Kryptowährungen

(Teil 1)

Peter Giger

Warum dieses Thema?

- Wer hat die Wirtschaftskrise 2008 verursacht?
- Dezentrale Währung (keine Banken notwendig)
- (Pseudo-) Anonymität
- Kryptowährungen als Investment
- Fast tägliche News über Krypto
- ...

"I do think Bitcoin is the first [encrypted money] that has the potential to do something like change the world." – Peter Thiel, co-founder of PayPal

Forbes

Apr 29, 2013, 01:45pm EDT

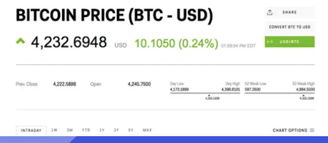
Big VC Says Bitcoin Is 'Gold 2.0. It's a Huge, Huge, Huge Deal'

HOME > MARKETS

JAMIE DIMON: Bitcoin is a fraud that's 'worse than tulip bulbs'

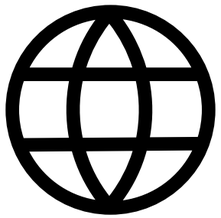
Akin Oyedele Sep 12, 2017, 8:02 PM

JPMorgan CEO Jamie Dimon says bitcoin is worse than the most famous asset bubble in history.



Lernziele

Grobe Lernziele



Grundwissen über Kryptowährungen

- Sie können bei Diskussionen über das Thema "Kryptowährungen" mitreden.
- Sie verstehen Newsartikel zu Krypto-Themen und können sich eine eigene Meinung dazu bilden.

Detailwissen über Kryptowährungen

- Sie haben ein vertieftes Wissen bezüglich der Funktionsweise von Kryptowährungen.

  Stichworte:
  - Double-Spending Problem
  - Kryptografiische Hashfunktion
  - Proof-of-Work
  - ...

Was verstehst du unter dem Begriff "Kryptowährung"?

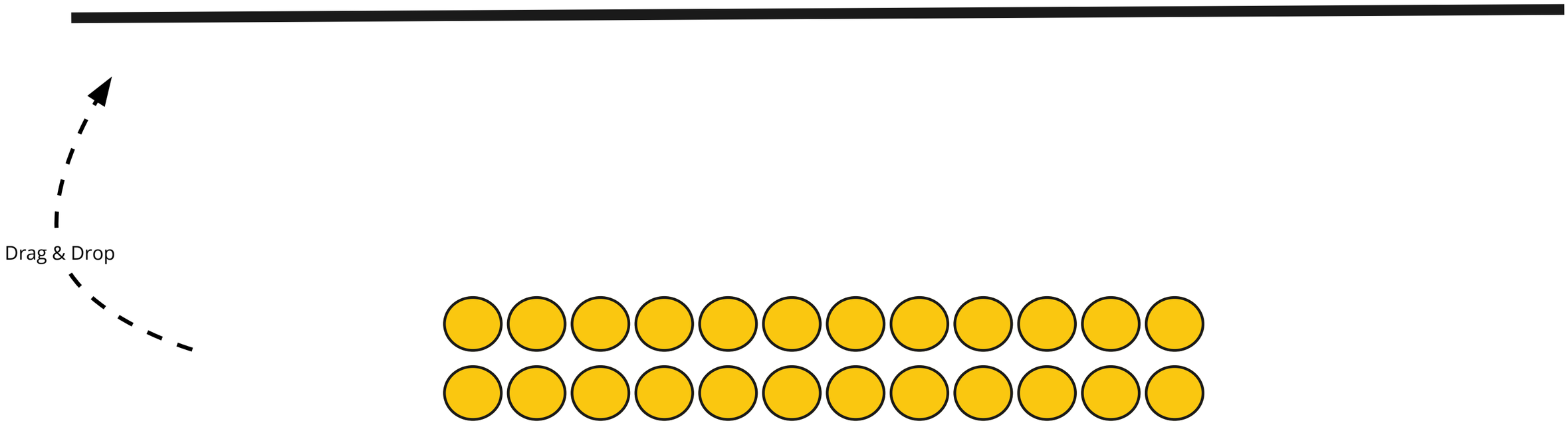
(Doppelklick auf die Notizzettel)

Halten sie ihre Gedanken auf diesen Notizzettel fest

Wie würdest du dein Vorwissen bzgl. Kryptowährungen einschätzen?

(Punkte auf die Skala ziehen)

Anfänger **Experte**



Agenda

- Was ist eine Kryptowährung?
- Zentrale vs. dezentrale Datenbank
- Double-Spending Problem

☕ Pause ☕

- Kryptografische Hashfunktion
- Blockchain

Einfach(er)

Schwierig(er)

Was ist eine Kryptowährung?

Was ist eine Kryptowährung?

Definition

"Eine Kryptowährung ist ein **digitaler Vermögenswert,** der auch als Tauschmittel fungiert. Einzelne Vermögenszuschreibungen sind dabei in einer **dezentralen Datenbank** (Distributed- Ledger-Technologie), in der Regel einer **Blockchain**, festgehalten. Diese öffentliche Finanz- transaktionsdatenbank verwendet starke **Kryptographie**, um die **Transaktionen** und Be- sitztümer und gegebenenfalls die Erschaffung von weiteren Coins oder auch die Vernichtung von Coins zu verifizieren und zu sichern."

-- Wikipedia

Was ist eine Kryptowährung?

Bitcoin

- Erste und bekannteste Kryptowährung
- White Paper wurde 2008/2009 veröffentlicht
- Author: Santoshi Nakamoto (Pseudonym)
- 1 Bitcoin = 40'000.- (ungefähr)
- Ca. 18.7 Mio. Bitcoins im Umlauf
- Max. 21 Mio. Bitcoins wird es geben

Was ist eine Kryptowährung?

Aufgabe (Teil 1)

Notieren sie verschiedene Kryptowährungen inkl. deren ungefähren Wert in CHF (aktuell, vor einem Monat und vor einem Jahr):

Bitcoin

Aktuell: 45000.-
Monat: 35000.-
Jahr: 10000.-

Was ist eine Kryptowährung?

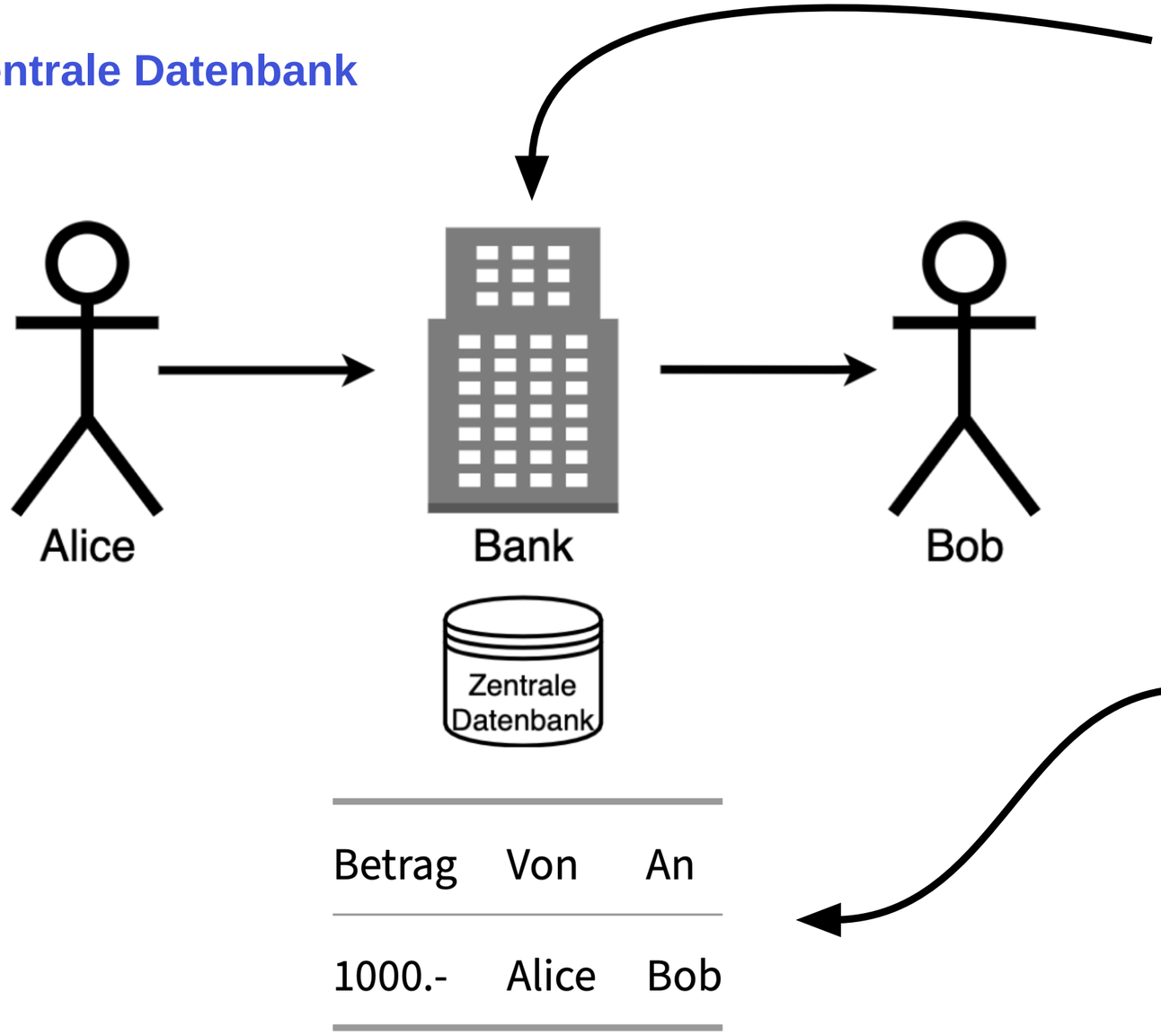
Aufgabe (Teil 2)

Was ist auffällig? Welche Faktoren beeinflussen den Wert von Kryptowährungen?

Zentrale vs. dezentrale Datenbank

Zentrale vs. dezentrale Datenbank

Zentrale Datenbank



Intermediär:

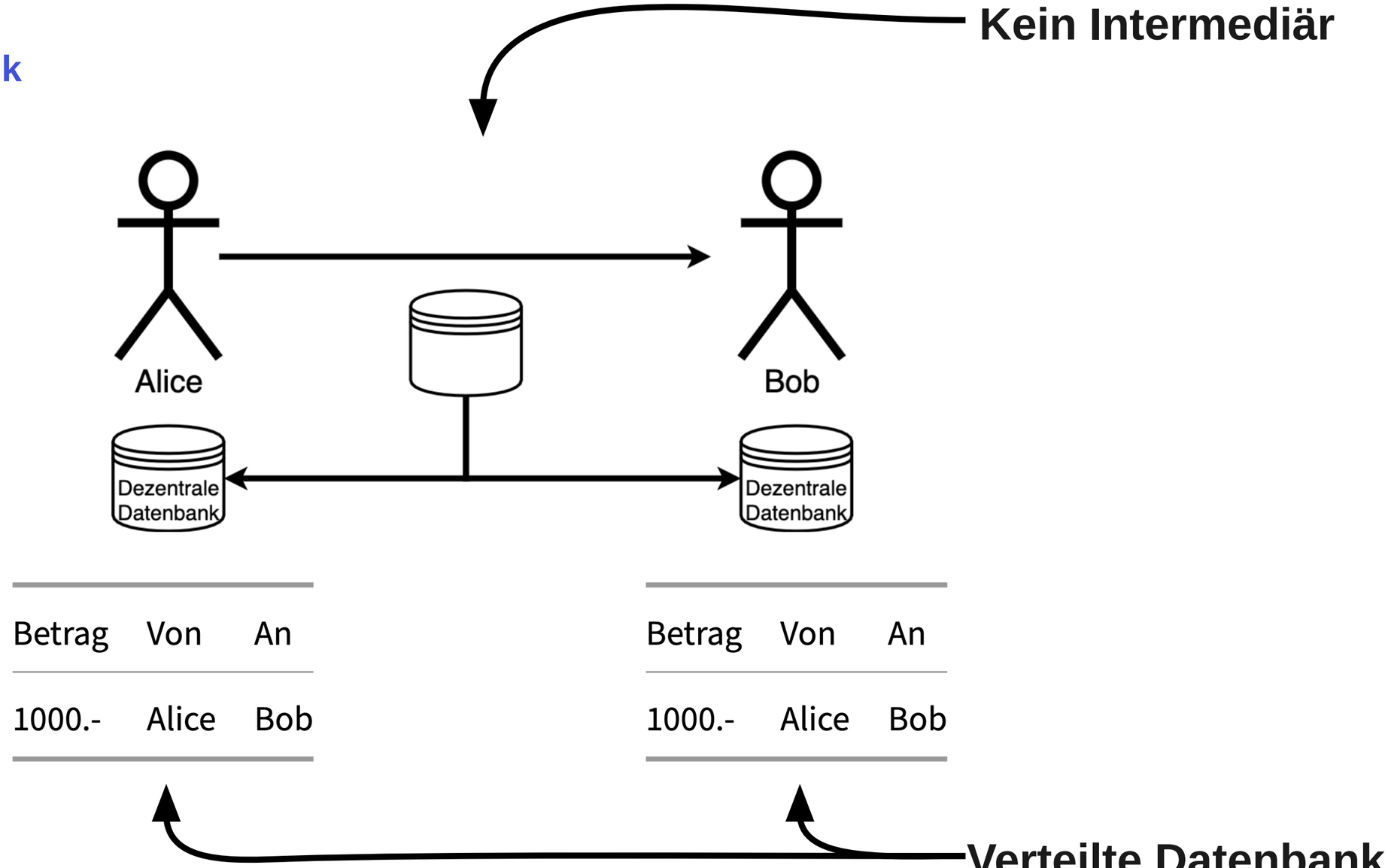
- Muss vertrauenswürdig sein
- Prüft Transaktionen

Beispiel: Alice überweist 1000.- auf Bob's Konto.

Zentrale Datenbank (Transaktionstabelle)

Zentrale vs. dezentrale Datenbank

Dezentrale Datenbank



Zentrale vs. dezentrale Datenbank

Aufgabe

Erstellen sie eine Transaktionstabelle für folgendes Beispiel:

Alice überweist Charlie 200.-, Bob überweist Alice 300.- und Charlie überweist Bob 100.-.

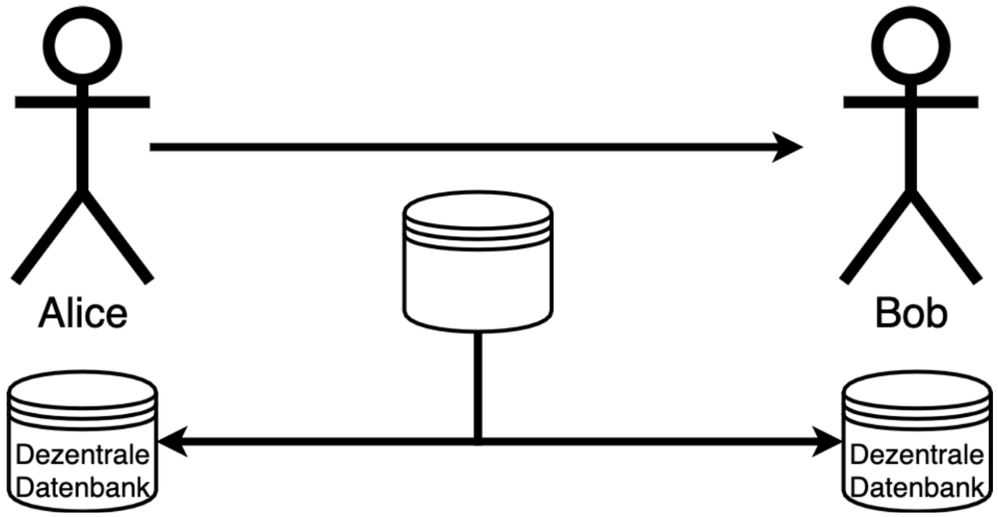
Lösung:

Transaktionstabelle

Double-Spending Problem

Double-Spending Problem

Ein Problem von dezentralen Datenbanken



Betrag	Von	An
1000.-	Alice	Bob

Betrag	Von	An
1000.-	Alice	Bob
1000.-	**Alice**	**Bob**

Bob könnte die Transaktion von Alice doppelt ausführen und hätte dann 2000.- auf seinem Konto.

Oder andersrum könnte Alice eine Transaktion von Bob löschen und müsste nur den halben Betrag bezahlen

Beschreiben sie das “Double-Spending Problem” in eigenen Worten

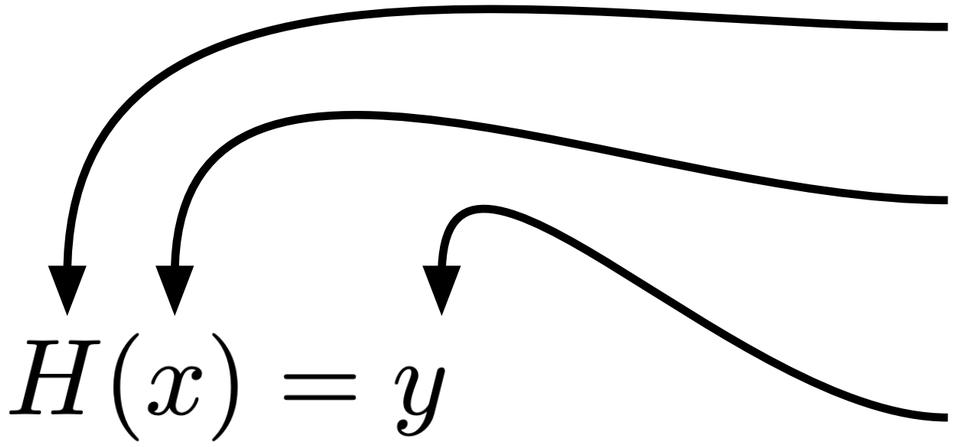
Aufgabe

Halten sie ihre Gedanken auf diesen Notizzettel fest

Kryptografische Hashfunktion

Kryptografische Hashfunktion

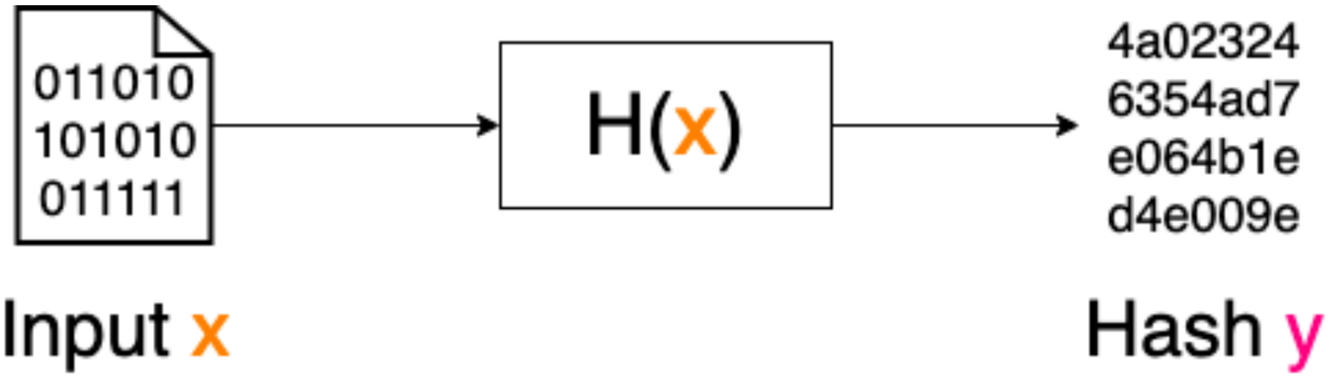
Grundlegendes kryptografisches Verfahren von Kryptowährungen



Hashfunktion

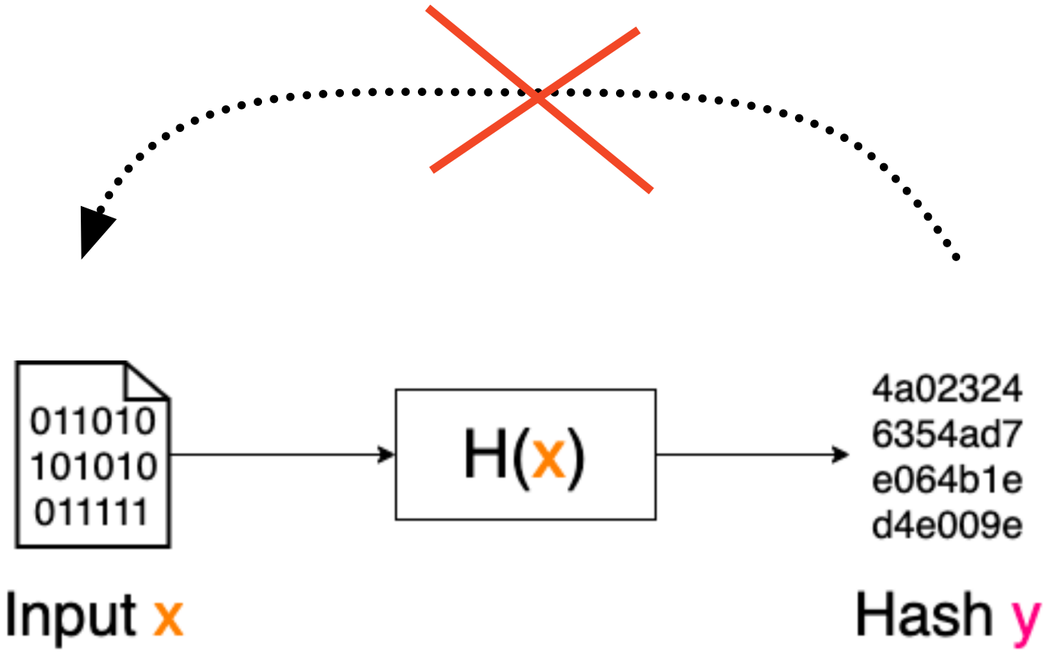
Input: Beliebig langer Bitstring
z. B. 0010101010101010101

Output: Hash mit
vordefinierter Länge



Kryptografische Hashfunktion

Wichtigste Eigenschaft



Einwegfunktion

Beispiel:

einfach

4 * 60 = 240

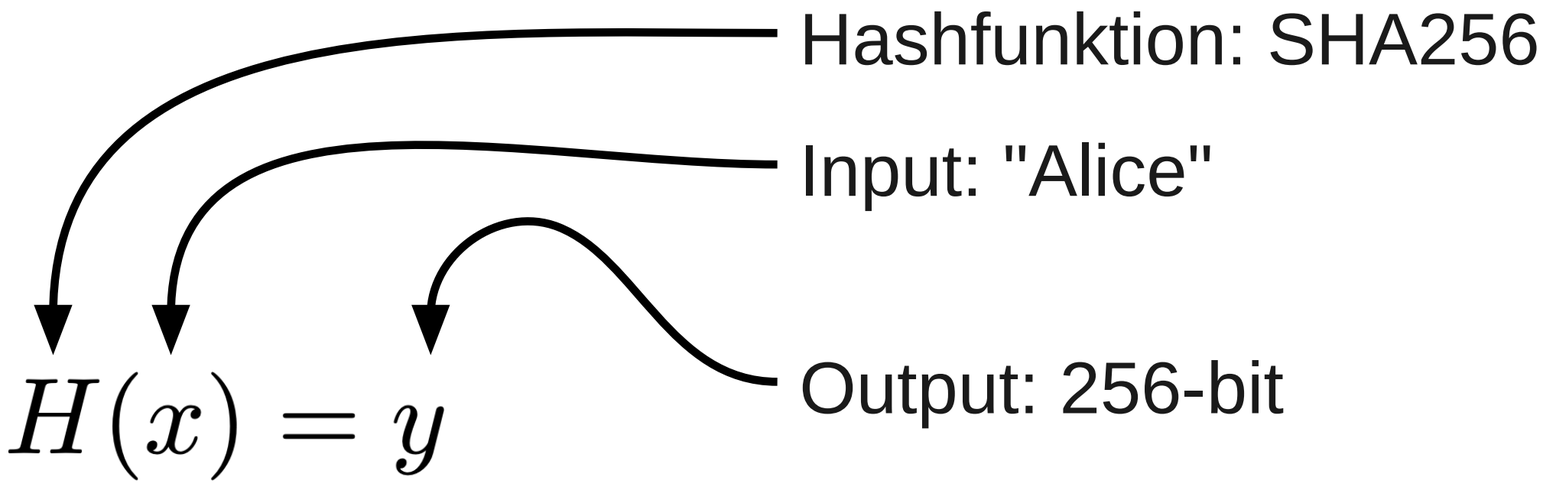
schwierig

1 * 240 = 240
2 * 120 = 240
3 * 80 = 240
...

Kryptografische Hashfunktion

Beispiel: SHA256 (Secure Hash Algorithm)

H("Alice") = 3bc51062973c458d5a6f2d8d64a023246354ad7e064b1e4e009ec8a0699a3043



Kryptografische Hashfunktion

Aufgabe (Teil 1)

Generieren sie den SHA256-Hash für ihren Namen und eine beliebige Datei (z.B. ein Word-Dokument). Tragen sie ihren Namen + Hash in den Notizzettel (unten) ein. Online-Tools: Link1 Link2

H(Peter Giger)
= 2051256ecaef76
3a62c50e958f473
ab1eac51ee62cb1
2a19b28af757060
81ec9

Kryptografische Hashfunktion

Aufgabe (Teil 2)

Wie kann ein Hash verwendet werden, um Passwörter nicht im Klartext speichern zu müssen?

Lösung:

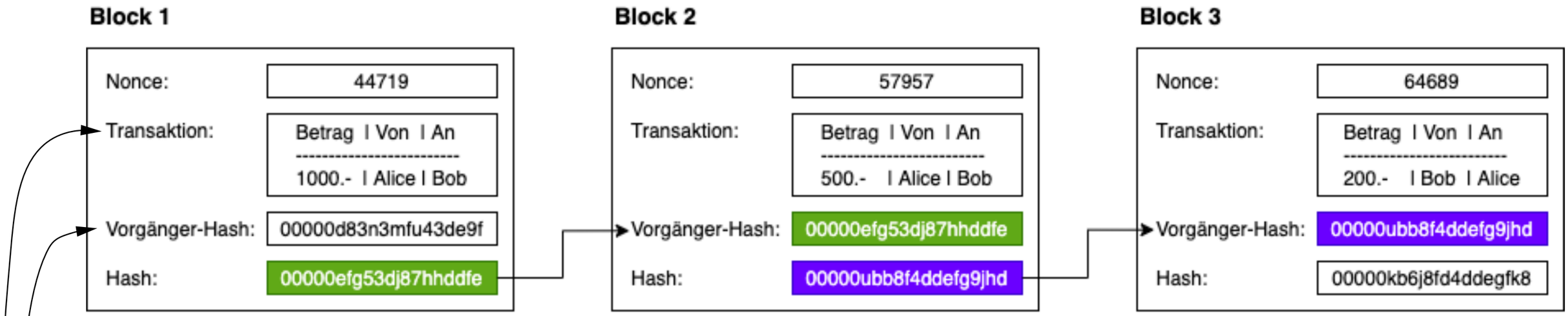
Was ist der Input x für folgenden Hash? Begründen sie ihre Antwort.
SHA256-Hash: bfd730470c1f0cd737eb895bf9de2d7996e05cb09b6a0b9be6eca53524a044a7

Lösung:

Blockchain

Blockchain

Basis von Kryptowährungen

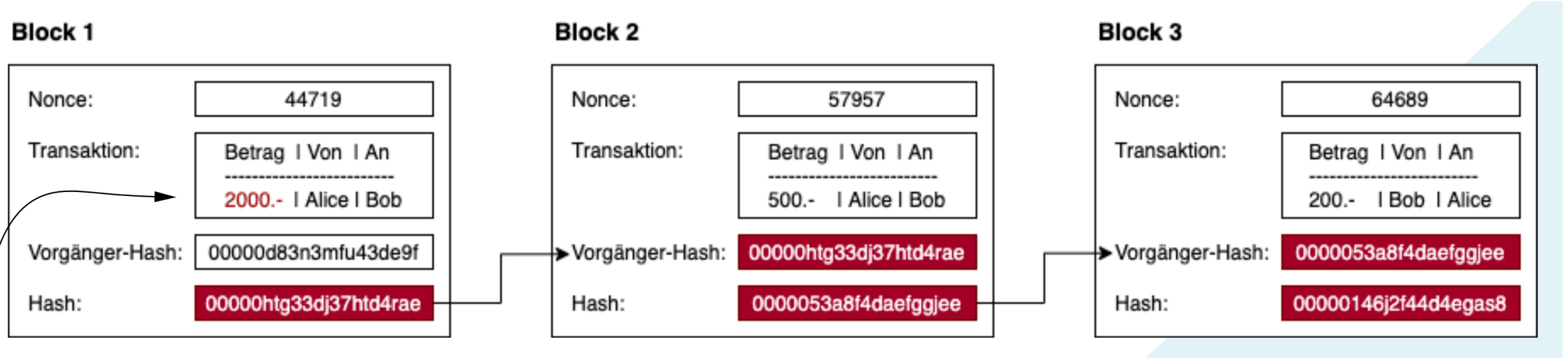


"Revolution" des Bitcoin-Paper:

- Transaktionen werden in Blöcke verpackt und aneinandergereiht
- Jeder Block enthält den Hash des Vorgängers

Blockchain

Basis von Kryptowährungen



Schützt vor Manipulationen:

- Bei einer Manipulation müssen alle Hashes neu berechnet werden (da der nächste Block den Vorgänger-Hash gespeichert hat)

> Aber: Hashes neu berechnen geht schnell und problemlos

Blockchain

Basis von Kryptowährungen

Proof-of-Work:

- > Verlangsamt die Neuberechnung der Hashes

- Ein Angreifer müsste (extrem) viel Rechenleistung haben d. h. die Mehrheit (>50%) der Rechenleistung in einem Netzwerk

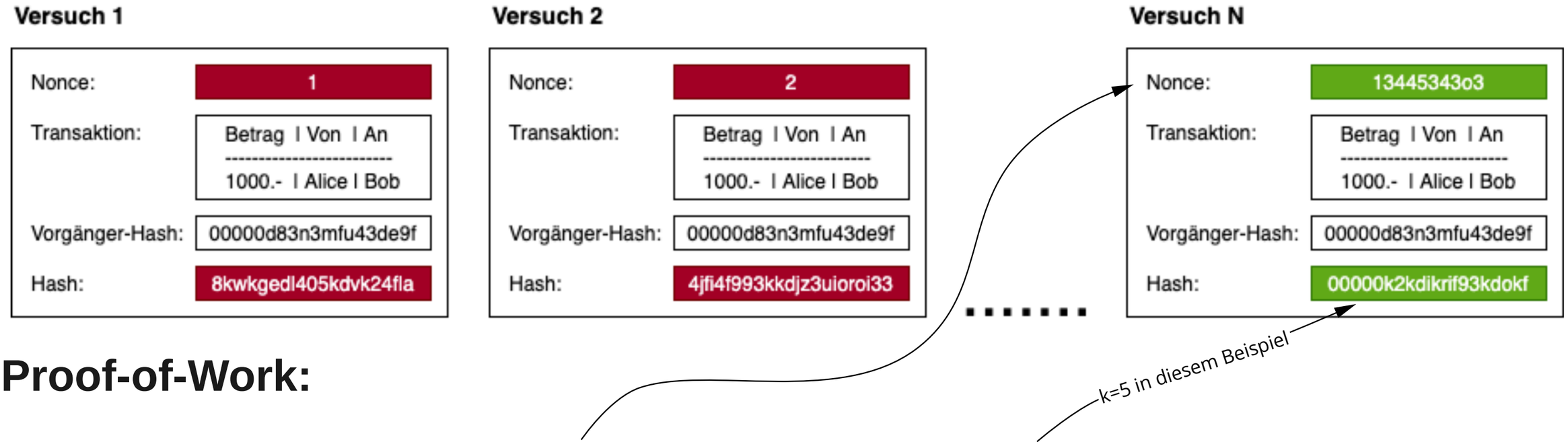
Prinzip:

Der Hash des Blocks muss mit **(k) Nullen** beginnen. Eine **Nonce** ("Willkürliche Zahl") wird **durchprobiert**, bis der Hash mit (k) Nullen beginnt.

Ein Hash mit k=4 muss mit vier Nullen beginnen z.B. 0000af2mm42d423d

Blockchain

Basis von Kryptowährungen



Proof-of-Work:

- Durchprobieren einer Nonce bis der Hash mit (k) Nullen beginnt
- Wird auch "Mining" genannt
- Funktioniert, da Einwegfunktion (durchprobieren ist die einzige Möglichkeit)

Blockchain

Aufgabe (Teil 1)

Finden sie einen input x für den der SHA256-Hash mit k = 2 Nullen beginnt. Was ist das Beste Vorgehen? Tragen sie ihr Ergebnis in den Notizzettel (unten) ein. Online-Tool: Link1

Blockchain

Aufgabe (Teil 2)

Was ist Bitcoin-Mining, wie funktioniert es und warum gibt es so viele Bitcoin-Miner? Tipp: Suchen sie im Internet nach dem Begriff.

Lösung:

Benutzen dieses Tool um ein Gefühl für die Blockchain zu bekommen. Was sind ihre Erkenntnisse? Tipp: Verändern sie dabei Daten, BlockNr, Nonce etc.

Lösung: