8.12 Exkurs: Blockchain, Kryptowährungen und Mining

ZUSATZ

> ZUSATZ
>
> Ein Exkurs im Wortsinn: Kein Lehrplan verlangt ihn. Er benutzt ausschließlich Bausteine, die Sie schon kennen — Hashfunktion und Signatur — und zeigt, was sich daraus bauen lässt.

Über kaum eine Technik ist so viel geschrieben worden wie über die Blockchain, und kaum eine ist so einfach. Sie besteht fast nur aus dem Baustein des vorigen Abschnitts: der Hashfunktion. Wer verstanden hat, was SHA-256 tut, versteht in zwanzig Minuten eine Blockchain.

8.12.1 Das Problem: ein Kassenbuch ohne Kassenwart

Eine Überweisung ist nichts Körperliches. Sie ist eine Zeile in einem Buch: *Lena zahlt 10 an Jonas*. Damit das funktioniert, muss jemand das Buch führen, dem alle vertrauen — eine Bank. Sie verhindert, dass Lena dieselben 10 Euro zweimal ausgibt, und sie verhindert, dass jemand nachträglich Zeilen ändert.

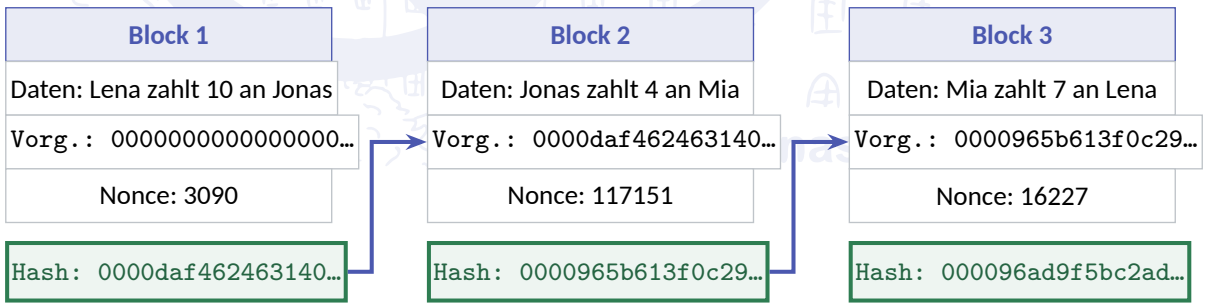
Leitidee: Die Frage hinter der Blockchain

Kann man ein Kassenbuch führen, das **alle** besitzen, in das **jeder** schreiben darf — und in dem trotzdem niemand nachträglich etwas ändern kann?

Die erste Hälfte ist leicht: Man schickt das Buch an alle. Die zweite ist das Problem. Wer eine Kopie hat, kann darin radieren.

8.12.2 Die Kette

Der Trick ist eine Kette aus Hashwerten. Die Zeilen werden zu **Blöcken** zusammengefasst, und jeder Block enthält — neben seinen eigenen Daten — den **Hashwert seines Vorgängers**.



Jeder Hash deckt alles ab, was über ihm im Block steht — auch den Hash des Vorgängers.

Eine Blockchain mit drei Blöcken. Die Werte sind echte SHA-256-Hashes.

Was das bewirkt, sieht man am besten beim Versuch zu betrügen. Angenommen, jemand ändert in Block 1 den Betrag von 10 auf 100. Dann ändert sich der Hashwert von Block 1 vollständig:

```
vorher:  0000daf462463140…
nachher: 3448594b61837fab…
```

Block 2 trägt aber noch den alten Wert als Vorgänger-Hash. Die Kette passt nicht mehr zusammen, und zwar sichtbar für jeden, der nachrechnet. Wer die Fälschung verbergen will, muss auch Block 2 neu berechnen — und dann Block 3, und alle weiteren.

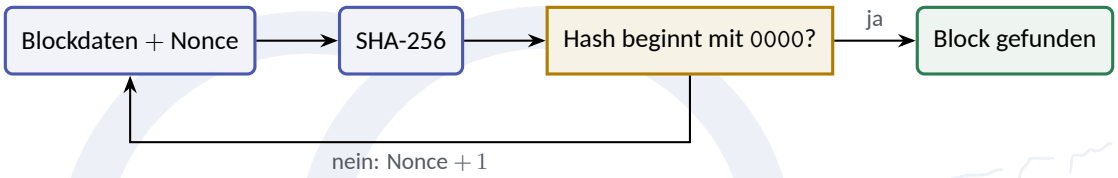
Merke

Eine Blockchain macht Änderungen nicht *unmöglich*. Sie macht sie **auffällig**: Wer einen alten Block ändert, muss die gesamte Kette dahinter neu bauen.

8.12.3 Mining: Arbeit als Bremse

Neu bauen wäre für einen Rechner eine Sache von Millisekunden. Deshalb kommt eine zweite Zutat hinzu: Ein Block gilt nur dann als gültig, wenn sein Hashwert eine **Bedingung** erfüllt — zum Beispiel, dass er mit mehreren Nullen beginnt.

Am Hashwert selbst lässt sich nicht drehen; er ergibt sich aus dem Inhalt. Also baut man ein Feld in den Block ein, das sonst keinen Zweck hat: die **Nonce** (von *number used once*). Man zählt sie hoch und rechnet jedes Mal den Hash neu, bis die Bedingung zufällig erfüllt ist. Dieses Suchen heißt **Mining**.



Mining ist Ausprobieren. Einen anderen Weg gibt es nicht.

Beispiel: Wie teuer die Bedingung ist

Gehasht wird jeweils die Zeichenkette aus Datensatz, einem senkrechten Strich und der Nonce, also `Lena zahlt 10 an Jonas|0`, dann `Lena zahlt 10 an Jonas|1` und so fort. Gesucht ist die kleinste Nonce, bei der der SHA-256-Wert mit einer bestimmten Zahl von Nullen beginnt:

Bedingung	gefundene Nonce	Versuche	Rechenzeit
`0…`	7	8	unmessbar
`00…`	370	371	unmessbar
`000…`	9 815	9 816	0,01 s
`0000…`	10 021	10 022	0,01 s
`00000…`	4 728 918	4 728 919	3,4 s

Jede zusätzliche Null macht die Suche im Mittel **sechzehnmal** teurer — eine Hexadezimal stelle hat sechzehn mögliche Werte. Das echte Bitcoin-Netz arbeitet derzeit mit einer Bedingung, für die ungefähr 10^{23} Versuche nötig sind.

Merke

Prüfen ist billig, Finden ist teuer. Diese Asymmetrie ist der ganze Mechanismus: Ein einziger Hashdurchlauf bestätigt, was Billionen Versuche gekostet hat. Man nennt das **Proof of Work** — Arbeitsnachweis.

8.12.4 Was eine Kryptowährung daraus macht

Eine Kryptowährung ist dieses Kassenbuch, verteilt auf viele tausend Rechner.

- Wer eine Überweisung tätigen will, **signiert** sie mit seinem privaten Schlüssel (Abschnitt 8.11). Die „Kontonummer" ist der zugehörige öffentliche Schlüssel. Es gibt kein Konto, keinen Namen, keine Bank — nur ein Schlüsselpaar.
- Die Rechner im Netz sammeln Überweisungen und suchen nach einer gültigen Nonce. Wer zuerst eine findet, verbreitet seinen Block, und alle anderen hängen ihn an.
- Als Lohn darf der Finder sich selbst eine festgelegte Menge neuer Münzen gutschreiben. Daher der Name *Mining*: Es sieht aus, als würde Geld geschürft, tatsächlich wird eine Rechenleistung bezahlt.
- Gehen zwei Ketten auseinander, gilt die Regel: **Die längste Kette zählt.** Wer eine Fälschung durchsetzen will, muss also schneller rechnen als der gesamte Rest des Netzes zusammen.

Leitidee: Was wirklich gelöst wurde

Das Problem war nie die Verschlüsselung — die gab es längst. Gelöst wurde die Frage, wie sich Fremde, die einander nicht trauen und keine gemeinsame Instanz anerkennen, auf **eine** Reihenfolge von Ereignissen einigen. Der Preis dafür ist, dass diese Einigung Rechenarbeit kostet, und zwar absichtlich.

8.12.5 Was es kostet

Die absichtliche Verschwendung ist kein Nebeneffekt, sondern das Sicherheitsmerkmal — und sie hat eine Größenordnung. Das Bitcoin-Netz verbrauchte zuletzt Strom in der Größenordnung eines mittleren europäischen Staates, für eine Zahl von Überweisungen, die ein einzelner Bankrechner nebenbei abwickelt. Neuere Netze wie Ethereum sind deshalb auf **Proof of Stake** umgestiegen: Dort entscheidet nicht Rechenarbeit, wer den nächsten Block anhängen darf, sondern ein hinterlegtes Pfand.

Dazu kommen Eigenschaften, die je nach Standpunkt Vorzug oder Mangel sind:

Eigenschaft	Folge
keine zentrale Stelle	niemand kann Konten sperren — und niemand hilft bei Verlust
Schlüssel statt Konto	wer den privaten Schlüssel verliert, verliert alles, endgültig
unumkehrbare Buchungen	kein Rückruf bei Irrtum oder Betrug
öffentliche Kette	jede Überweisung ist für immer einsehbar, pseudonym, nicht anonym
Kurs ohne Deckung	der Wert folgt allein Angebot und Nachfrage

Merke

Die Technik ist nachprüfbar, die Bewertung ist es nicht. Dieser Exkurs erklärt, **wie** eine Blockchain funktioniert — ob sie für eine bestimmte Aufgabe das richtige Werkzeug ist, ist eine wirtschaftliche und politische Frage, keine informatische.

Arbeitsauftrag 12

46. Berechnen Sie mit einem Programm die SHA-256-Werte von `Informatik` und `informatik`. Wie viele Stellen stimmen überein? Welche Eigenschaft einer Hashfunktion zeigt sich daran?
47. Schreiben Sie ein Programm, das zu einem Text die kleinste Nonce sucht, deren SHA-256-Wert mit `000` beginnt. Gehasht wird `<Text>|<Nonce>` wie in der Tabelle oben; in Python genügt `import hashlib`.
48. Erweitern Sie es auf vier und fünf Nullen und messen Sie die Zeit. Vergleichen Sie mit der Tabelle oben. Warum weichen Ihre Nonce-Werte nicht ab, Ihre Zeiten aber schon?
49. Bauen Sie eine Kette aus drei Blöcken nach. Ändern Sie dann den Inhalt von Block 1 und zeigen Sie an den Hashwerten, dass die Kette bricht.
50. Begründen Sie, warum ein Angreifer mit 10 % der Rechenleistung des Netzes eine Fälschung praktisch nicht durchsetzen kann.
51. Erläutern Sie den Unterschied zwischen *pseudonym* und *anonym* am Beispiel einer öffentlichen Blockchain.

Selbstcheck

Können Sie in zwei Sätzen erklären, warum eine Blockchain ohne Proof of Work nichts nützt — und was genau die Nonce mit Sicherheit zu tun hat?

Gymnasium Ottweiler