Cryptocurrencies

① Eine Simulation mit Schecks bringt verschiedene Schwierigkeiten von Zahlungssystemen zutage: Geld muss immer durch die Zentrale Autorität ausgegeben werden! In der ersten, Simulation sah die Zahlung wie folgt aus (Überweisung Alice an Bob):
1. Alice schreibt einen Betrag, Bobs Namen und ihre Account-Nummer auf den Scheck
2. Sie tütet den
3. unterschriebenen Brief ein.
Was könnte das Äquivalent im Digitalen sein? Trage die Begriffe Überweisungsdaten, digitale Signatur, verschlüsselten vorangegangenen Transaktionen, öffentlichen Schlüssel, Hash ein:

digitale Signatur 1x | Hash 1x | Transaktionen 1x | öffentlichen Schlüssel 1x | Überweisungsdaten 1x

1. Alice schreibt den Betrag (die) und den

von Bob, sowie die vorangegangenen

des Gelds ein.

2. Sie berechnet den dieser Daten.

3. Sie hängt eine an

② Im zweiten Ablauf mit mir als sicherem Hafen sieht der Ablauf so aus:
1. Eine Überweisung von Alice an Bob ist eine Überweisung von Alice an die Bank und einer von der Bank an Bob.
2. Man vertraut der CA.

Bob 2x | digitale Signatur 1x | Hash 1x | macht dasselbe 1x | Transaktionen 1x | öffentlichen Schlüssel 1x | Überweisungsdaten 1x

1. Alice schreibt den Betrag (die) und den

der Bank, sowie die vorangegangenen

des Gelds auf den Scheck. Auf die Rückseite schreibt sie die

Bitte, dass das Geld an gehen soll.

2. Sie berechnet den dieser Daten.

3. Sie hängt eine an

4. Die Bank nur mit Empfänger

③ Lest gemeinsam das Szenario eurer Gruppe

- Stelle das Szenario in einer Szene dar. Ihr sollt alle beteiligt sein und werdet euer Szenario uns allen gleich vorstellen
- Falls ihr bereits fertig seid: Denkt euch zwei Möglichkeiten aus, wie diese Gruppe wieder einen funktionierenden Geldverkehr herstellen könnte. Diese Ideen könnt ihr der Gruppe auch vorstellen.

Double Spending

Zwei Personen wollen sich etwas überweisen. Sie haben leider beide keinen Kontakt zu einer Bank, da die Bank gehackt wurde. Nun könnte A an B etwas überweisen und denselben Betrag an C, obwohl A diesen Betrag gar nicht mehr besitzt. Dieses Problem ist als *Double Spending* bekannt. Nehmen wir an, eine Gruppe von Personen tut sich zusammen.

Modifikations-Attack

Zwei Personen wollen sich etwas überweisen. Sie haben leider beide keinen Kontakt zu einer Bank, da die Bank gehackt wurde. Daher machen alle Menschen eine gemeinsame Liste aller Transaktionen, die getätigt wurden. Eine Person schreibt sich eigene Transaktionen in die Liste, die aber gar nicht stattgefunden haben. Dies ist eine *Attacke durch Modifikation*.

Neuschreib-Attacke

Zwei Personen wollen sich etwas überweisen. Sie haben leider beide keinen Kontakt zu einer Bank, da die Bank gehackt wurde. Daher machen alle Menschen eine gemeinsame Liste aller Transaktionen, die getätigt wurden. Nun kommt eine Person her, und behauptet, dass sie eigentlich die „richtige“ Liste hätte. Dies ist eine *Attacke durch Neuschreiben*.

④ Zusatzaufgabe: Beantworte die folgenden Leitfragen bei Lektüre des nachfolgenden Textes: Antworte in drei Sätzen.

1) Was ist ein Block?
2) Beschreibe, wie in der Blockchain die Attacke, für die Du Experte warst, verhindert wird.
3) Was meint der Text, wenn es heißt „Unsere bisherige Geldwirtschaft basiert darauf, dass die Überweisungen immer über eine Bank getätigt werden.“?
4) Wofür braucht es einen Nonce?

Wie Blockchain funktioniert (freiwillige Lektüre)

Bitcoin hat zwei Strukturen: Zum einen einen eine Reihe von Überweisungen in unserer ersten Simulation . Zum anderen ein gemeinsames "Buch" aller Überweisungen. Wir betrachten beide einzeln.

Die Reihe von Überweisungen sieht aus wie oben: Jedes Stück Geld (denke: jeder Cent) hat einzeln einen Besitzer und besteht lediglich aus einem Binärstring (seiner bisherigen Transaktionshistorie). Möchte diese*r seinen Coin weitergeben, so erstellt er einen neuen Binärstring wie folgt: Er nimmt den öffentlichen Schlüssel des nächsten Besitzers (dieser wird als Name für den neuen Besitzer benutzt) zusammen mit dem bisherigen Binärstring, hasht beide und hängt eine Signatur dieser Daten an, nachdem er verifiziert hat, dass er das Geld auch wirklich senden möchte.

Wie wir gesehen haben: Hier benötigt die Empfängerin großes Vertrauen, da der Überweiser einen Cent mehrmals ausgeben muss. Unsere bisherige Geldwirtschaft basiert darauf, dass die Überweisungen immer über eine Bank getätigt werden, wie wir in der zweiten Simulation gesehen haben.

Die zweite Struktur ist eine Blockchain. Diese notiert Blöcke, die jeweils aus einer Reihe von Transaktionen in einem Zeitraum und einem Zeitstempel (also einer Uhrzeit) wann dieser Zeitraum war, bestehen. Die Blockchain besteht zu jedem Zeitpunkt aus einem Binärstring. Wird ein neuer Block in die Blockchain (=„Kette von Blöcken“) notiert, so nimmt man den bisherigen Wert, hängt Zeitstempel und Transaktionen und eine weitere Zahl, genannt *Nonce* an.

Die Nonce ist eine Zahl, die so gewählt sein muss, dass viele Nullen am Anfang des Hash-Ergebnisses stehen. Diese sorgt dafür, dass eine Attacke durch Neuschreiben und eine Attacke durch Modifikation nicht möglich sind: Die Nonce zu finden ist hart. Und für unterschiedliche Transaktionen muss die Nonce eine andere sein. Weiterhin müsste, wenn man eine eine Attacke durch Neuschreiben versucht, man selbst sehr schnell rechnen: Denn es ist für alle Beteiligten vorteilhaft, die Blockchain für wahr zu halten, in der am meisten gerechnet wird: Diese ist die „Wahrheit“. Und auf der Wahrheit kann man "nachschauen", ob Personen genug Geld haben, um eine Überweisung zu tätigen.

Double Spending wird wie folgt verhindert: In einem gemeinsamen werden Block Double Spends von niemandem außer der Betrügerin geglaubt, also rechnet niemand an dieser Blockchain nicht weitergerechnet wird. Wird später überwiesen, so können alle anderen "nachschauen, ob der Überweisende genug Geld hat.