentielle Begriffsverengung, welche generell durch die Präsentation dieser Beispielswährung entstehen kann. Schülerinnen und Schüler könnten annehmen, dass *alle* Kryptowährungen mit Coins der Form $c = (A, B, r)$ funktionieren. Als Lösung dafür muss die Lehrperson immer wieder betonen, dass die vorgestellte Kryptowährung nur *ein Beispiel*, stark vereinfacht und dazu gedacht ist, dass die Teilnehmenden einen ersten Anhaltspunkt für ihre eigene Währung haben. Eine weitere Schwierigkeit sehe ich darin, dass manche Schülerinnen und Schüler nicht über die nötige Abstraktionskompetenz verfügen, um zu verstehen, dass Coins nur eine Art Beweis dafür sind, dass man wirklich einen gewissen Gegenwert besitzt, die Währung generell also gedeckt ist. Die Lösung für dieses Problem ist relativ simpel: Jeder Teilnehmende kennt „normales“ Geld, wie zum Beispiel Euro. Man nimmt also einen Geldschein aus seinem Portemonaie und macht den Schülerinnen und Schülern klar, dass dieser Schein auch „nur“ ein Stück Papier ist und bestimmt keinen Warenwert von beispielsweise 20 Euro hat. Als eines der größten Probleme sehe ich die Analyse der Sicherheit, da die Teilnehmenden wahrscheinlich noch nie Protokolle detailliert auf Sicherheitslücken geprüft haben. Für die Lösung sehe ich hier verschiedene anregende Fragestellungen seitlich der Lehrperson vor, also beispielsweise *Was passiert wenn jemand versucht eine Coin doppelt auszugeben?*. Die Schülerinnen und Schüler müssen sich so immer noch Gedanken über die Folgen machen *und* herausfinden, wie man das Problem beheben kann. Diese Methode mag zwar etwas faul wirken, aber das detaillierte Analysieren *aller* Sicherheitslücken ist auch nicht einer der zentralen Inhalte der Stunde. Zusätzlich sollten die Teilnehmenden nach ein oder zwei in solch einer Weise gestellten Hilfen auch selbst verstanden haben, welche Fragen man sich stellen kann, um Sicherheitslücken auszuloten. Die letzte Schwierigkeit sehe ich im Verständnis des diskreten Logarithmusproblems. Die Schülerinnen und Schüler werden zwar *selbst* das Problem entdecken, aber um das ganze Ausmaß des DLP begreifen zu können, habe ich eine Visualisierung programmiert, welche ihnen zeigen soll, dass das Potenzieren zufällige Muster entstehen lässt und auch eine Beispielrechnung vorbereitet, die zeigt, wie lange es dauern würde, um alle

Potenzen (modulo einer 300-stelligen Zahl) durchzuprobieren 7.5.

Didaktische Reduktion: Um ein solch modernes und vor allem wirtschaftlich interessantes Thema wie Kryptowährungen für Schülerinnen und Schüler zugänglich zu machen, ist es nicht verwunderlich, dass manche fachlich komplexen Aspekte aus didaktischen Gründen reduziert werden müssen. Jedoch können einige dieser Reduktionen auch zu einem Vorteil gewandelt werden.
Die wohl offensichtlichste Reduktion ist das Ersetzen der Verschlüsselung von Daten mit Hilfe von elliptischen Kurven (siehe Abschnitt 1.1.1). Ich habe mich dafür entschieden, da sie weder zu meiner Zufriedenheit (oder auch der Teilnehmenden) innerhalb von ein paar Stunden fachlich fundiert erarbeitet werden können. Des Weiteren wird ECC weder benötigt, um die Grundideen dieses Typs von Kryptowährung zu verstehen, noch um eine eigene Version davon zu erstellen. Weitere didaktische Reduktionen habe ich bei der Erstellung der Beispielkryptowährung in Form vom Verkleinern der Coindaten vorgenommen (vergleiche 2.5 und 3.2). Dies ist hauptsächlich aus zwei Gründen geschehen: Oftmals bedeuten mehr Variablen in der Coindefinition mehr und vor allem auch komplexere Gleichungen und Protokollschritte, welche, wenn man in der Erstellung einer neuen Kryptowährung noch nicht geübt ist, diese erheblich erschweren und gleichzeitig auch mehr und mehr die grundlegenden Ideen in den Hintergrund rücken lassen. Weiterhin wurden Hashfunktionen und die Tatsache, dass man für das DLP im besten Fall einen Erzeuger als Basis verwendet nicht direkt in der interaktiven Präsentation vorgestellt, da diese als Puffermaterial für schnelle Gruppen eingesetzt werden und deswegen im Skript erwähnt sind. Aus den gleichen Gründen wird auch die Wohldefiniertheit der Addition, sowie Multiplikation von Restklassen in $\mathbb{Z}/n\mathbb{Z}$ nicht direkt präsentiert und für schnelle, interessierte Schülerinnen und Schüler als Zusatzaufgabe ermöglicht (siehe Anhang 7.2).

4.7.6 Methodische Überlegungen

In diesem Abschnitt wird erörtert, *wie* und *warum* der Lerngegenstand innerhalb der Lerneinheit erarbeitet wird. Meiner Meinung nach sind didaktische und methodische Überlegungen nicht gänzlich unabhängig voneinander zu betrachten, weshalb an manchen Stellen Referenzen entstehen.

Generell ist die Lerneinheit problemorientiert angelegt, da sich die Schülerinnen und Schüler nach jedem Sinnabschnitt wieder auf natürliche Weise neue Fragen stellen müssen, anhand derer sie dann ihre weitere Vorgehensweise planen und Lösungen erarbeiten. Weiterhin kann die Lerneinheit in zwei größere Teile zerlegt werden: die interaktive Präsentation, sowie die eigenständige Projektarbeit, wobei sich der erste Teil eher als fragend-entwickelnd einstufen lässt. Meiner Meinung nach ist es definitiv möglich den Lerngegenstand auch in einer freieren Arbeitsmethode wie Stationenarbeit oder einem Gruppenpuzzle von den Schülerinnen und Schülern erarbeiten zu lassen. Aufgrund des sehr begrenzten Zeitrahmens, den Vorgaben des KOMMS und meinem Wunsch den Teilnehmenden so viel Zeit wie möglich für die eigenständige Erstellung ihrer Kryptowährung in der Projektarbeitsphase zu geben, habe ich mich für eine interaktive

Präsentationsform entschieden, in welcher die Schülerinnen und Schüler dennoch Aufgaben selbstständig lösen, sowie Fragen *und* Antworten darauf in Diskussionen erarbeiten müssen.
Die Erkenntnisschritte sind durch die Didaktik weitgehend festgelegt. Die Teilnehmenden erkennen durch die Beschreibung des Kreislaufs einer Coin (6.4 Folie 4) selbstständig, wer die Akteure in unserem System sind und welche Grundschritte es zu beachten gibt. Um das Verständnis zu überprüfen und auf einen wichtigen Punkt hinzuarbeiten, ist die Frage nach der Ähnlichkeit zu Transaktionen via Überweisungsträger oder Bargeld vital, denn die Grundidee solch eines Systems ist vor allem die Simulation und somit auch Ausnutzung der Vorteile von Bargeld. Eine ähnliche Idee wird im SetUp-Schritt (6.4 Folie 6) verfolgt. Dadurch, dass die Schülerinnen und Schüler selbstständig herausfinden, was die Pfeile zwischen Nutzer und Bank darstellen, soll ihnen der enge Zusammenhang zwischen Nutzerdaten und Kontonummer bewusst gemacht werden. Bei der Definition einer Coin (6.4 Folie 7) habe ich mich dazu entschieden den Impuls von Lehrerseite aus zu geben und somit Fragen bei den Schülerinnen und Schülern aufzuwerfen, welche auf der Folie gesammelt werden. Diese Fragen sind die Grundlage für das weitere Vorgehen. Da die Teilnehmenden noch keinen Kontakt mit Kryptowährungen haben und sich somit auch nicht vorstellen können, wie die eingeführten Variablen dazu benutzt werden Coins abzuheben, habe ich mich dafür entschieden mit den Schülerinnen und Schülern einen analytischen Weg zu gehen. Das Abheben (6.4 Folie 8) wird Schritt für Schritt vorgestellt und gleichzeitig auch eine Methode gezeigt, wie man solche Protokolle übersichtlich darstellen kann. Die folgende Diskussion über die Eigenschaften von Coins ist sehr wichtig für das Verständnis von Kryptowährungen. Durch Beispiele wie das Vorzeigen eines Euroscheines erkennen die Schülerinnen und Schüler, dass sie nur eine Art Beweis für den Besitz eines entsprechenden Gegenwertes sind. Als Übergang wird von den Teilnehmenden noch einmal kurz wiederholt, welchen Schritt des Kreislaufs man jetzt abgearbeitet hat und welcher jetzt Thema der Überlegungen sein sollte: Das Bezahlen. Hierbei ist es auch wieder wichtig, dass die Schülerinnen und Schüler *selbst* erkennen, dass es erst einmal wichtig ist zu verstehen, was „Bezahlen“ hier überhaupt bedeutet. Nachdem diese Frage gestellt worden ist, sollte eigentlich relativ schnell auch die Idee aufkommen, dass es etwas mit den Variablen s und t zu tun hat. Um dieses Problem zu lösen, bekommen sie einen Denkanstoß in Form eines Tipps, mit Hilfe dessen sie dann darauf kommen, dass Geraden hilfreich sein werden. Jedoch ist das Rätsel hier noch nicht ganz gelöst, da man immer noch nicht weiß, wie ein Zero Knowledge Beweis damit funktionieren soll. Dazu sollen die Schülerinnen und Schüler eine Aufgabe lösen, welche durch Tipps in der Schwierigkeit variiert werden kann, um ein erstes Gefühl für die Geradenchallenge zu bekommen, welches sie dann auch in der Gruppe versuchen zu erklären. Das vollständige Verständnis kommt durch den Einsatz der folgenden Methode: Der Gruppe wird an einem Tablet-Bildschirm die Geradenchallenge Schritt für Schritt vorgestellt. Der Unterschied zum vorherigen analytischen Ansatz ist nun, das sie nicht nur beschreiben sollen, was passiert, sondern auch, *warum* dieses Protokoll einen Zero Knowledge Beweis darstellt. Damit weiter-

hin ein relativ zügiger Ablauf gesichert werden kann, sollen die Schülerinnen und Schüler bei den Sicherheitsproblemen auch wieder im Plenum Ideen sammeln, damit zeitnah das Problem der einfachen Berechenbarkeit des Logarithmus im Reellen genannt wird, was auch gleichzeitig die Motivation für Restklassenarithmetik darstellt. Hier soll sich die Gruppe anhand eines durchgespielten „Algorithmus-Beispiels“ selbständig die Definition eines Restklasse in $\mathbb{Z}/n\mathbb{Z}$ erarbeiten. Da die Rechenregeln recht naheliegend sind, werden sie präsentiert (6.4 Folie 19) und zur Überprüfung des Verständnisses eine selbstdifferenzierende Aufgabe gestellt, welche auch für schnellere Schülerinnen und Schüler mit Hilfe eines Zusatzes die Möglichkeit bietet einen passenden Übergang zur Potenzschreibweise zu finden. Die folgende Aufgabe (6.4 Folie 20) hat zwei Funktionen. Zum einen soll sie sicherstellen, dass die Gruppe das Potenzieren von Restklassen verstanden hat und zum anderen sollen die Schülerinnen und Schüler durch das „einfache Aussehen“ der Aufgabe noch mehr verwundert werden, dass das Logarithmusproblem im Restklassenfall sehr schwer zu lösen ist. Um diese *selbstständig* gemachte Erfahrung noch zu verdeutlichen, wird mit den Teilnehmenden eine Beispielrechnung für die Dauer des Ausprobierens aller Möglichkeiten unter der Verwendung eines großen Moduls (>300 Stellen) 7.5 gerechnet und um auf den scheinbaren Zufallscharakter weiter hinzuweisen ein Excelprogramm zur Visualisierung des DLP mit Restklassen in $\mathbb{Z}/n\mathbb{Z}$ vorgestellt. Die restliche Arbeitszeit besteht aus der schülergeleiteten Projektarbeitsphase, in welcher sie eigenständig ihr weiteres Vorgehen planen, also welche Schritte in welcher Reihenfolge abgearbeitet werden sollen, dieses in Gruppen- oder Partnerarbeit umsetzen und schließlich ihre Ergebnisse dem ganzen Kurs in einer Präsentationsform ihrer Wahl vorstellen.
Die benutzten **Unterrichtsmittel [UM], Medien [M] und deren Funktion** sind im Folgenden noch einmal aufgelistet:

UM/M	**Funktion**
Tafel	Zusammenfassung (von Schüler/innenlösungen), Visualisierung (von Schüler/innenlösungen)
PC	Präsentation, Visualisierung, Anregung von Diskussionen
Skript	Festigung, Nachschlagewerk, Vertiefung
Arbeitsblatt	Erarbeitung, Analyse
Notizblatt	Sicherung der Ergebnisse, Anregung
Excelprogramm	Visualisierung, Festigung

Tabelle 6: Verwendete Unterrichtsmittel, Medien und deren Funktion {tab:Medien

4.8 Reflexion der Lerneinheit

Im Folgenden wird die Lerneinheit in ihren verschiedenen Abschnitten reflektiert. Wir beginnen mit der Vorstellungspräsentation der zur Verfügung stehenden Probleme für die Modellierungstage 2019, fahren mit der interaktiven Einführungspräsentation fort und betrachten schließlich die Projektarbeitsphase einschließlich der Präsentation.

4.8.1 Reflexion der Vorstellungspräsentation

Bei der Vorstellung der Themen vor dem Kurs habe ich mich wie geplant kurz fassen können. Mein Ziel war es den Schülerinnen und Schülern kurz und prägnant vorzustellen, was das Thema und die grobe Vorgehensweise sein würde. Es war mir wichtig, dass es den Teilnehmenden klar ist, dass es bei meinem Thema eine kleine interaktive Einführungssequenz geben wird, in welcher sie die benötigten Grundlagen für die Erstellung einer Kryptowährung erarbeiten, da dies nicht der „normale“ Ablauf von Modellierungstagen ist. Der einzige Negativpunkt ist, dass ich vergessen hatte zu erwähnen, dass keine Informatik-, beziehungsweise Programmierkenntnisse vorausgesetzt sind. Die Präsentationsfolie kann in Anhang 7.3 gefunden werden.

4.8.2 Reflexion der interaktiven Einführungspräsentation

Meine größte Befürchtung war anfangs der Zeitmangel für die interaktive Präsentation. Letztendlich konnte ich sie aber mit nur einer Minute Verspätung zu einem runden Abschluss bringen. Auch in Retrospektive finde ich es gut, dass ich den Teilnehmenden die Ziele für diese Präsentation vorgestellt hatte, da das ganze Programm so transparenter wurde und die Schülerinnen und Schüler danach auch die Möglichkeit hatten zu fragen, falls aus ihrer Sicht eines der Ziele nicht zu ihrer Zufriedenheit behandelt wurde. Die erste einleitende Phase lief wie erwartet reibungslos ab. Es wurde schnell erkannt, welche die wichtigen Eckpunkte im System sind und wie diese miteinander interagieren. Besonders die Frage nach der Ähnlichkeit zum Bargeld hatte noch letzte Fehlvorstellungen beseitigt, da erst nach kurzem Überlegen klar wurde, dass bei Überweisungen die Bank noch eine Zwischenrolle einnimmt.
In der Erarbeitung des SetUps & Abhebens hat die gewagte Lehrerbehaputung der Definition einer Coin genau den gewünschten Effekt erzielt. Die Gruppe war zuerst sichtlich verwirrt, wie ein Tripel aus rellen Zahlen die Grundlage einer ganzen Währung sein kann. Da die Schülerinnen und Schüler ihre Fragen kurz auf ihrem Notizzettel notiert hatten war auch das Übertragen in die Folie zum Sammeln schnell erledigt. Wie zu erwarten war, wurden auch Fragen formuliert, welche zu sehr auf die technische Umsetzung mit einem Computer abzielten, wie zum Beispiel, dass relle Zahlen im allgemeinen gerundet werden müssen, damit man sie im Speicher halten kann. Diese Fragen wurden jedoch in der kurzen Gruppendiskussion schnell als irrelevant für den Moment betrachtet, da es bei dieser Erstellung einer Kryptowährung nur auf die Grundlagen ankam. Bei der

Sicherung dieser Phase musste ich auf den Trick mit dem physischen Geldschein zurückgreifen, um den Teilnehmenden klarzumachen, dass auch bei „normalen“ Währungen die Währungseinheiten oft nicht die Wertträger sind. Auch musste ich der Gruppe durch einen kleinen Hinweis auf $A = I_{\mathcal{U}}^{s}$ zur Erkenntnis verhelfen, dass die persönlichen Daten des Besitzers eine große Rolle bei einer abgehobenen Coin spielen. Relativ schnell wurde dafür aber erkannt, dass r nur eine Art Beweis dafür ist, dass die Bank diese Coin ausgezahlt hat.
Dadurch, dass anfangs der Kreislauf einer Coin analysiert wurde, hatten die Schülerinnen und Schüler immer einen Überblick darüber, was der nächste sinnvolle Schritt ist und beantworteten meine Frage diesbezüglich richtig mit *Bezahlen*. Nach dem der Impuls *Was heißt Bezahlen hier überhaupt?* gesetzt war, kam die Gruppe nach kurzer Diskussion auf die Idee, dass s und t übertragen werden müssten, erkannten aber auch gleichzeitig, da dies im vorherigen Schritt gesichert wurde, dass das Wissen über diese Variablen den *ursprünglichen* Besitz anzeigt, welcher nicht weitergegeben werden soll. Die Schülerinnen und Schüler realisierten, dass man seinem Gegenüber beweisen muss, dass man s und t kennt, ohne diese zu übertragen. In der folgenden Sequenz ist mir recht schnell aufgefallen, dass es nicht offensichtlich ist, warum Geraden benutzt werden sollten, da es recht viele mathematische Objekte geben kann, die eindeutig durch zwei Parameter festgelegt werden, wie zum Beispiel ein einfacher Punkt im zweidimensionalen Koordinatensystem. Dass die Teilnehmenden als erste Idee Geraden äußerten und sich auch einig bei dieser Antwort waren, war zugegebenermaßen etwas Zufall. Der Gedankengang an dieser Stelle müsste entweder durch einen genaueren Anreiz oder eine andere Hinführung in die richtige Bahn gelenkt werden, sodass die Benutzung von Geradengleichungen als eindeutige Wahl erscheint. Bei der folgenden Aufgabe waren für fast alle Teilnehmenden die Tipps wichtig, damit sie sich eine Meinung bilden konnten, warum gerade $I_{\mathcal{U}}^{y}$ eine passende Lösung für unser derzeitiges Problem ist, von daher hat mir dies auch wieder gezeigt, warum es so wichtig ist sich auf alle Eventualitäten vorzubereiten und differenzierende Aufgaben zu stellen.
Der analytische Ansatz für die Geradenchallenge ist meiner Meinung nach auch in Retrospektive der richtige gewesen. Der begrenzte Zeitrahmen hätte eine eigenständige Erarbeitung einfach nicht zugelassen, da alleine die Gruppendiskussion nach der Vorstellung des Protokolls 7 Minuten in Anspruch genommen hatte. Letztendlich konnten sich die Schülerinnen und Schüler aber klarmachen, *wie* und vor allem *warum* dieses Protokoll als Zero Knowledge Beweis funktioniert. Auch die Analyse der Sicherheit lief reibungslos, da die Teilnehmenden in der vorherigen Aufgabe explizit mit den Variablen gerechnet haben und es so recht offensichtlich wurde, dass der Logarithmus im Reellen das Hauptproblem des Systems ist.
Die Überleitung zur Restklassenarithmetik lief meiner Meinung nach gut, hat aber auch noch Verbesserungspotential. Natürlich ist es passend zu sagen, dass man das Problem mit dem Logarithmus hat und der nächste Abschnitt dieses löst, aber ich denke, dass er zwei Schwachpunkte hat: Es ist kein natürlicher Übergang, das heißt, dass ihn vor allem die Schülerinnen und Schüler schon von Anfang an als „sinnvoll“ und „beste Wahl“ betrachten, denn diese kennen den Be-

griff der Restklassenarithmetik zu diesem Zeitpunkt noch nicht. Der zweite Punkt ist etwas schwächer, muss aber auch überlegt sein. Es dreht sich dabei um die Tatsache, dass ein bisschen vorweggenommen wird, dass das Logarithmusproblem im Speziellen damit gelöst werden kann, was eine schöne und wichtige Erkenntnis für Schülerinnen und Schüler ist. Die folgende Sequenz über Restklassenarithmetik verlief etwas schneller als gedacht, da die Teilnehmenden anhand des Beispiels schnell eine passende Definition für Restklassen in $\mathbb{Z}/n\mathbb{Z}$ fanden. Durch die Übungsaufgaben fühlten sie sich sichtbar sicherer im Umgang mit Restklassen und stellten sogar beispielsweise eigenständig fest, dass bei $n = 5$ gilt, dass $\bar{6} = \bar{1}$. Die Aufgabe, welche zum DLP hinführt, erzielte genau die gewünschten Reaktionen der Gruppe. Einige versuchten naiv den Logarithmus zu berechnen und mussten dann feststellen, dass eigentlich nur ganze Zahlen als Exponenten sinnvoll sind, andere iterierten den Exponenten, kamen dann aber zu dem Schluss, dass es keine „gute“ Lösung ist. Bei der darauf folgenden Präsentation des Excel-Scripts zur Visualisierung des DLP hatte ich das Gefühl, dass die Schülerinnen und Schüler einen weiteren „Aha-Moment“ durchliefen, da sie so schon an einem kleinen Beispiel den scheinbar zufälligen Charakter der Potenzierung mit Restklassen in $\mathbb{Z}/n\mathbb{Z}$ visuell dargestellt erkennen konnten. So wie das Excel-Script bei der Visualisierung der Vorteile geholfen hat, war auch die Beispielsrechnung, wie lange ein Computer brauchen würde, bis er alle Möglichkeiten für ein n mit mehr als 300 Stellen, eine große Hilfe dabei der Gruppe klarzumachen, um welche Dimensionen es sich bei der expliziten Laufzeit dieses Ansatzes handelt.

4.8.3 Reflexion der Projektarbeit

Die Projektarbeit der Schülerinnen und Schüler verlief weitestgehend geordnet und strukturiert ab. Sie einigten sich zuerst darauf, etwaige persönliche Fragen mit dem Skript zu klären und sie dann gegebenenfalls noch einmal in der Gruppe zu diskutieren. Ihr nächster Gedanke war es, meine Version zu vervollständigen, sodass sie ein funktionierendes und vollständiges Beispiel als Referenzmaterial für ihre eigene Version haben. Nachdem sie das Einzahlen nachvollzogen hatten, machten sie sich daran die einzelnen Schritte nach Ihrer Vorstellung zu erstellen. Hier begannen die ersten Probleme aufzutreten, welche aber hauptsächlich organisatorischer Natur waren, da sie sich nicht im Klaren darüber waren, wie ihre weitere Planung aussehen könnte. Hier habe ich dann eingegriffen und ihnen einen Tipp zur Planungsphase gegeben. Die Teilnehmenden sollten sich zuerst einen Moderator für ihre Diskussionen wählen, welcher die Wortmeldungen strukturiert abarbeitet und dem aktiven Sprecher ein störungsfreies Umfeld bietet. Des Weiteren sollten sich die Schülerinnen und Schüler Gedanken darüber machen, was ihre Kryptowährung „können soll“ damit sie anhand dieser Ziele ihre Weitere Arbeit planen können. Letztlich habe ich ihnen noch ans Herz gelegt die Tafel als Visualisierungs- und Sicherungsmedium in Diskussionen zu verwenden, sodass jeder Teilnehmende versteht, was gerade der Diskussionsgegenstand ist.
Die restliche Arbeitsphase folgte dem Muster, dass die Gruppe einen Grundschritt des Systems nach dem anderen betrachtet, ihre eigenen Ideen diskutiert und eingearbeitet hat. Wenn ich eingegriffen habe, war es meistens nur, weil die gerade

geführte Diskussion nicht zielführend war oder sich im Kreis drehte. Ein Beispiel hierfür war eine Auseinandersetzung darüber, welche Variablennamen für den Benutzer und die Bank eingeführt werden sollten.
Die Entscheidung über die Art der Präsentation war den Schülerinnen und Schülern selbst überlassen. Sie einigten sich darauf ein Rollenspiel vor dem Kurs aufzuführen, in welchem die einzelnen Schritte an der Tafel festgehalten und erklärt wurden. Die Präsentation ist generell sehr gut verlaufen, mit nur wenigen Negativ- aber dafür vielen Positivpunkten. Die **negativen Punkte** wären, dass die Präsentierenden erwähnten, dass sie eine eigene *Coin* erstellen wollen, obwohl es eigentlich um das ganze System geht. Weiterhin hat bei der Erklärung des Bezahlens der Händler angefangen zu reden, obwohl ihr Protokoll vorsieht, dass der Nutzer den ersten Schritt tätigt. Der letzte Negativpunkt ist das Auslassen der Einzahlung von Coins. Dieser Punkt ist diskussionswürdig, da die Schülerinnen und Schüler einen knappen Zeitrahmen von zehn Minuten für ihre Präsentation hatten, welcher, vor allem für Lernende der elften Klassenstufe, noch schwer einzuhalten ist. Des Weiteren wurde den Teilnehmenden geraten, sich bei ihren Vorstellungen auf wichtige Eckpunkte ihrer Lösung zu konzentrieren (Adressatengerechte Sprache bei der Präsentation). Nichtsdestotrotz hätte die Gruppe zumindest *erwähnen* können, dass es noch einen solchen Schritt gibt. Die **positiven Punkte** überwiegen meiner Meinung nach. Insgesamt empfand ich die Idee eines Rollenspiels als sehr motivierend für die Präsentierenden *und* leicht verständlich, sowie unterhaltsam für die Zuhörer. An der Tafel benutzten die Schülerinnen und Schüler konsistent einen sinnvollen Color-Code, um wichtige Eigenschaften und Gegebenheiten hervorzuheben. Weiterhin war ihnen wichtig, dass Restklassen kurz anhand eines Beispieles vorgestellt werden, damit die Zuhörer eine fachliche Grundlage bekommen. Am wichtigsten fand ich jedoch, dass sie erkannten, dass die Geradenchallenge das „Herzstück“ dieses Systems ist und dies auch dem Kurs durch einen eigenen Sinnabschnitt innerhalb der Präsentation, sowie der expliziten Erwähnung dessen, deutlich machten.

4.9 Feedback

Nach dem ersten Tag der Lerneinheit hatte ich die Schülerinnen und Schüler noch um eine kurze Feedbackrunde gebeten, aus welcher die folgenden Punkte stammen:

- Gut gewählte Aufgaben für das Verständnis von Problemen.
- Manchmal noch allgemeinere Informationen anfügen, also wie wird manches technisch Umgesetzt usw.
- Insgesamt gute Schwierigkeit, man kann gut folgen.
- Fachliche Vorbereitung gut.
- Zielführende Tipps.

- Spannendes Thema, gutes Beispiel für ein mathematisches Thema in einem nicht-schulischen Kontext.

Im Anhang 7.7 befindet sich das Feedback der Teilnehmenden meiner Themengruppe, welches sie ohne Einfluss einer Lehrperson –weder mir noch ihrer Mathematiklehrerin– frei verfasst haben. Man kann deutlich erkennen, dass die von mir in der Feedbackrunde gesammelten Aussagen nicht durch die Anwesenheit meiner Person verfälscht wurden.

5 Fazit

Im ersten Teil dieser Arbeit wurden die fachlichen Grundlagen zweier großer Kryptowährungsparadigmen vorgestellt und für das Konzept des Central Authority eCash auch eine allgemeine Version ausgearbeitet. Da sie als individualisierbare Vorlage dient, kann nicht nur die ursprünglich untersuchte Implementation umgesetzt, sondern auch eine Iteration basierend auf $\mathbb{R}$ realisiert werden, welche eine graphische Darstellung des wichtigsten Protokolles zum besseren Verständnis zulässt. Durch das Studium der verschiedenen Ansätze konnten die wichtigsten Kernelemente einer Central Authority eCash-Währung herausgearbeitet und als Grundlage für eine vereinfachte Version, welche als Anschauungsmaterial für Schülerinnen und Schüler dienen kann, benutzt werden. Eben jene, auf ihre Grundideen reduzierte Implementation, stellt den zugrunde liegenden fachlichen Aspekt des zweiten, didaktischen Teils der Arbeit dar. Durch die didaktische, sowie methodische Analyse einer geplanten und durchgeführten Lerneinheit zu dem Thema „Erstellung einer Kryptowährung“ wird gezeigt, dass auch komplexere kryptographische Themen wie Kryptowährungen, selbst unter engeren zeitlichen Restriktionen, in einem schulischen Kontext behandelt werden können.

6 Danksagung

Ich möchte mich zuallererst bei meinem Zweitkorrektor Herrn Thilo Vollrath bedanken, da es mir durch seine pädagogische Expertise ermöglicht wurde einen didaktischen Teil in dieser Arbeit zu verfassen.

Weiterhin bedanke ich mich bei meinem Betreuer Prof. Dr. Fieker, der mir immer mit Rat und Anregungen bei Problemen zur Seite stand und so geholfen hat, diese Arbeit zu dem zu formen, was sie nun ist.

Den Mitarbeitern des KOMMS, Dr. Martin Bracke und Dr. Jana Kreckler gilt auch meine Dankbarkeit, da ich ohne ihren Einsatz meine geplante Unterrichtseinheit nicht hätte in der Praxis umsetzen können.

Vielen Dank auch an alle meine Freunde und Lieben, die mich immer wieder unterstützt und mir so durch stressige Studienzeiten geholfen haben. Einem besonderen Dank gilt hierbei natürlich auch den Probelesern dieser Arbeit (TODO:liste).

Zu guter Letzt möchte ich mich ganz herzlich bei meinen Eltern bedanken, ohne deren Hilfe und Unterstützung nicht nur dieses Lehramtsstudium nicht möglich gewesen wäre. Vielen Dank, dass ihr immer an mich geglaubt und hinter meinen Entscheidungen gestanden habt.

7 Anhang

Im Folgenden sind alle Materialien und Unterlagen zu finden, welche im Umfang dieser Arbeit entstanden sind.

7.1 Handout Modellierungstage

{anh:Handou

Es folgt ein Handout, welches im Rahmen der Modellierungstage 2019 von mir erstellt wurde, passend zu einer kurzen Vorstellung der Problemstellung. Dieses Handout soll den Schülerinnen und Schülern noch einmal genauere Informationen über den Ablauf und ein paar erste Fragestellungen für das Thema „Erstellung einer Kryptowährung“ an die Hand geben.

Erstellung einer Kryptowährung

Worum geht es?



Kryptowährungen, oder manchmal auch Kryptogeld genannt, sind im Grunde digitalisierte Zahlungsmittel. Ähnlich zu „Alltagswährungen“ wie dem Euro oder Dollar, kann man es sparen oder auch damit handeln. Der große Unterschied besteht jedoch darin, dass man mit Kryptowährungen anonym, schnell und sicher bezahlen können sollte, ohne dass irgendeine Instanz (noch nicht einmal die Regierung) weiß, welche Personen an einem Handel teilgenommen haben. Diese Eigenschaften werden durch sogenannte kryptographische Verfahren erlangt, welche (oftmals) durch mathematische Grundlagen eine beweisbare Sicherheit liefern.

Was wird getan?

Nach einer kurzen Einführung ins Thema Kryptowährungen und Kryptographie, in welcher ihr mathematische Werkzeuge nahegelegt bekommt, die euch bei der Erstellung eurer eigenen Kryptowährung helfen, könnt ihr mit dem Basteln beginnen! Natürlich habt ihr bei der Erstellung freie Hand, aber um eine möglichst gute Währung zu erschaffen, könnt ihr euch mit den folgenden Eigenschaften/Fragestellungen auseinandersetzen:

- **Abheben:** Wie heben Nutzer eure Währung von ihren Konten ab?
- **Handeln:** Wie wandert eine Währungseinheit von einem Nutzer zum Nächsten?
- **Einzahlen:** Wie zahlen Nutzer eure Währung auf ihr Konto ein?
- **Sicherheit:** *„Im Computer sind alles nur 0en und 1en!“* – Wie kann man also das Fälschen oder zum Beispiel auch mehrfache Ausgeben einer Währungseinheit vermeiden?
- **Geheimhaltung:** *Bei einer Transaktion mit Bargeld könnten sich die Handelspartner vermummen und niemand würde die Identität der beiden kennen.* – Wie sollen also Identitäten in Zeiten von NSA und Cyberkriminalität anonym bleiben?
- **Effizienz:** *Es ist 2019 und Banküberweisungen dauern manchmal immer noch 3 Tage!* – Nutzer eurer Währung wollen schnell und einfach nur mit der Hilfe eines (potenziell langsamen) PCs oder Handys Transaktionen tätigen.

PS: Informatikkenntnisse sind keinesfalls vorausgesetzt.

Bildquelle: https://schliesslich-ist-es-ihr-geld.de/wp-content/uploads/2018/01/Abb_Logos_KryptowährungenWG.png

7.2 Skript Modellierungstage

{anh:Skript

Auf den nächsten Seiten befindet sich ein Skript, welches auch im Rahmen der Modellierungstage 2019, passend zur interaktiven Einleitungspräsentation, entstanden ist. Es dient den Schülerinnen und Schülern als Nachschlage- und Recherchewerk, da es oft tiefer und ausführlicher in die Materie eindringt als die Präsentation.



Modellierungstage
Kryptowährungen

Marcel Schütz

18.06.2019

Bildquelle: https://schliesslich-ist-es-ihr-geld.de/wp-content/uploads/2018/01/Abb_Logos_KryptowährungenWG.png

Inhaltsverzeichnis

1 Eine erste Kryptowährung **3**

2 Bargeld simulieren mit Mathematik **4**
2.1 Abheben 4
2.2 Bezahlen 5
2.3 Einzahlen 6

3 Restklassenarithmetik **7**
3.1 Restklassen 7
3.2 Restklassenarithmetik 8
3.3 Das diskrete Logarithmusproblem 9

4 Anhang **12**
4.1 Beweispuzzle 12

1 Eine erste Kryptowährung

Um einen ersten Einblick in die Welt der Kryptowährungen zu erlangen, muss man zuerst die Grundlagen verstehen. Im folgenden Schaubild könnt ihr die Grundschritte eines solchen Systems erkennen:

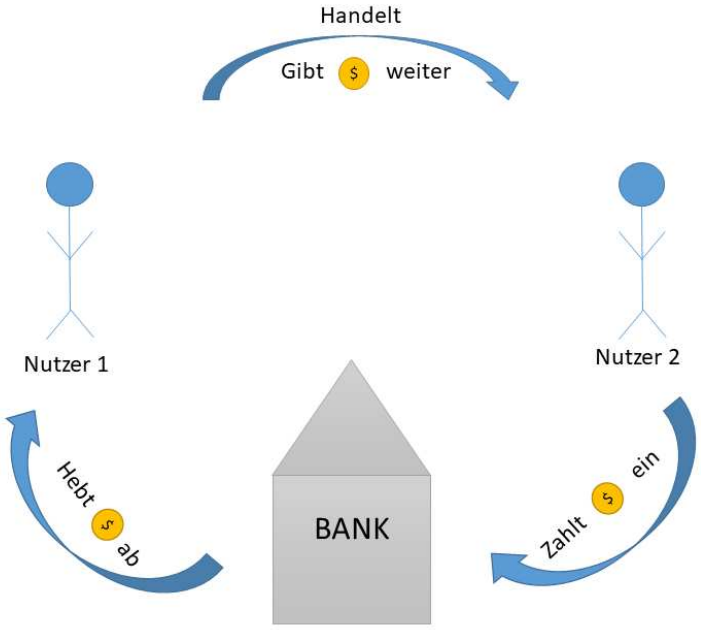


Abbildung 1: Kreislauf einer Währungseinheit

Es ist unschwer zu erkennen, dass sich das Grundprinzip im Vergleich zu „normalen“ Währungen nicht geändert hat. Es gibt eine Bank, welche bestimmt wer am System teilhaben darf, Währungseinheiten (wir werden diese von nun an *Coins* nennen) können abgehoben sowie eingezahlt werden und natürlich sind sie auch als Zahlungsmittel in einem Handel einsetzbar. Da die Bank bei diesem System im Mittelpunkt als zentrale Anlaufstelle steht, nennt man solche Kryptowährungen auch **Central Authority Systeme**, also Kryptogeld mit einer zentralen Autorität, welche die Entscheidungsmacht über Ein- und Auszahlungen hat.

Frage 1: *Mit welchem der beiden Konzepte kann das obige Schaubild am ehesten verglichen werden:*

a) Bargeld

b) Überweisungen

c) Zahlung via PayPal

2 Bargeld simulieren mit Mathematik

Es stellt sich jetzt natürlich die Frage:

Wie kann ich mit Hilfe von mathematischen Formeln Bargeld simulieren?

Um ehrlich zu sein ist dies gar nicht so schwer. Man braucht zur eigenen Umsetzung nur die Grundideen zu verstehen, welche dann individuell angepasst werden können. Diese grundlegenden Schritte werden wir uns im Folgenden näher betrachten:

2.1 Abheben

Zunächst einmal müssen wir uns klarmachen, was eine Coin nun wirklich ist und wie wir mit mathematischen Methoden ein „Abheben“ von einer Bank modellieren könnten.

Definition 2.1: Coins
In unserer Beispielversion soll eine Coin c wie folgt aufgebaut sein:

$$c = (A, B, r) \tag{1}$$

wobei A, B, r reelle Zahlen und **öffentlich einsehbar** sind. c ist hier also ein sogenanntes 3-Tupel (oder Tripel).

Unsere Coins sollen also nur aus drei reellen Zahlen bestehen? Diese Frage und weitere, wie zum Beispiel *Wieso kann ich mir nicht einfach drei reelle Zahlen wählen und habe eine Coin?* sind berechtigt und nicht nur das, sie bilden in einem gewissen Sinne auch die Grundlage für das weitere Vorgehen. Im Folgenden sei $\mathcal{U}$ ein Nutzer unseres Systems, $\mathcal{B}$ die Bank und $\mathcal{M}$ ein Händler (auch ein Nutzer). Jeder Nutzer bekommt von der Bank eine eindeutige, öffentliche Kontonummer I (oder manchmal auch $I_{\mathcal{U}}$, um zu verdeutlichen, dass es die Kontonummer des Nutzers $\mathcal{U}$ ist) aus den reellen Zahlen, ähnlich zu Kontonummern, die ihr auch von euren Banken kennt.

Definition 2.2: Abheben
Das Abheben einer Coin wird in vier Schritten durchgeführt.

1. $\mathcal{U}$ wählt s, t als reelle Zahlen beliebig und **geheim**.
2. $\mathcal{B}$ wählt r als reelle Zahl beliebig und speichert es.
3. $\mathcal{B}$ schickt r an $\mathcal{U}$.
4. $\mathcal{U}$ berechnet $A = I_{\mathcal{U}}^s$ und $B = I_{\mathcal{U}}^t$.

Wenn alles funktioniert, besitzt $\mathcal{U}$ nun eine Coin $c = (A, B, r)$.

Bei genauerem Hinschauen fällt auf, dass Coins eigentlich nur eine Art „Beweis“ für das Besitzen von Währung sind: A und B sind durch die geheime Wahl von s, t und das damit zugehörige Verrechnen der individuellen Kontonummer „an den Nutzer gebunden“, während r der Nachweis ist, dass $\mathcal{B}$ diese Coin auch wirklich ausgezahlt hat.

2.2 Bezahlen

Nachdem wir im vorherigen Abschnitt gelernt haben, wie Coins von der Bank abgehoben werden, stellt sich jetzt die Frage, wie man mit ihnen bezahlen kann. Klassischerweise geht man davon aus, dass nur wieder eingezahlt wird, nachdem gehandelt wurde. Es wird also beim Handel eine Art „Beweis“ benötigt, dass der Nutzer $\mathcal{U}_1$, welcher mit einer Coin bezahlt hat, wirklich der Besitzer ist. Doch nicht nur das: Man soll auch erkennen können, dass der Nutzer $\mathcal{U}_2$, der versucht die Coin nach dem Handel bei sich einzuzahlen, auch der Händler war, mit dem die Transaktion abgeschlossen wurde. Die große Frage ist nun also:

Wie kann ein Nutzer einem Händler beweisen, dass er eine Coin besitzt, ohne ihm zu sagen, welches s und t er gewählt hat?

Die Antwort auf diese Frage können wir in simpler Mittelstufenmathematik finden: *Geraden*. Wenn wir uns an die allgemeine Geradengleichung

$$y = s \cdot x + t$$

erinnern, fällt leicht auf, dass Geraden durch ihre **Steigung** s und ihren **y-Achsenabschnitt** t eindeutig bestimmt sind. Würde der Händler dem Nutzer also ein x geben, an dem die Geradengleichung ausgewertet werden soll, wäre das ein leichtes für den Nutzer, da er ja s und t kennt. Jetzt muss der Händler nur noch überprüfen, ob das Ergebnis stimmt... Aber wie soll das denn nun wieder funktionieren, wenn dieser die Parameter ja nicht kennt?

Die Antwort darauf findet ihr in folgender Aufgabe.

Frage 2: *Sei $I_{\mathcal{U}}$ die Kontonummer des Nutzers $\mathcal{U}$, welcher mit einer Coin $c = (A, B, r)$ einen Händler $\mathcal{M}$ bezahlen will. $\mathcal{M}$ gibt $\mathcal{U}$ ein x, zu dem er ein passendes y berechnen soll.*

a) Vereinfache so weit wie möglich $I^y_{\mathcal{U}}$.

b) Wieso löst diese Gleichung das Problem des Besitznachweises?

Dieses Vorgehen bezeichnen wir als **Geradenchallenge**. Warum das *Geraden-* im Namen steckt ist wohl offensichtlich. Der *Challenge*-Teil kommt aus dem Englischen (Challenge = Herausforderung). Der Händler stellt dem Nutzer sozusagen eine Herausforderung (Challenge) zu einem gegebenen x ein passendes y zu berechnen, sodass der Nutzer sein Wissen über s und t (also im Endeffekt seinen Besitz der Coin) beweisen kann, ohne, dass er diese Parameter an den Händler weitergeben muss.

Bisher haben wir also das Problem des ursprünglichen Besitznachweises gelöst. Wie kann nun der Händler später der Bank beweisen, dass er wirklich die Coin in einem Handel erworben hat? Er benutzt eine ganz bestimmte Challenge: Anstatt ein beliebigen x aus den reellen Zahlen zu wählen, erstellt er ein x, welches aus Informationen des Handels (wir nennen sie **Transaktionsdaten**) berechnet wurde, wie zum Beispiel dem Datum, der Uhrzeit, seiner Kontonummer und den Coin-Daten. Je mehr Aspekte des Handels er in die Berechnung einfließen lässt, desto unwahrscheinlicher ist es, dass zwei Händler zufällig die gleiche Challenge stellen.

Zusammengefasst können wir das Bezahlen in der folgenden Definition sehen.

Definition 2.3: Bezahlen
Der Bezahlvorgang besteht aus den folgenden Schritten:

1. $\mathcal{U}$ schickt c an $\mathcal{M}$.
2. $\mathcal{M}$ schickt $\mathcal{U}$ seine Challenge x, welche **genügend wichtige** Handelsinformationen enthält.
3. $\mathcal{U}$ berechnet $y = s \cdot x + t$.
4. $\mathcal{M}$ verifiziert $I_{\mathcal{U}}^{y} = I_{\mathcal{U}}^{s \cdot x} \cdot I_{\mathcal{U}}^{t} = A^{x} \cdot B$.

2.3 Einzahlen

Wie schon in dem vorangegangenen Abschnitt erwähnt, fehlt uns für den kompletten Kreislauf einer Coin nur noch das Einzahlen. Damit Angreifer es möglichst schwer haben, soll die Bank vor dem Akzeptieren der Coin die bisherigen Schritte noch einmal überprüfen. Das heißt, es muss sichergestellt werden, dass die Geradenchallenge mit der Challenge des Händlers berechnet, die Challenge auch wirklich mit den Transaktionsdaten erstellt und die Coin nicht schon einmal eingezahlt wurde. Die Vorgehensweise könnt ihr in der nächsten Definition sehen.

Definition 2.4: Einzahlen

1. $\mathcal{M}$ schickt c, y und die Transaktionsdaten zum Berechnen von x an $\mathcal{B}$.
2. $\mathcal{B}$ verifiziert $I_{\mathcal{U}}^{y} = A^{x} \cdot B$.
3. $\mathcal{B}$ überprüft mit Hilfe von r, ob die Coin schon einmal eingezahlt wurde.

Man kann hier erkennen, dass ein einzahlender Nutzer der Bank alle Informationen schicken muss, damit diese alle Rechenschritte *selbst* nachrechnen kann. Mehrfaches Einzahlen einer Coin wird durch Überprüfung von r verhindert: Da sich die Bank eine Liste aller r speichert und einfach markieren kann, wenn eines davon wieder zu ihr zurückkehrt, merkt sie sofort, wenn jemand versucht eine Coin zum wiederholten Male einzuzahlen.

3 Restklassenarithmetik

In diesem Kapitel wollen wir uns ein wenig mit klassischer Kryptographie befassen. Der Name „Kryptographie“ setzt sich aus zwei Teilen zusammen, welche aus dem altgriechischen stammen: *kryptós* (deutsch: geheim, verborgen) und *gráphein* (deutsch: schreiben) (Quelle: Wikipedia). Wie ihr euch schon denken könnt, geht es hierbei nicht darum wo man am besten im Verborgenen Texte schreiben kann, sondern fast schon das Gegenteil: Wie kann ich Texte/Dokumente so *verschlüsseln*, dass sie, auch wenn diese an die Öffentlichkeit gelangen, nicht gelesen werden können?

Im vorhergehenden Kapitel haben wir schon gesehen, dass die erste Version der Kryptowährung von Sicherheitslücken geplagt war. Allen voran das Problem, dass man Logarithmen in den reellen Zahlen sehr einfach berechnen kann und sie somit keine Sicherheit bieten. Eine einfache Möglichkeit, wie man Informationen verschlüsseln kann, werden wir uns nun Schritt für Schritt herleiten.

3.1 Restklassen

Um einen ersten Einblick in das Thema zu gewinnen, bearbeiten wir die folgende Aufgabe:

Frage 3: *Wir betrachten uns eine digitale Zeitanzeige, wie in Abbildung 2 zu sehen. Wie ihr wisst, zeigen Uhren dieser Art im klassischen Fall die Stunden nur mit Zahlen von 0-23 an.*

a) Es ist 9 Uhr und 2/3/4 Stunden vergehen. Es ist 21 Uhr und 2/3/12 Stunden vergehen. Drücke dies in „Gleichungen“ aus.

b) Beschreibe, wie die Gleichung $a = d \cdot 24 + r$ mit deinen Gleichungen vereinbar ist.

c) Wie müsste die Gleichung aus b) verändert werden, um das Problem mit analogen Uhren zu beschreiben?



Abbildung 2: Eine digitale Zeitanzeige

Die Gleichungen aus *b)* und *c)* sind natürlich nicht einfach so vom Himmel gefallen, sondern sind euch in einer umgeformten Version schon in der Grundschule begegnet:

$$\begin{aligned} & a \quad = d \cdot 24 + r \\ \Leftrightarrow \quad & a/24 = d + r/24 \\ \Leftrightarrow \quad & a/24 = d \text{ Rest r} \end{aligned}$$

An der letzten Zeile könnt ihr schon erkennen, worum es sich handelt: *Division mit Rest* (oder hier: **Modulorechnung**). Und genau dieser Rest ist, was den Restklassen den Namen gibt. Doch was genau sind sie jetzt? Die Antwort auf diese Frage könnt ihr in den folgenden Definitionen nachlesen.

Definition 3.1: Modulorechnung
Seien a und b zwei ganze Zahlen. Die Modulofunktion **mod** ordnet a, b den Rest r der Division von a geteilt durch b zu. Dies kann man so schreiben:

$$a \bmod b = r$$

Wir sagen: *„a modulo b ist gleich r.*

Beispiel:

- $15 \bmod 12 = 3$
- $27 \bmod 12 = 3$
- $5 \bmod 12 = 5$
- $10 \bmod 7 = 3$

Wie ihr in diesem Beispiel erkennt, können Zahlen öfter als Ergebnis einer Modulorechnung entstehen (erste und zweite Gleichung). Eben diese Tatsache motiviert nun die Definition von Restklassen.

Definition 3.2: Restklassen
Wir bezeichnen als Restklasse der Zahl a modulo b die Menge aller Zahlen, die geteilt durch b den gleichen Rest haben wie a. Wir schreiben

$$\bar{a} := \{x | x \bmod b = a \bmod b\} \tag{2}$$

(sprich: *„Die Menge aller x, für die gilt, dass x modulo b gleich a modulo b ist.*)

3.2 Restklassenarithmetik

Nachdem die Grundlagen nun gelegt sind, beschäftigen wir uns damit, wie man mit Restklassen rechnet. Praktisch wäre es wohl für den Anfang, wenn wir in der Lage wären zwei Restklassen $\bar{a}$ und $\bar{b}$ zu addieren beziehungsweise multiplizieren. Intuitiv würden sich bei der Addition wohl viele auf die folgende Vorgehensweise festlegen wollen:

$$\overline{x} + \overline{y} = \overline{x + y} \tag{3}$$

Wie wir sehen werden ist diese auch sinnvoll. Bei genauerer Betrachtung fällt jedoch ein kleines Detail auf, welches auf folgender Überlegung basiert:

Wenn die Restklasse $\bar{a} = \{..., a, x, y, ...\}$ die Menge aller Zahlen ist, welche geteilt durch b den gleichen Rest r erzeugen, dann gilt auch $\bar{a} = \bar{x} = \bar{y} = ...$ Wollen wir nun die neue Addition wie in Gleichung 2 definieren, so müsste sichergestellt sein, dass

$$\bar{a} + \bar{z} = \overline{a + z} = \overline{x + z} = \bar{x} + \bar{z} = \bar{y} + \bar{z} \tag{4}$$

gilt, also dass es egal ist, welchen Repräsentanten von Restklassen man wählt, um diese zu addieren. Falls unsere Addition diese Eigenschaft besitzt, so nennen wir sie ***wohldefiniert****.*

Frage 4: *Im Anhang findet ihr ein sogenanntes Beweispuzzle. Das Ziel dieser Aufgabe ist es die einzelnen Schritte des Beweises in eine logische Reihenfolge zu bringen, um letztendlich zu zeigen, dass unsere Addition wohldefiniert ist.*

Wir haben nun also bewiesen, dass die Addition von Restklassen wohldefiniert ist. Wenn wir uns an die Grundschulzeit zurückerinnern, wäre der nächste logische Schritt also die Multiplikation, welche analog zur Addition funktionieren soll:

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

Auch hier kann man wieder die Wohldefiniertheit beweisen, was aber an dieser Stelle dem Leser als Übung vorgeschlagen wird. Im Folgenden sind ein paar Beispiele für die Multiplikation gezeigt.

Beispiel:

- $\bar{4} \cdot \bar{3} = \overline{4 \cdot 3} = \overline{12} = \bar{2}$ (Restklassen **modulo 5**)
- $\bar{4} \cdot \bar{3} = \overline{4 \cdot 3} = \overline{12} = \bar{5}$ (Restklassen **modulo 7**)
- $\bar{12} \cdot \bar{11} = \overline{12 \cdot 11} = \overline{132} = \bar{2}$ (Restklassen **modulo 13**)

Machen wir nun einen Sprung in die Mittelstufenzeit, so stellen wir fest, dass die wiederholte Multiplikation einer Zahl mit sich selbst auch als *Potenz* geschrieben werden kann, was uns definitiv etwas Schreibarbeit sparen könnte. Da Mathematiker eher als faul bekannt sind, übernehmen wir die Potenzschreibweise gerne.

Definition 3.3: Potenzschreibweise
Sei n eine ganze Zahl und $\bar{x}$ eine Restklasse modulo n. Wir definieren:

$$\bar{x}^t := \underbrace{\bar{x} \cdot \ldots \cdot \bar{x}}_{\text{t mal}} = \underbrace{\overline{x \cdot \ldots \cdot x}}_{\text{t mal}}$$

3.3 Das diskrete Logarithmusproblem

Wie ihr euch vielleicht erinnert, ist es heutzutage, selbst für große Zahlen, kein Problem Logarithmen zu berechnen. Dies war auch eines der Hauptprobleme unserer ersten Version einer Kryptowährung. Ein Angreifer konnte viel zu einfach s

und t bestimmen, auch wenn er nur A und B kannte (die Kontonummer ist sowieso öffentlich). Wäre es nicht praktisch, wenn es eine Art des Rechnens gäbe, die nicht so leicht umkehrbar ist? Die Antwort könnt ihr euch wahrscheinlich schon denken, da wir die ganze Zeit darauf zugearbeitet haben: *das Logarithmusproblem mit Restklassen* oder auch

Das diskrete Logarithmusproblem (DLP)

genannt. Mit Restklassen ausgedrückt sieht das ganze wie folgt aus:

$$\bar{x}^t = \bar{y} \Rightarrow t = ?$$

Wir suchen also zu einer bekannten *Basis* $\bar{x}$ einen *Exponenten* t, sodass die t-malige Multiplikation von $\bar{x}$ mit sich selbst $\bar{y}$ ergibt. Natürlich stellen sich hier wieder Fragen:

- Zu einem festen n: Gibt es zu jedem $\bar{x}$ und $\bar{y}$ ein t, sodass $\bar{x}^t = \bar{y}$?
- Falls nicht: Gibt es gewisse n, für die man zumindest *ein* $\bar{x}$ (*Erzeuger*) finden kann, sodass jedes $\bar{y}$ durch Potenzierung erreicht werden kann?

Die erste Frage ist relativ leicht durch dieses Beispiel zu beantworten:

Beispiel: *Sei $n = 4$. Es folgt also, dass sich alle Restklassen auf diese vier zurückführen lassen: $\bar{0}, \bar{1}, \bar{2}, \bar{3}$. Betrachten wir uns folgende Tabelle:*

Exponent / Restklasse	$t = 1$	$t = 2$	$t = 3$	$t = 4$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{2}$	$\bar{4} = \bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{3}$	$\bar{3}$	$\bar{9} = \bar{1}$	$\bar{3}$	$\bar{1}$

*Wie wir erkennen können, gibt es zu $n = 4$ keine Restklasse, welche durch Potenzierung alle anderen Restklassen „erreicht". Dies bedeutet, dass die erste Frage mit **nein** zu beantworten ist, da man eben **nicht** für **alle** n ein $\bar{x}$ finden kann, welches durch Potenzierung alle anderen Restklassen modulo n erreicht.*

Die zweite Frage ist leider etwas komplizierter zu beantworten und die Erklärung würde den zeitlichen Rahmen dieser Veranstaltung sprengen. Von daher nehmen wir hier einfach hin, **dass** es gewisse n gibt, sodass man ein $\bar{x}$ finden kann, welches durch Potenzierung **fast** alle anderen Restklassen erreicht. Diese n sind genau die **Primzahlen**! Wenn wir uns Restklassen modulo p betrachten, so gibt es **immer** eine davon, die alle anderen Restklassen durch Potenzierung bilden kann, außer $\bar{0}$ (Dieses Detail soll uns nun aber nicht weiter stören).

Beispiel: *Sei $n = 7$. Es folgt also, dass es sieben Restklassen modulo n gibt: $\bar{0}, ..., \bar{6}$. Für diese Restklassen kann man zwei Erzeuger finden, nämlich $\bar{3}$ und $\bar{5}$. Hier der Beweis dafür:*

Restklasse \ Exponent	$t=1$	$t=2$	$t=3$	$t=4$	$t=5$	$t=6$
$\bar{3}$	$\bar{3}$	$\bar{9}=\bar{2}$	$\bar{6}$	$\bar{18}=\bar{4}$	$\bar{12}=\bar{5}$	$\bar{15}=\bar{1}$
$\bar{5}$	$\bar{5}$	$\bar{25}=\bar{4}$	$\bar{20}=\bar{6}$	$\bar{30}=\bar{2}$	$\bar{10}=\bar{3}$	$\bar{15}=\bar{1}$

Was bringt es uns, dass wir für Primzahlen immer einen Erzeuger finden können, welcher alle Restklassen durch Potenzierung abdeckt? Die Antwort darauf ist eigentlich recht einfach: Im Moment gibt es schlicht und ergreifend keinen schnellen Weg diskrete Logarithmen zu berechnen und je mehr Möglichkeiten es gibt, was bei einer Potenzierung als Ergebnis entstehen kann, desto länger dauert es eine Lösung zu finden. Heutzutage kann man sehr leicht große Primzahlen bestimmen, wie zum Beispiel diese hier: 12199949263707004049746488065348245112215971569843166186250493426898746988567771079779952330742212056845459314172766868233221667946521634760971824199815044396987126232661593987883484450714719240457440132587027694521884527204119511338020114562697439975909285050098837115617106389956839791918194778737758017949 1. Das ist eine Primzahl mit **309 Stellen**.

Das Finden von Erzeugern ist wieder eine andere Geschichte. Wir werden für unsere Zwecke Primzahlen nutzen, für welche es bekannte Erzeuger gibt.

4 Anhang

4.1 Beweispuzzle

Beweis.
Voraussetzung:

1. Seien n, x, y, a, a', b, b' ganze Zahlen.
2. Seien $\bar{x}$ und $\bar{y}$ die Restklassen von x und y modulo n.
3. Seien a, a' aus $\bar{x}$ und b, b' aus $\bar{y}$.

Gesucht:
Wir wollen zeigen, dass die Addition aus Gleichung 2 wohldefiniert ist, also die folgende Eigenschaft besitzt:

$$\bar{a} + \bar{b} = \overline{a + b} = \overline{a' + b'} = \bar{a'} + \bar{b'}$$

Beweisführung:

Es gilt also:
$$\bar{a} + \bar{b} = \overline{a + b} = \overline{a' + b'} = \bar{a'} + \bar{b'}$$

Laut Definition von Restklassen liegen $a + b$ und $a' + b'$ also in der selben Restklasse.

$$r_a + r_b = e * n + r$$
Wobei e, r ganze Zahlen sind, mit $0 \leq r < n$.

Es folgt:
$$a + b = (c + d) * n + e * n + r = (c + d + e) * n + r$$

Für $a' + b'$ folgt:

$$a' + b' = (c' * n + r_a) + (d' * n + r_b) = (c' + d') * n + r_a + r_b = (c' + d' + e) * n + r$$

Aus V3) folgt, dass

1. $a = c * n + r_a$ und $a' = c' * n + r_a$
2. $b = d * n + r_b$ und $b' = d' * n + r_b$

Wobei c, c', d, d', r_a, r_b ganze Zahlen sind und $0 \leq r_a < n$, sowie $0 \leq r_b < n$ gilt.

Da $(r_a + r_b)$ wieder eine ganze Zahl ergibt, kann man es auch in der folgenden Form darstellen:

Es gilt also, dass $a + b$ und $a' + b'$ bei Division durch n den gleichen Rest r haben.

Betrachten wir nun die Additionen $a + b$ und $a' + b'$:

$$a + b = (c * n + r_a) + (d * n + r_b) = (c + d) * n + r_a + r_b$$

□

7.3 Präsentationsfolie für das Thema

{anh:Introl

Die folgende Folie wurde zum Präsentieren des Themas *Erstellung einer Kryptowährung* im Rahmen der Modellierungstage 2019 genutzt. Es ist anzumerken, dass diese Folie **nicht von mir**, sondern von der Organisatorin, Dr. Jana Kreckler, als Teil ihrer Einstiegspräsentation erstellt wurde. Obwohl diese Folie nicht von mir erstellt wurde, darf ich sie mit freundlicher Erlaubnis hier anführen, damit der Leser einen vollständigen Überblick über alle relevanten Materialien erhalten kann.



Abbildung 5: Die Folie der Einleitungspräsentation

7.4 Interaktive Präsentation

{anh:Folier

Die folgenden Präsentationsfolien sind die Grundlage für die interaktive Präsentation, in welcher die Schülerinnen und Schüler grundlegende Kompetenzen erwerben, um ihre eigene Kryptowährung erstellen zu können. Es ist anzumerken, dass die hier abgedruckte Version aus Platzgründen keine Indikatoren für Animationen, also nacheinander erscheinende Texte und Abbildungen, enthält. Um dies auszugleichen wird die Reihenfolge des Erscheinens in den nebenstehenden Notizen erwähnt.

{anh:pres1}

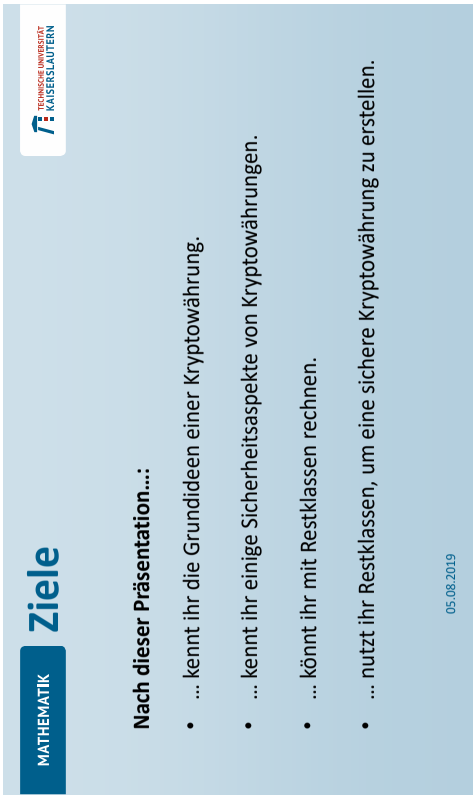


Folie 1:
Diese Folie dient hauptsächlich der Vorstellung des Themanamens, der Lehrperson, sowie der spezielleren Begrüßung der Teilnehmenden.

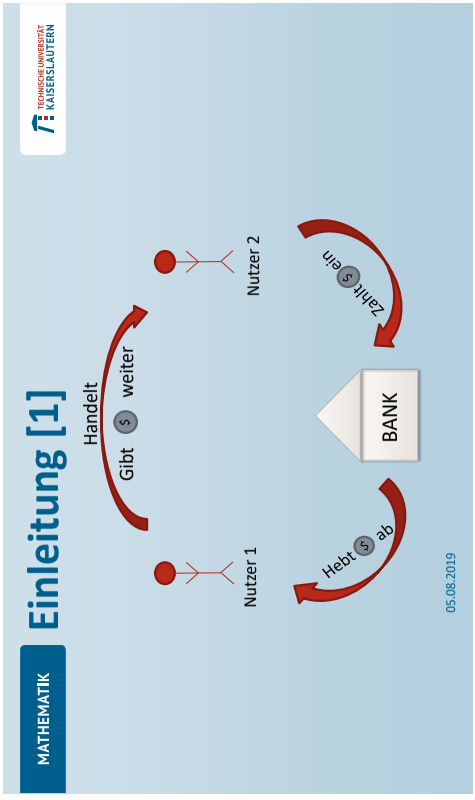
{anh:pres2}



Folie 2:
Die Inhaltsangabe der Präsentation. Soll die Transparenz gegenüber den Lernenden fördern. Gibt Gruppe einen roten Faden, dem sie folgen können.

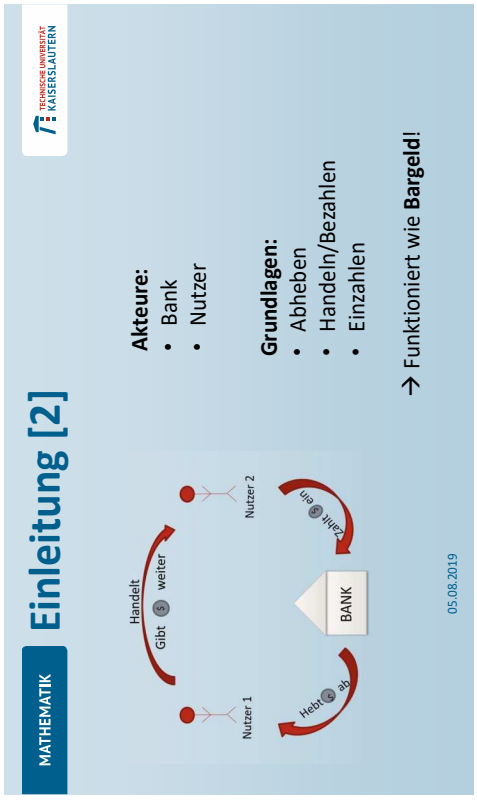


Folie 3:
{anh:pres3}
Auch hier soll durch die Präsentation der Ziele die Transparenz erhöht werden. Des Weiteren haben die Teilnehmenden eine Art Checkliste, die sie mit ihrem neu erworbenen Wissen nach der Präsentation gegenprüfen können.



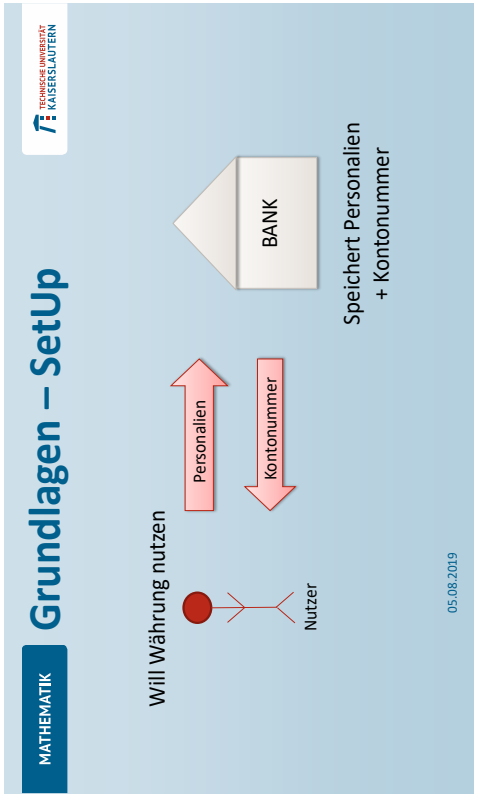
Folie 4:
{anh:pres4}
Der Kreislauf einer Währungseinheit in unserem Beispiel Central Authority eCash System. Die Teilnehmenden analysieren es und nennen die wichtigen Eckpunkte der Abbildung.

{anh:pres5}

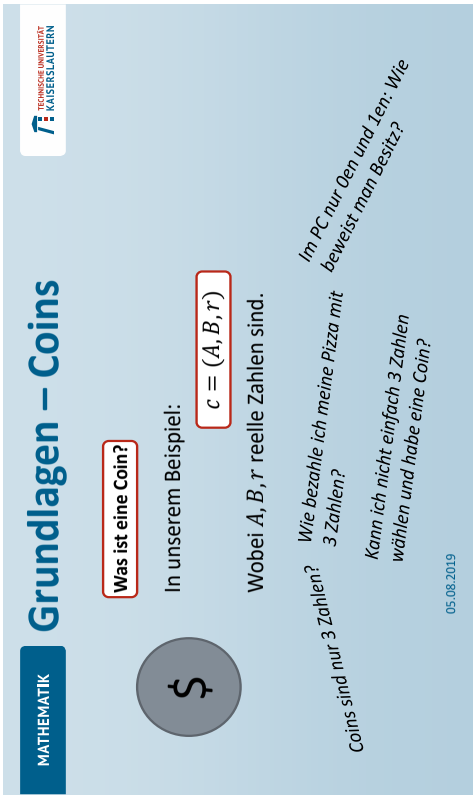


Folie 5:
Genutzt zur Sicherung der Teilnehmenden-Antworten. Pfeilanmerkung erscheint erst nach der Frage *Passt dieses Diagramm besser zur Bezahlen mit Bargeld oder einer Überweisung?*

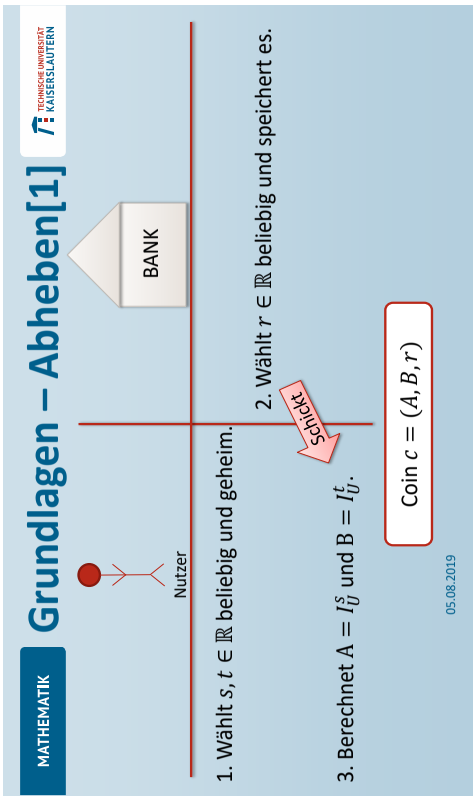
{anh:pres6}



Folie 6:
Die Pfeile sind zunächst unbeschriftet. Die Anmerkung unter der Bank wurde auch von den Teilnehmenden eingefügt.

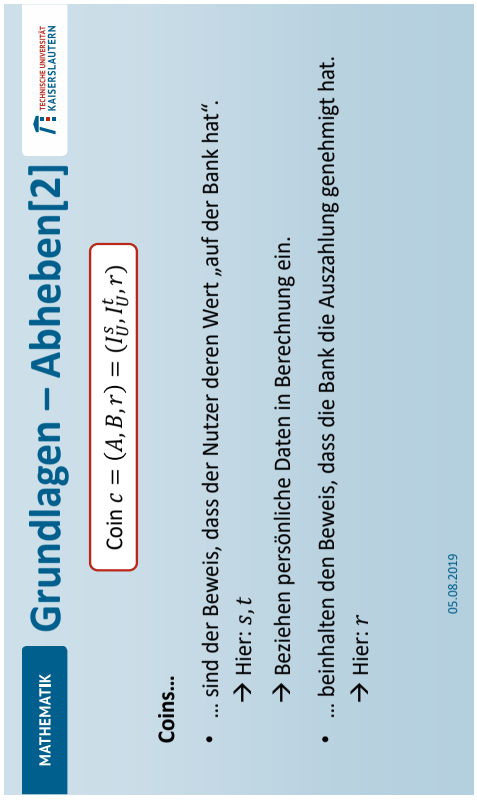


Folie 7:
{anh:pres7}
Definition der Coin wird präsentiert. Die gesammelten Teilnehmenden-Fragen werden hier zur Sicherung gesammelt.



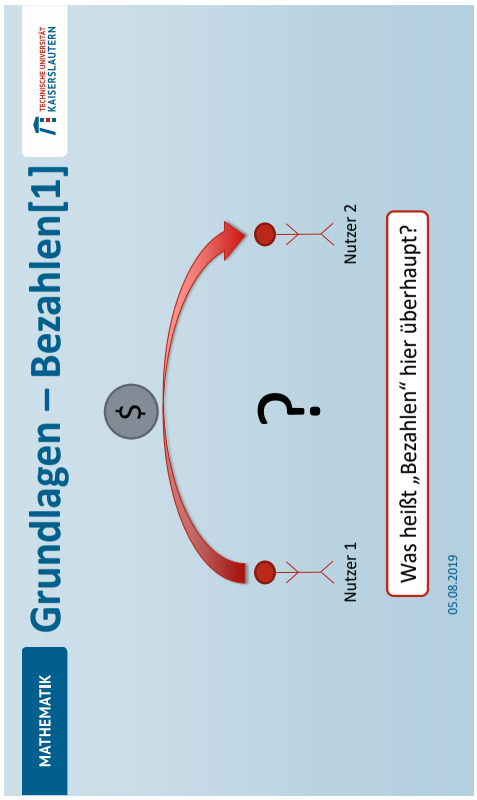
Folie 8:
{anh:pres8}
Stellt den Grundschritt des Abhebens in Diagrammform dar. Text erscheint in nummerierter Reihenfolge. Coin erscheint als letztes.

{anh:pres9}

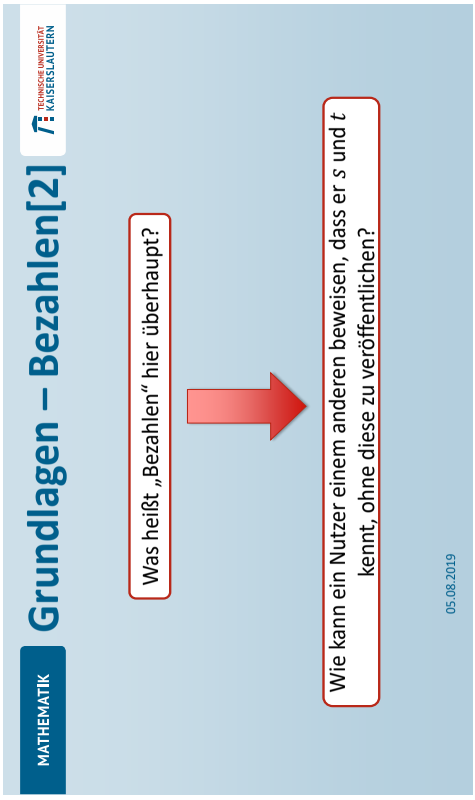


Folie 9:
Eigenschaften einer Coin werden hier gesammelt.

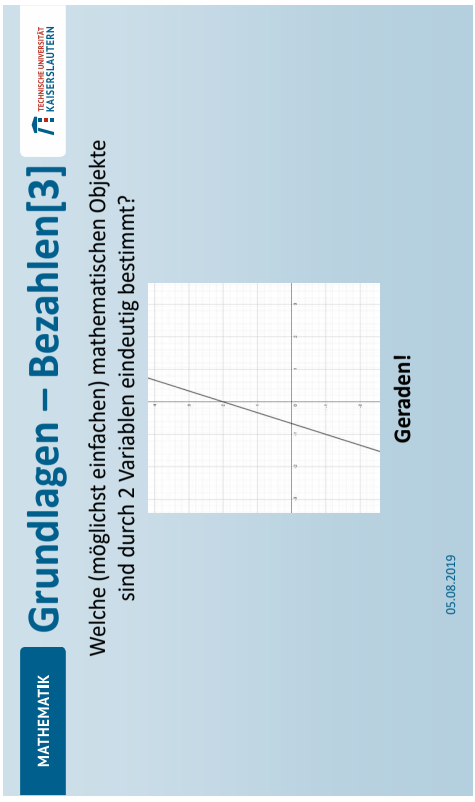
{anh:pres10}



Folie 10:
Übergangsfolie, welche das Problem des Zero Knowledge Beweis motiviert. Die Teilnehmenden machen sich klar, dass sie erst herausfinden müssen, was „Bezahlen" in diesem Kontext überhaupt bedeutet.

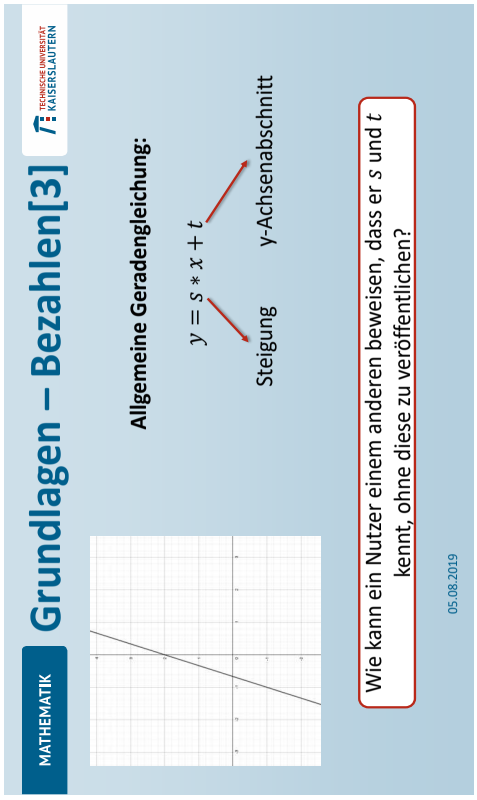


Folie 11:
{anh:pres11}
Die Erkenntnis, dass man durch den Beweis des Wissens über s und t bezahlt, wird hier festgehalten.



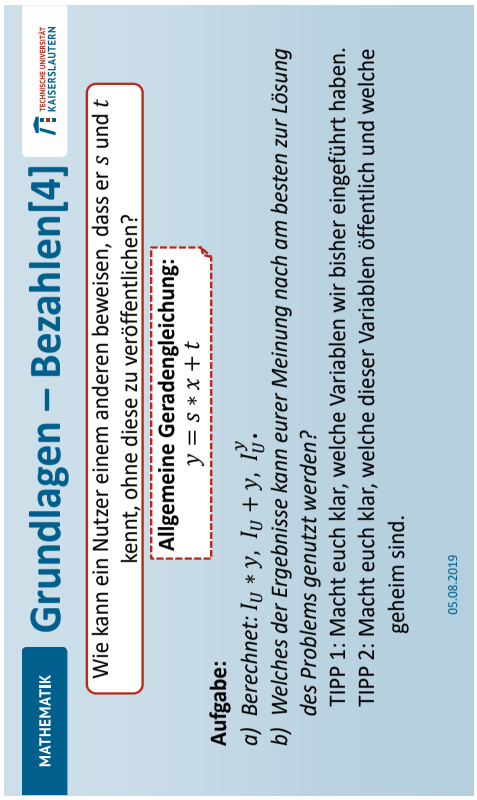
Folie 12:
{anh:pres12}
Zuerst wird die Frage nach einem passenden mathematischen Objekt noch einmal angezeigt, damit diese während der Diskussion präsent ist. Das Koordinatensystem samt Gerade wird erst als Auflösung eingeblendet.

{anh:pres13}

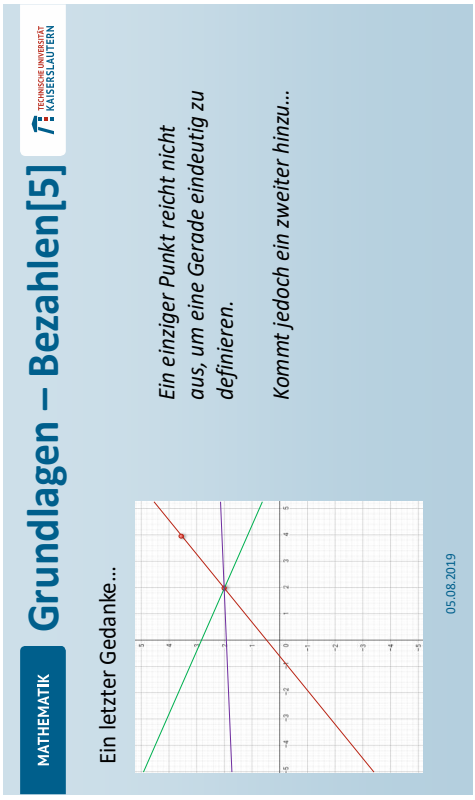


Folie 13:
Zur Wiederholung die Frage nach der allgemeinen Geradengleichung. Explizite Gleichung mit Pfeilen erst nach der richtigen Antwort eingeblendet. Untere Frage zum Schluss eingeblendet, da sie immer noch nicht geklärt ist.

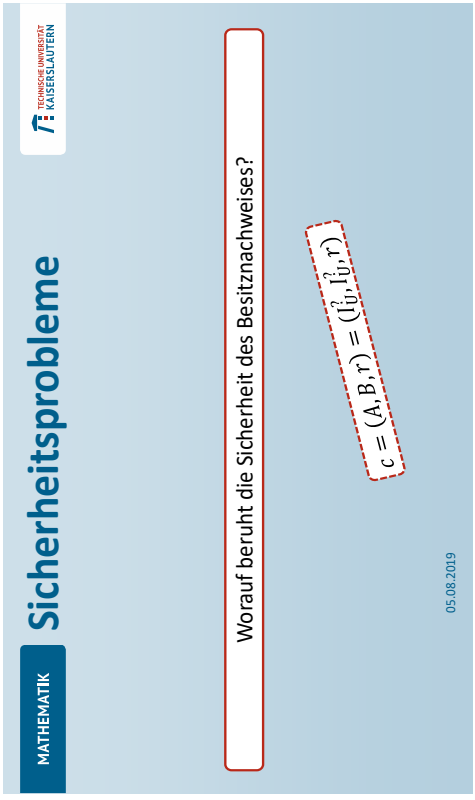
{anh:pres14}



Folie 14:
Aufgabenstellung als Hinleitung zum Verständnis der Geradenchallenge. Tipps zur Differenzierung können nacheinander eingeblendet werden.

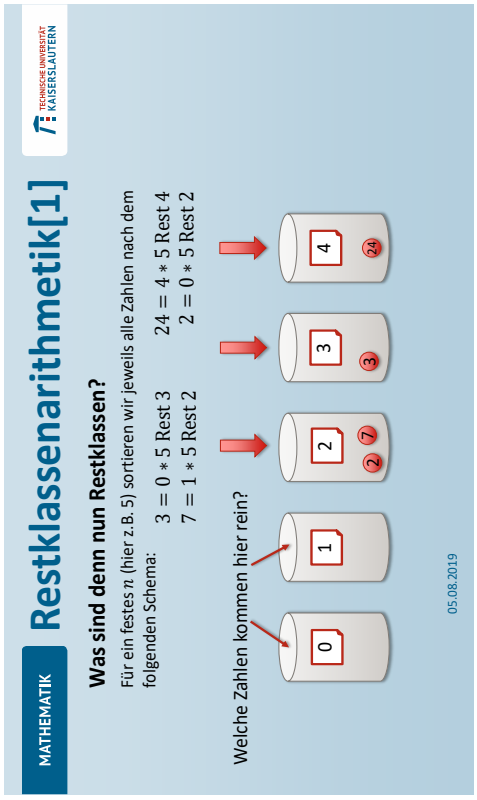


Folie 15:
{anh:pres15}
Eine Folie zum Denkanstoß, um Idee für Double Spending auf den Weg zu bringen. Zuerst erscheint Schnittpunkt der 3 Geraden, dann lila Gerade und gründe Gerade. Zweiter Punkt erscheint zusammen mit unterem Text, schließlich die rote Gerade.



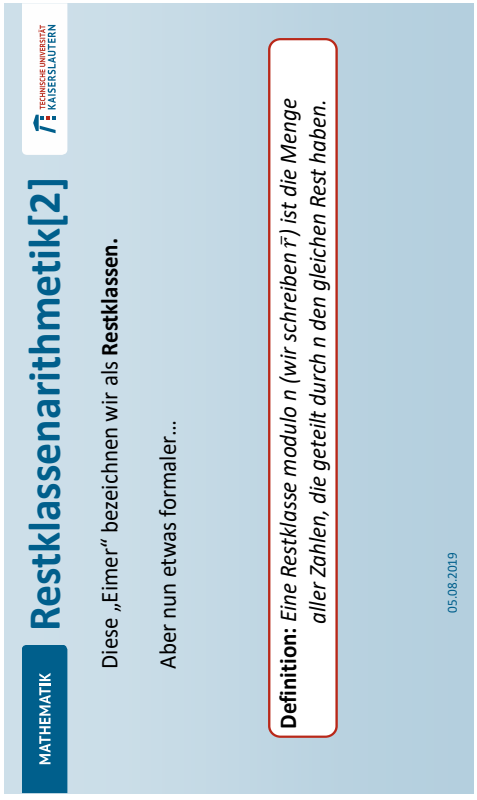
Folie 16:
{anh:pres16}
Fragestellung nach Sicherheitsproblemen, Teilnehmende notieren ihre Antworten. Als Tipp für Logarithmusproblem lässt sich der gestrichelte Kasten einblenden.

{anh:pres17}



Folie 17:
Hier anschaulich an einem Beispiel erklärt, wie Restklassen in $\mathbb{Z}/n\mathbb{Z}$ funktionieren. Die erste Frage erscheint zuerst, dann der darunterstehende Satz mit dem ersten Beispiel links oben. Danach erscheinen die restlichen Beispiele nacheinander und werden immer dann eingeblendet, wenn die Teilnehmenden das vorherige Beispiel richtig beantwortet haben. Schließlich wird die Frage links unten eingeblendet, um zu überprüfen, ob die Gruppe verstanden hat, wie Restklassen aufgebaut sind.

{anh:pres18}



Folie 18:
Nachdem die Gruppe Zeit zum überlegen hatte, wird die Definition in den unteren Kasten eingetragen, damit sie diese auch auf ihren Notizzettel übertragen können.

MATHEMATIK

Restklassenarithmetik[3]

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Man kann mit diesen neuen mathematischen Objekten auch wie gewohnt rechnen!
Es gilt:

$$\bar{x} + \bar{y} = \overline{x + y}$$
Und
$$\bar{x} * \bar{y} = \overline{x * y}$$

Aufgabe: *Probiert ein paar Beispiele aus, bis ihr euch sicher fühlt mit dem Rechnen.*
Zusatz: *Wie könnte man das wiederholte Multiplizieren einer Restklasse mit sich selbst in einer kürzeren Schreibweise darstellen?*

05.08.2019

Folie 19: {ann:pres19}
Es wird die Addition und Multiplikation definiert. Die Gruppe bearbeitet dann eine selbstdifferenzierende Übungsaufgabe mit Zusatzoption.

MATHEMATIK

Restklassenarithmetik[4]

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Wir stellen das wiederholte Multiplizieren einer Restklasse mit sich selbst wie gewohnt als Potenz dar:

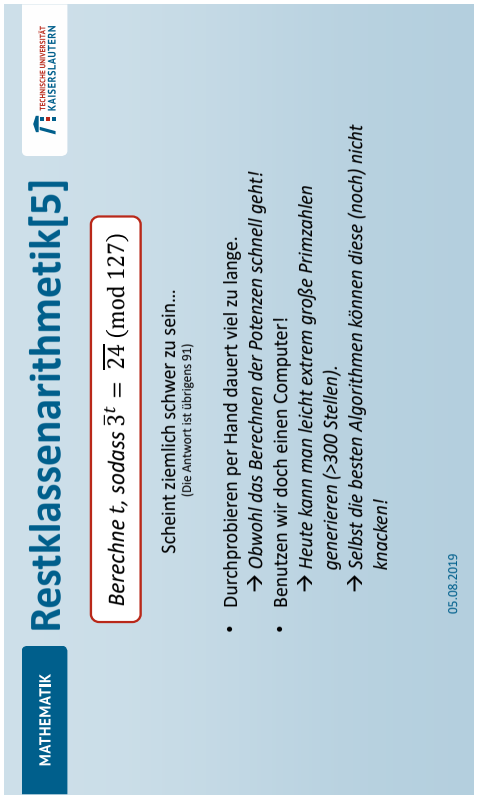
$$\underbrace{\bar{x} * \cdots * \bar{x}}_{\text{t-mal}} = \underbrace{\overline{x * \cdots * x}}_{\text{t-mal}} =: \bar{x}^t$$

Aufgabe:
a) Berechne die folgenden Potenzen: $\bar{5}^3 \pmod 4$, $\bar{6}^4 \pmod{12}$, $\bar{9}^9 \pmod{11}$
b) Berechne t, sodass $\bar{3}^t = \overline{24} \pmod{127}$

05.08.2019

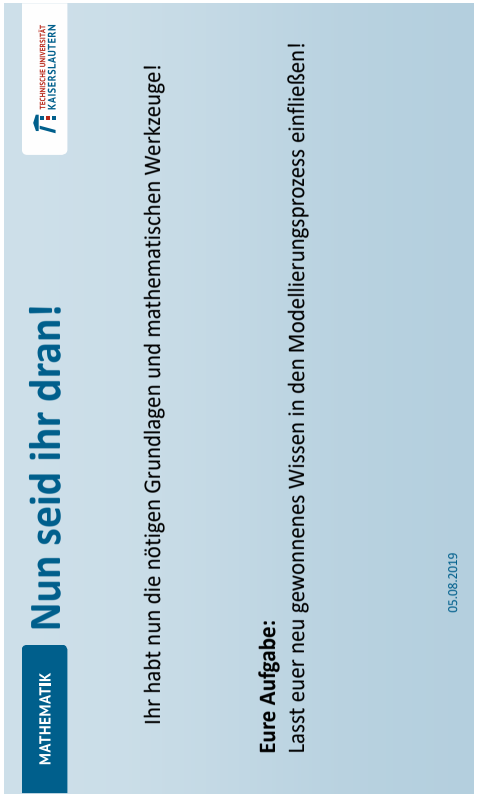
Folie 20: {ann:pres20}
Der Zusatz wird aufgegriffen und die Potenzschreibweise eingeführt. Der erste Aufgabenteil ist nur zur Übung, der zweite jedoch soll die Schülerinnen und Schüler selbst auf das DLP stoßen lassen.

{anh:pres21}



Folie 21:
Das DLP wird anhand der vorherigen Aufgabe aufgegriffen. Einige Einwände werden aufgezählt, aber gleichzeitig wieder entkräftet, um die Schwere des DLP hervorzuheben.

{anh:pres22}



Folie 22:
Eine Abschlussfolie, um die Schülerinnen und Schüler noch einmal zu motivieren und sie darauf hinzuweisen, dass ihnen das neu gewonnene Wissen auf jeden Fall hilfreich sein wird.

7.5 Beispielrechnung {anh:beisp

Diese Rechnung wurde zusammen mit den Schülerinnen und Schülern durchgerechnet, um ihnen ein besseres Verständnis dafür zu geben, wie sinnlos es ist den naiven Weg des Ausprobierens aller Potenzen zu gehen.

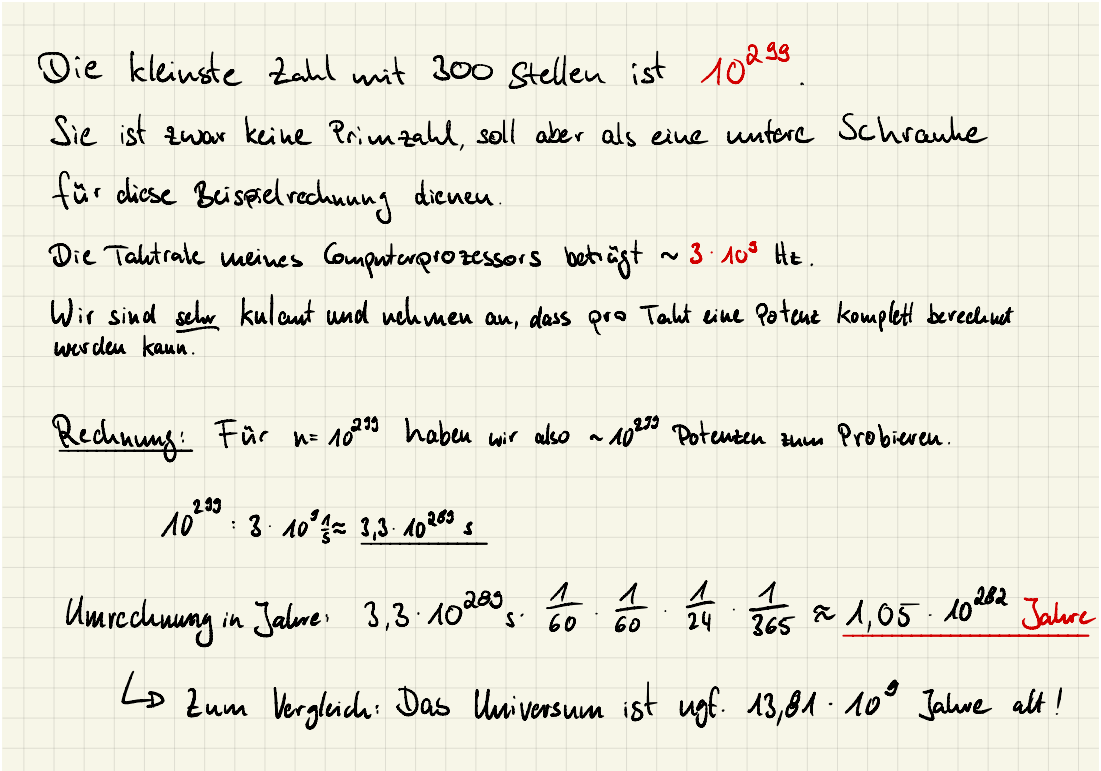


Abbildung 6: Eine Beispielrechnung zur Bestimmung der Dauer des Ausprobierens

7.6 Schüler*innenergebnis

{\SErgebnis}

Hier wird die fertige Kryptowährung der Schülerinnen und Schüler abgebildet. Diese Protokolle dienten größtenteils auch als Vorlage für Ihre Präsentation in Form eines Rollenspiels.

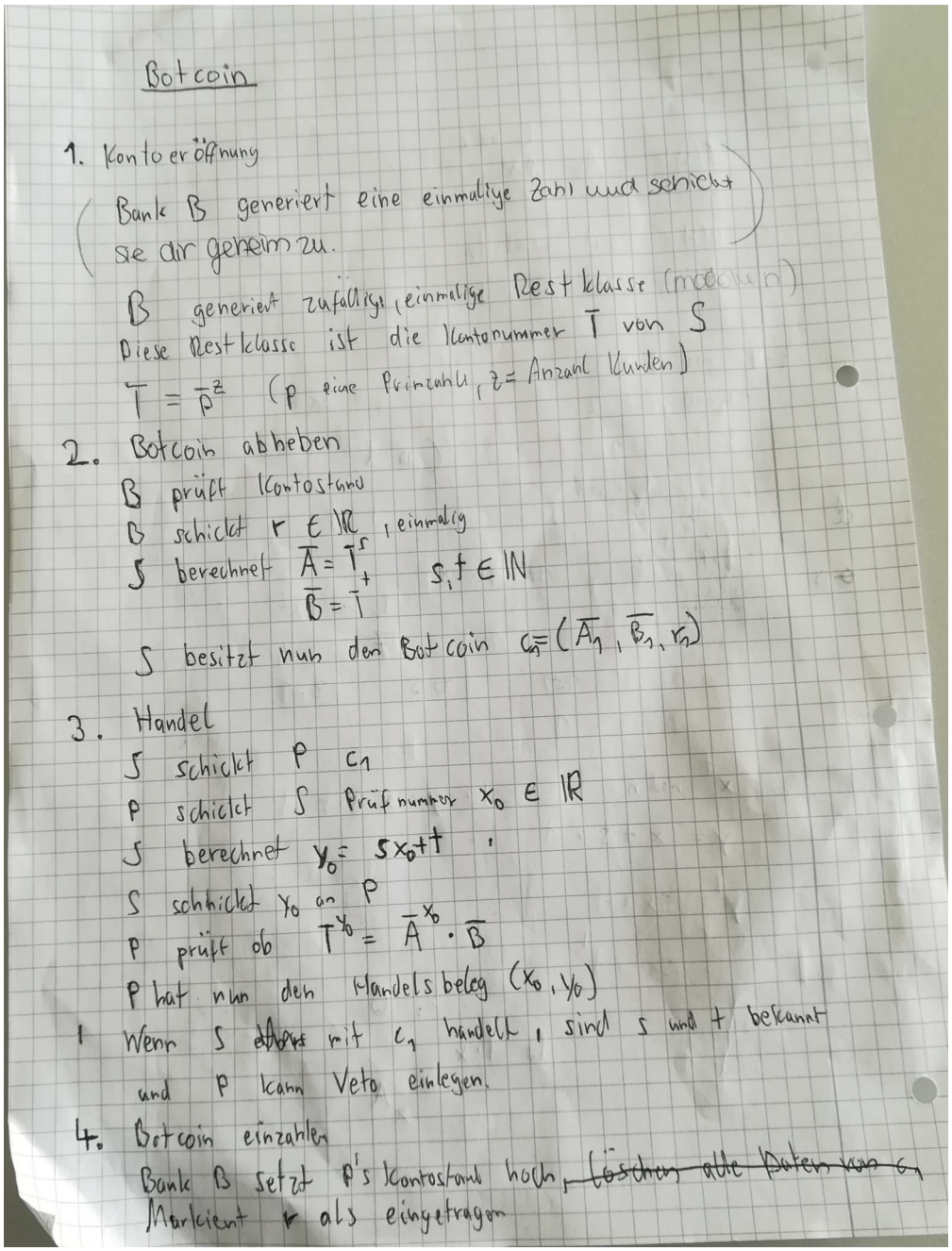


Abbildung 7: Die Grundschritte der Schüler*innen-Kryptowährung

7.7 Feedback der Schülerinnen und Schüler

{anh:Feedba

Die hier gezeigte Seite ist das gesammelte Feedback der Teilnehmendengruppe meines Themas. Es wurde separat und ohne weitere Einflüsse durch Lehrpersonen nach der Lerneinheit im Kursverband von den Schülerinnen und Schülern zusammengetragen.

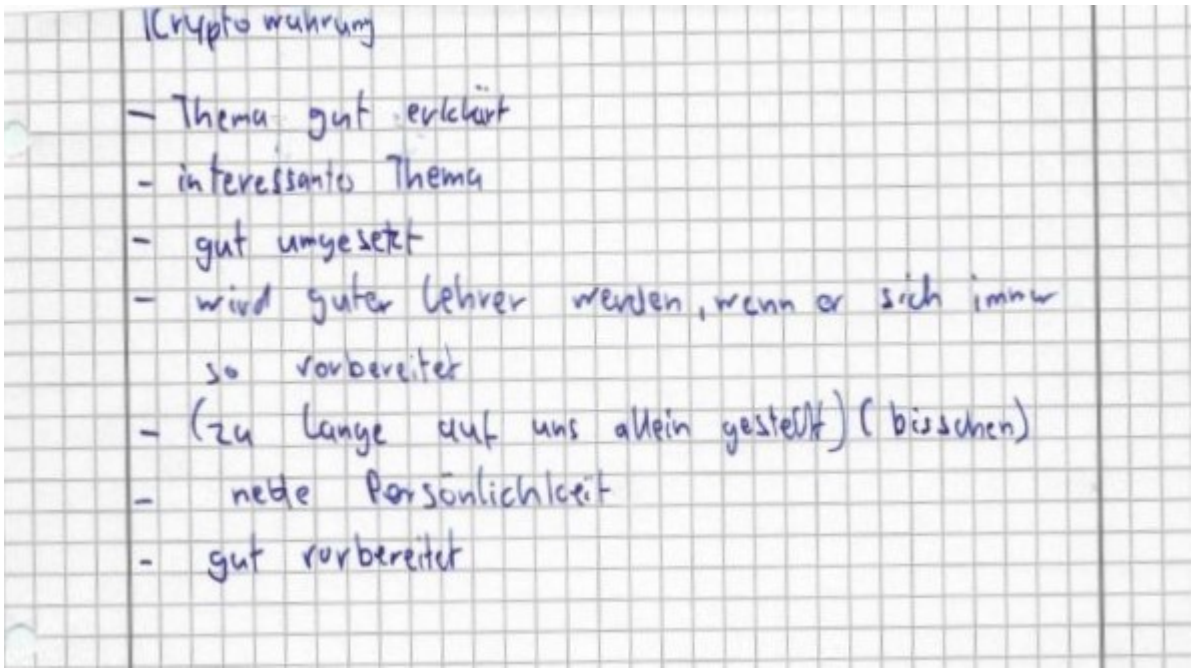


Abbildung 8: Das Feedback der Schülerinnen und Schüler

Literatur

[B+14] Buterin, Vitalik u. a.: A next-generation smart contract and decentralized application platform. In: *white paper* 3 (2014), S. 37

[Bar07] Barak, Boaz: *Zero Knowledge Proofs*. 2007. – `https://www.cs.princeton.edu/courses/archive/fall07/cos433/lec15.pdf`, Aufgerufen am 29.06.2019

[Bos14] Bosch, Siegfried: *Lineare Algebra*. Springer-Verlag, 2014

[Cha83] Chaum, David: Blind signatures for untraceable payments. In: *Advances in cryptology* Springer, 1983, S. 199–203

[EBH18] Eder, Christian ; Barakat, Mohamed ; Hanke, Timo: *An Introduction to Cryptography*. 2018. – Vorlesungsskript

[Gat18] Gathmann, Andreas: *Algebraische Strukturen; Vorlesungsskript TU Kaiserslautern 2017/18*. zuletzt aktualisiert am 08.10.2018. – Zum öffentlichen Download unter `https://www.mathematik.uni-kl.de/~gathmann/class/ags-2017/ags-2017.pdf`, Aufgerufen am 06.08.2019

[Har77] Hartshorne, Robin: *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. – Graduate Texts in Mathematics, No. 52

[Hul12] Hulek, Klaus: *Elementare algebraische Geometrie: grundlegende Begriffe und Techniken mit zahlreichen Beispielen und Anwendungen*. Springer-Verlag, 2012

[JMV01] Johnson, Don ; Menezes, Alfred ; Vanstone, Scott: The Elliptic Curve Digital Signature Algorithm (ECDSA). In: *International Journal of Information Security* 1 (2001), Aug, Nr. 1, S. 36–63

[KM16] Koblitz, Neal ; Menezes, Alfred J.: Cryptocash, cryptocurrencies, and cryptocontracts. In: *Designs, Codes and Cryptography* 78 (2016), Nr. 1, S. 87–102

[KOM19] KOMMS: *KOMMS Homepage*. 2019. – `https://komms.uni-kl.de/`, Aufgerufen am 06.08.2019

[Mer80] Merkle, Ralph C.: Protocols for Public Key Cryptosystems. Los Alamitos, CA, USA : IEEE Computer Society, apr 1980, S. 122–133

[Min98] Ministerium für Bildung, Wissenschaft, Jugend und Kultur: *Lehrplan Mathematik; Grund- und Leistungsfach; Jahrgangsstufen 11 bis 13 der gymnasialen Oberstufe (Mainzer Studienstufe)*. 1998. – Zum öffentlichen Download unter `https://lehrplaene.bildung-rp.de/?category=32`, Aufgerufen am 06.07.2019

[Min07] Ministerium für Bildung, Wissenschaft, Jugend und Kultur: *Rahmenlehrplan Mathematik (Klassenstufen 5-9/10).* 2007. – Zum öffentlichen Download unter `https://lehrplaene.bildung-rp.de/?category=32`, Aufgerufen am 06.07.2019

[Minhra] Ministerium für Bildung, Wissenschaft, Jugend und Kultur: *Lehrplan Informatik; Grund- und Leistungsfach; Einführungsphase und Qualifikationsphase der gymnsasialen Oberstufe (Mainzer Studienstufe).* unbekanntes Jahr. – Zum öffentlichen Download unter `https://lehrplaene.bildung-rp.de/?keyword=informatik`, Aufgerufen am 06.07.2019

[Minhrb] Ministerium für Bildung, Wissenschaft, Jugend und Kultur: *Lehrplan Informatik; Wahlfach und Wahlpflichtfach an Gymnasien und Integrierten Gesamtschulen (Sekundarstufe I).* unbekanntes Jahr. – Zum öffentlichen Download unter `https://lehrplaene.bildung-rp.de/?keyword=informatik`, Aufgerufen am 06.07.2019

[N+08] Nakamoto, Satoshi u. a.: Bitcoin: A peer-to-peer electronic cash system. (2008)

[Pay19] PayPal: *PayPal Homepage.* 2019. – `https://www.paypal.com/de/home`, Aufgerufen am 19.03.2019

[Pä07] Pädagogisches Zentrum Rheinland-Pfalz: *Anregungen zur Umsetzung des Rahmenlehrplans Mathematik Rheinland-Pfalz.* 2007. – Zum öffentlichen Download unter `https://lehrplaene.bildung-rp.de/?keyword=mathematik`, Aufgerufen am 06.07.2019

[Sch18] Schröder, Thorsten: *Die Zukunft der Kryptowährungen.* 2018. – `https://www.zeit.de/wirtschaft/2018-06/kryptowaehrung-bitcoin-boerse-coinbase`, Aufgerufen am 06.07.2019

[Syn17] Synek, Greg: *WikiLeaks thanks US government for blocking credit card donations.* 2017. – `https://www.techspot.com/news/71764-wikileaks-thanks-us-government-blocking-credit-card-donations.html`, Aufgerufen am 19.03.2019

Eidesstattliche Erklärung

Hiermit erkläre ich, Marcel Schütz, an Eides statt, dass ich diese vorliegende Arbeit mit dem Titel

Cryptowährungen

ohne weitere Hilfsmittel als den angegebenen Quellen selbstständig verfasst habe. Des Weiteren sind alle wörtlich oder sinnhaft zitierten Stellen aus anderen Werken als solche gekennzeichnet.

Diese Arbeit wurde weder in der vorliegenden, noch in einer veränderten Version als Abschlussarbeit oder Studienleistung an dieser oder einer anderen Universität vorgelegt.

Ort, Datum Unterschrift