# Kryptowährungen

## Einführung und praktische Ansätze

Noah Lehmann

Hochschule für Angewandte Wissenschaften Hof

Seminar Aktuelle Themen der IT-Sicherheit, 06.12.2021

# Überblick

# Was sind Kryptowährungen?

*Kryptowährungen sind digitale (Quasi-)Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem [1].*

# Zwischenstand

# Geschichte

## Teil I - Einfache Wertgegenstände

Womit hat man in der Vergangenheit bezahlt?

- Wertgegenstände
  - Schwer reproduzierbar
  - Leicht transportabel
  - Leicht verifizierbar
  - Beispiele:
    - Muscheln
    - Perlen
    - Silber
    - Gold

# Geschichte

## Teil II - Währungen

**Fiat** $\rightarrow$ *fieri* (Latein) – „es werde/ es soll“

- Zentrale Steuerung
- Beeinflussung durch Staaten

# Teil II - Währungen - Beeinflussung

*Der Zentralbank muss vertraut werden, dass sie die Währung nicht entwertet, aber die Geschichte der Fiat-Währungen ist voll von Verstößen gegen dieses Vertrauen [5].*

# Geschichte

## Teil II - Währungen

**Fiat** $\rightarrow$ *fieri* (Latein) – „es werde/ es soll“

- Zentrale Steuerung
- Beeinflussung durch Staaten
- Zentrale Fehlerquelle

# Teil II - Währungen - Zentrale Fehlerquelle

*Wir müssen ihnen unsere Privatsphäre anvertrauen und darauf hoffen, dass sie unsere Konten nicht von Betrügern leerräumen lassen [5].*

# Geschichte

## Teil III - Inspirationen für Bitcoin

**b-Money** (1999)

- digitale Währung
- Dezentralität und Transaktionen ohne Mittelsmänner

**Hashcash** (2002)

- DoS Schutz für Mail-Server
- **PoW** $\rightarrow$ *Proof of Work* (Englisch) – „Arbeitsnachweis“

# Zwischenstand

# Kryptowährung

## Blick auf Ziele

1. Dezentralisierung
2. Verteilter Konsens
3. Kein Vertrauen
4. Inflationssicherheit
5. Synchronisation
6. Stabilität

# Kryptowährung

## Aufbau eines Ledgers

**Ledger** $\rightarrow$ *Ledger* (Englisch) – „Hauptbuch“

# Kryptowährung

## Aufbau eines Ledgers

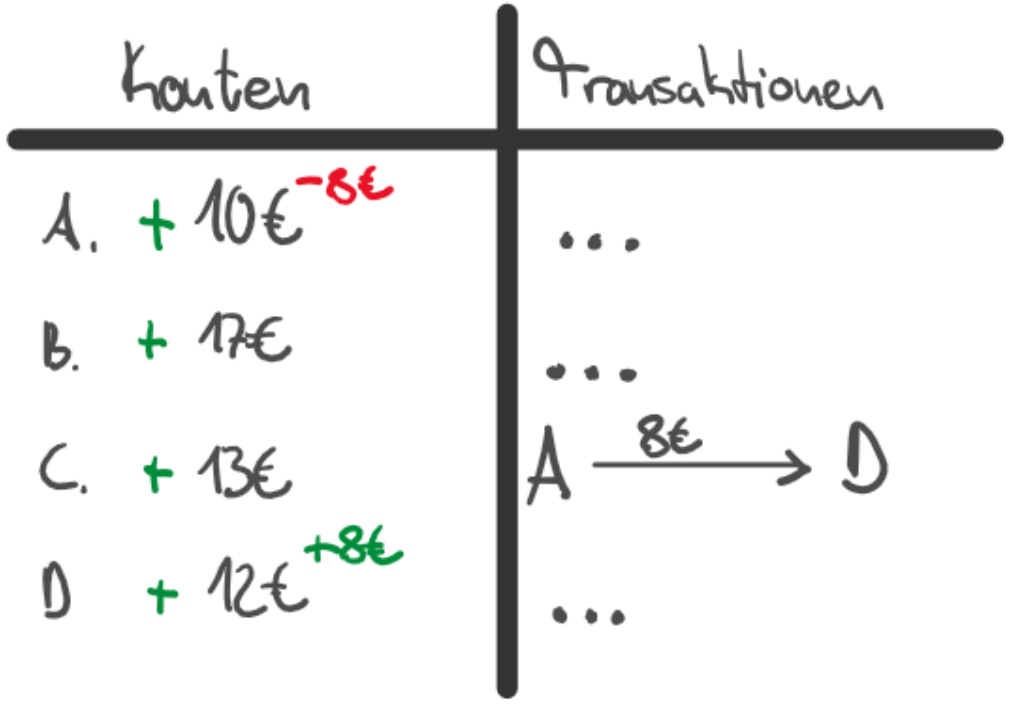


Abbildung: Zentrales Ledger

# Kryptowährung

## Verteilung des Ledgers

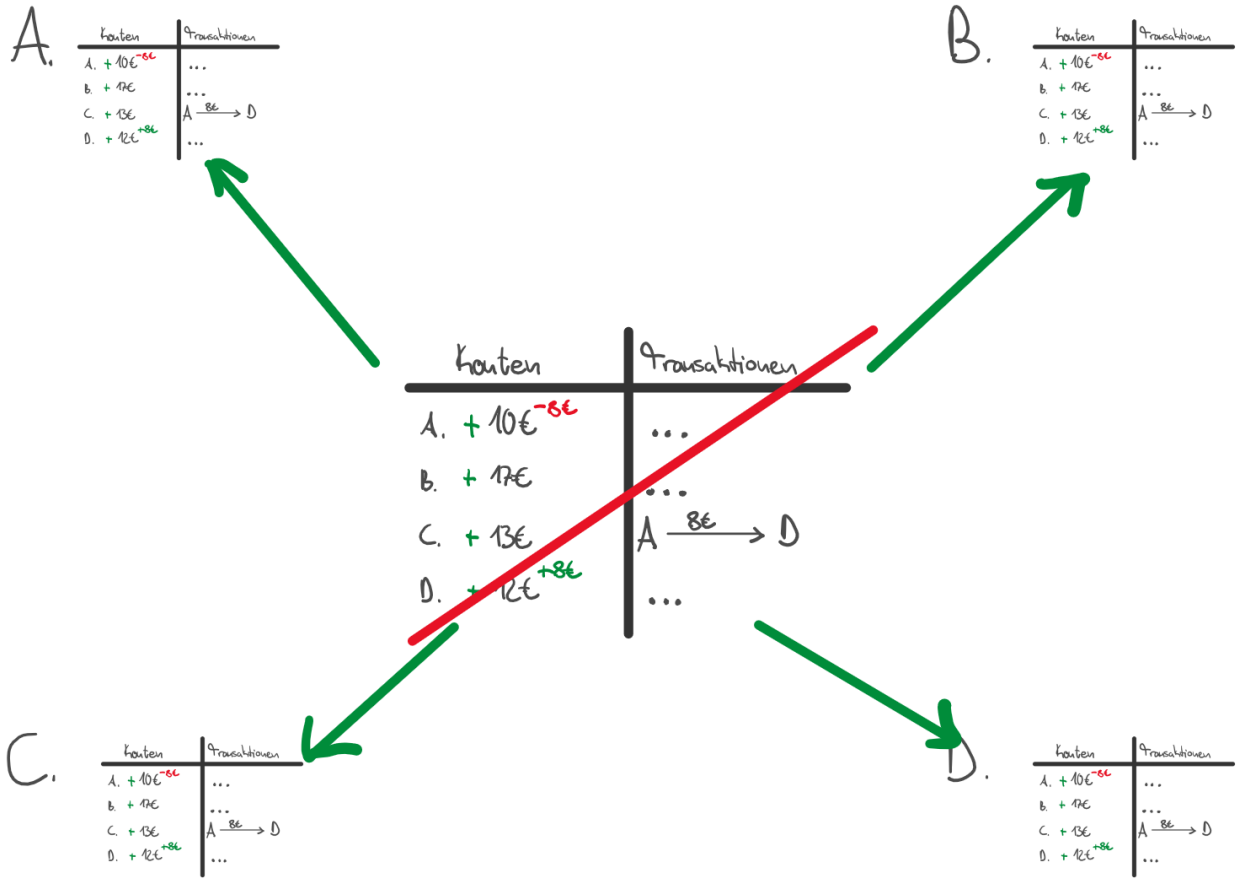


Abbildung: Verteiltes Ledger

# Kryptowährung

## Rückblick auf Ziele

1. ~~Dezentralisierung~~ → Verteilung des Ledgers
2. Verteilter Konsens
3. Kein Vertrauen
4. Inflationssicherheit
5. Synchronisation
6. Stabilität

# Kryptowährung

## Festlegen eines Schreibers

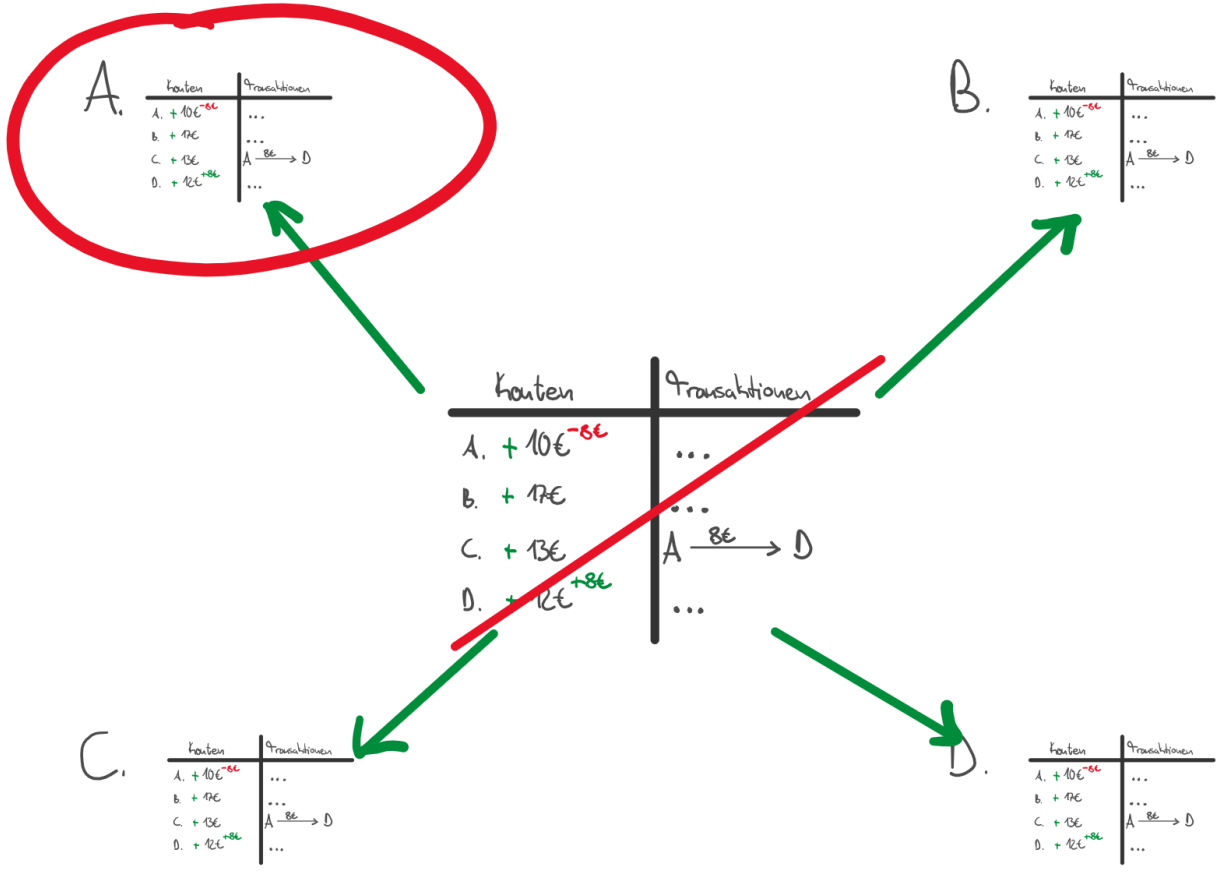


Abbildung: Vertrauenswürdiger Schreiber

# Kryptowährung

## Rückblick auf Ziele

1. ~~Dezentralisierung~~ → Verteilung des Ledgers
2. ~~Verteilter Konsens~~ → Vertrauenswürdiger Schreiber
3. Kein Vertrauen
4. Inflationssicherheit
5. Synchronisation
6. Stabilität

# Kryptowährung

## Einrichten einer Lotterie Teil I

- Zufälligkeit der Schreibberechtigung
- Kosten für Teilnahme
- Gewinnerbestimmung ohne zentrale Lotterieleitung

# Kryptowährung

## Einrichten einer Lotterie Teil II

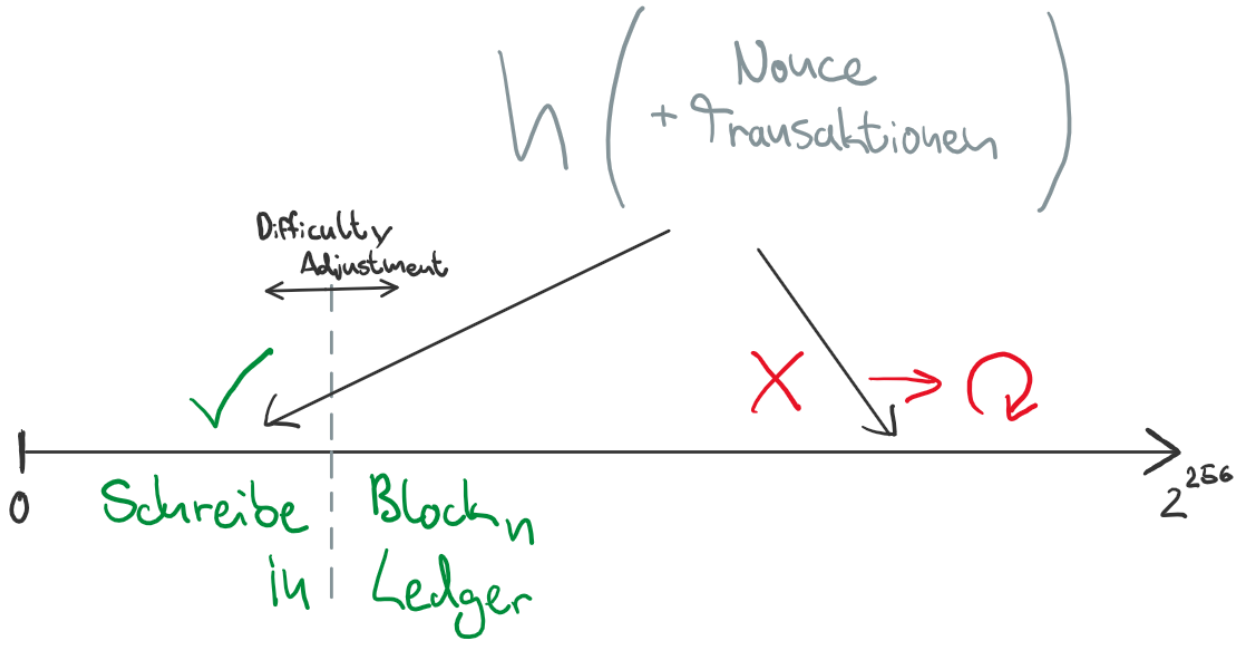


Abbildung: Einrichten einer Lotterie

# Kryptowährung

## Rückblick auf Ziele

1. ~~Dezentralisierung~~ → Verteilung des Ledgers
2. ~~Verteilter Konsens~~ → Vertrauenswürdiger Schreiber
3. ~~Kein Vertrauen~~ → Lotterie
4. Inflationssicherheit
5. Synchronisation
6. Stabilität

# Kryptowährung

## Währungsstabilität Teil I

- Coinbase-Transaktion für gültigen Proof of Work

# Kryptowährung

## Währungsstabilität Teil II

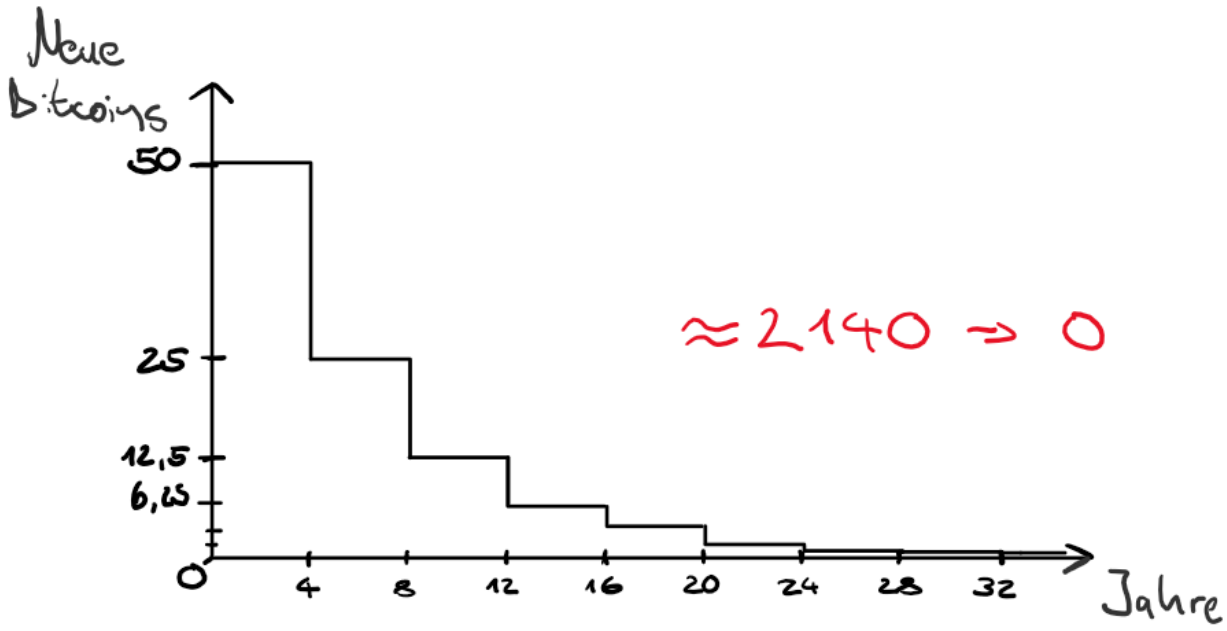


Abbildung: Verlauf der Coinbase Transaktionen

# Kryptowährung

## Rückblick auf Ziele

1. ~~Dezentralisierung~~ → Verteilung des Ledgers
2. ~~Verteilter Konsens~~ → Vertrauenswürdiger Schreiber
3. ~~Kein Vertrauen~~ → Lotterie
4. ~~Inflationssicherheit~~ → Coinbase, Halving und Tx-Gebühr
5. Synchronisation
6. Stabilität

# Kryptowährung

## Sicherung und Synchronisation

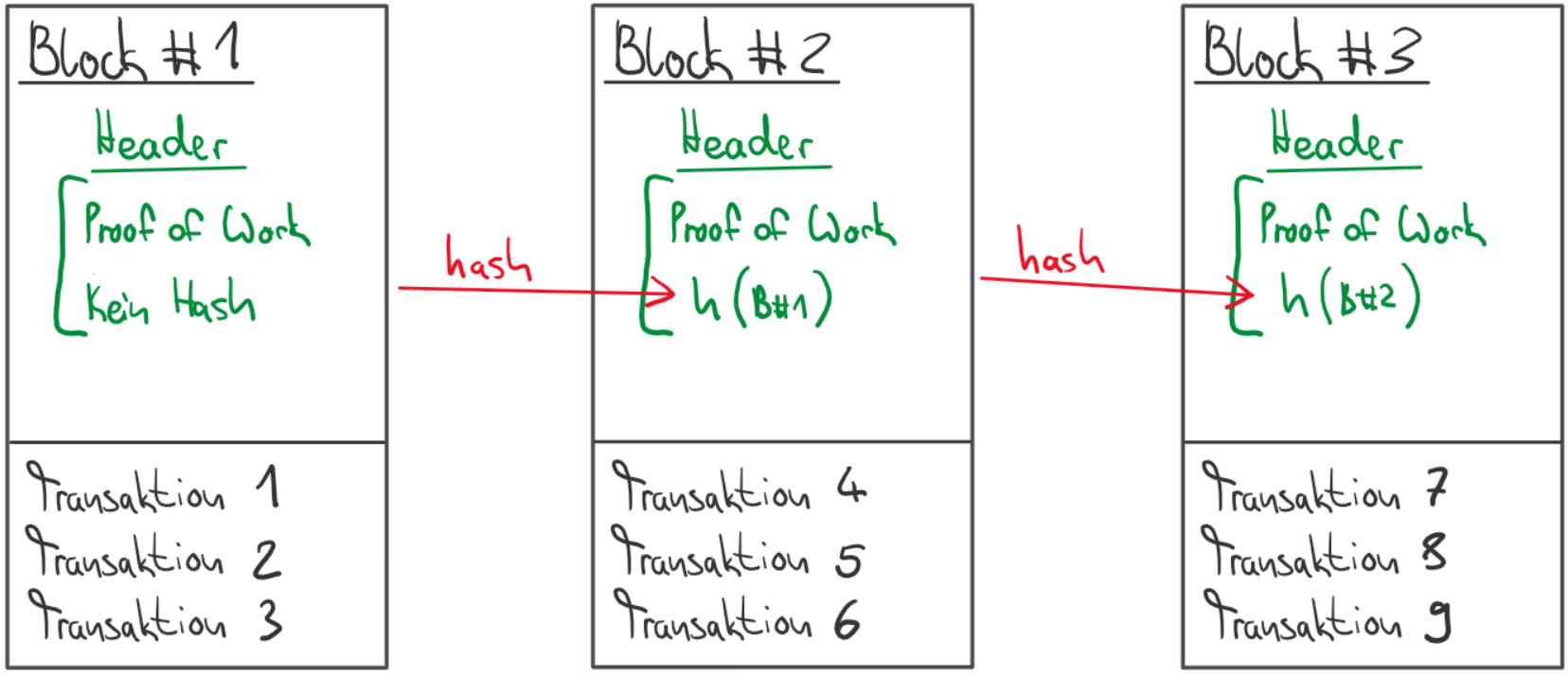


Abbildung: Blockchain

# Kryptowährung

## Anpassung der Lotterie

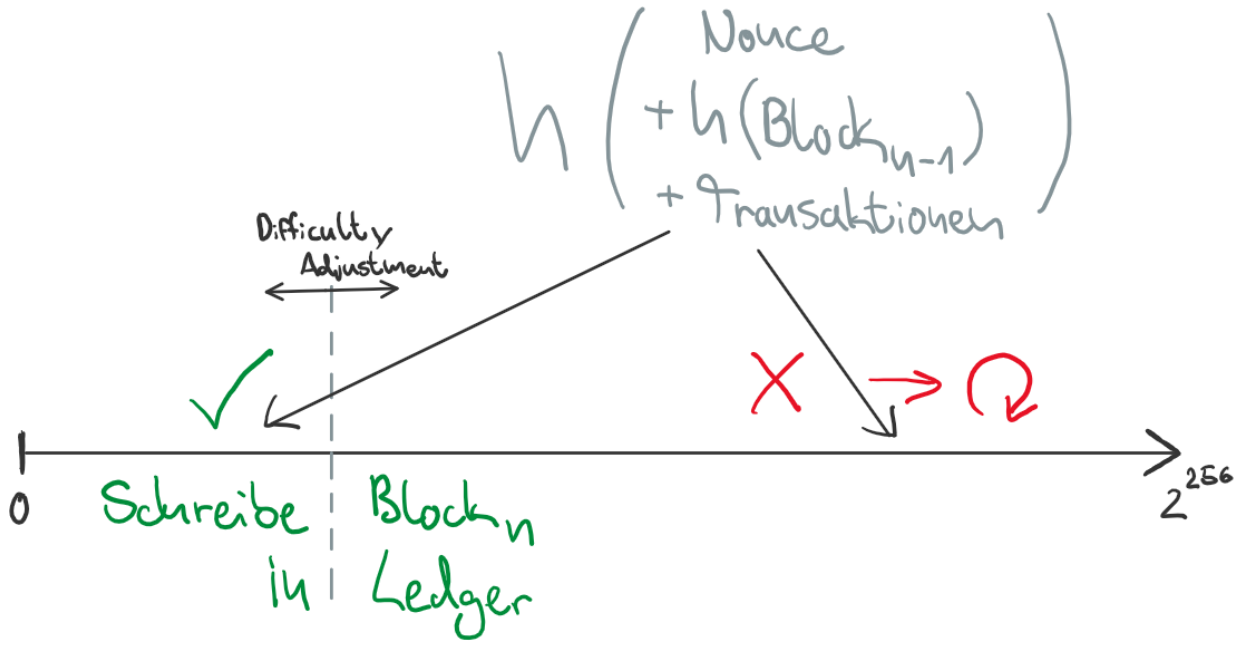


Abbildung: Einbinden der Blockchain in Lotterie

# Kryptowährung

## Blick auf Ziele

1. ~~Dezentralisierung~~ → Verteilung des Ledgers
2. ~~Verteilter Konsens~~ → Vertrauenswürdiger Schreiber
3. ~~Kein Vertrauen~~ → Lotterie
4. ~~Inflationssicherheit~~ → TX-Gebühr, Coinbase und Halving
5. ~~Synchronisation~~ → Blockchain
6. Stabilität

# Kryptowährung

## Blockkollisionen

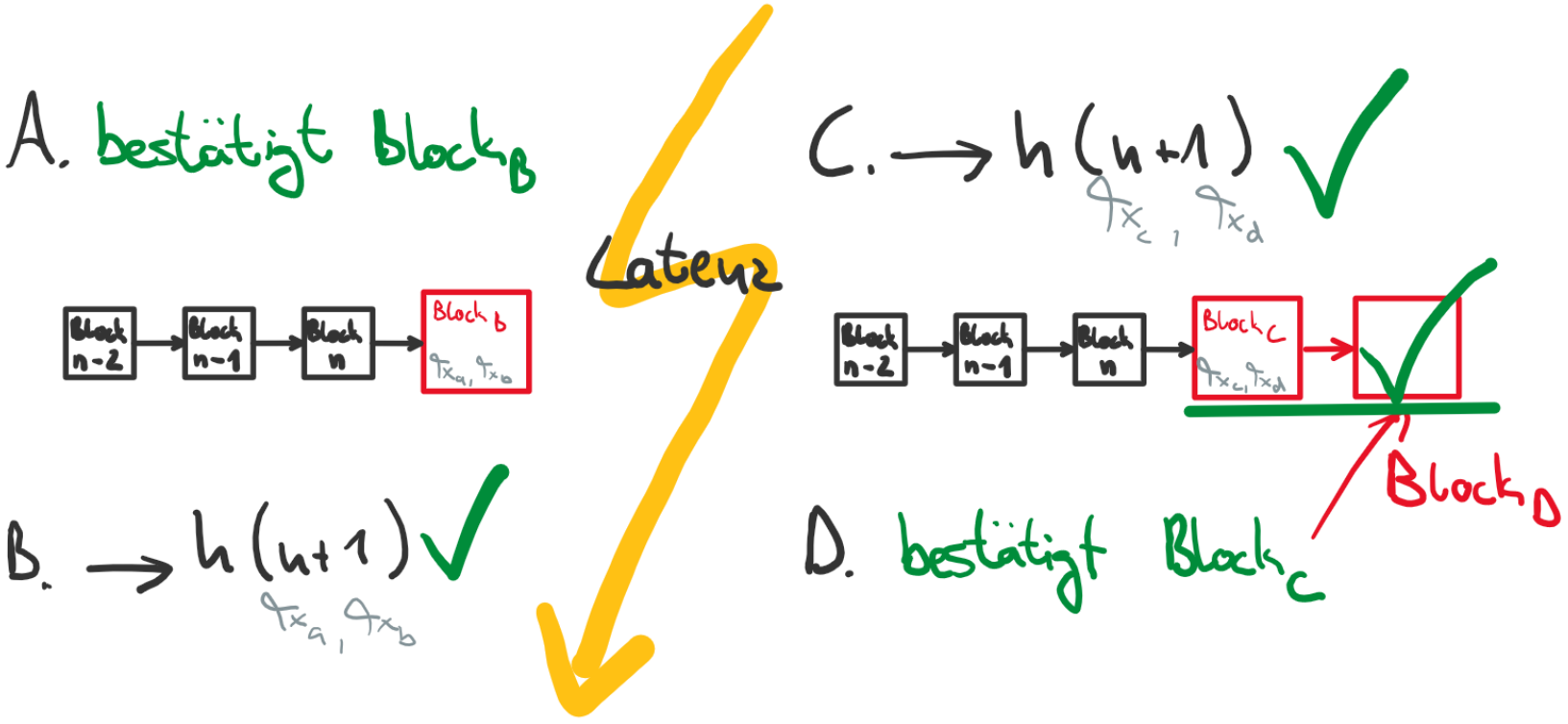


Abbildung: Nagamoto Konsens

# Kryptowährung

## Transaktionspool

Was passiert mit den verworfenen Transaktionen?

- Broadcasting der Transaktionen
- Ungeschriebene Transaktionen werden in Transaktionspool gehalten
- Verworfene Transaktionen werden in Transaktionspool zurückgeschrieben

# Kryptowährung

## Rückblick auf Ziele

1. ~~Dezentralisierung~~ → Verteilung des Ledgers
2. ~~Verteilter Konsens~~ → Vertrauenswürdiger Schreiber
3. ~~Kein Vertrauen~~ → Lotterie
4. ~~Inflationssicherheit~~ → Coinbase, Halving und Tx-Gebühr
5. ~~Synchronisation~~ → Blockchain
6. ~~Stabilität~~ → Nagamoto Konsens und Tx-Pool

# Zwischenstand

# Anwendung

## Gründe zur Nutzung

- Unabhängigkeit von zentralen Instanzen
- Kryptografisch abgesichert
- Privatsphäre
- Wertstabilität

# Anwendung

## Wallets Teil I

**Anlegen eines Kontos** Primäres Ziel: Entfernen der Identifizierbarkeit aus Finanzen Problem: Registrierung eines Kontos ohne zentrale Bank

# Anwendung

## Wallets Teil II

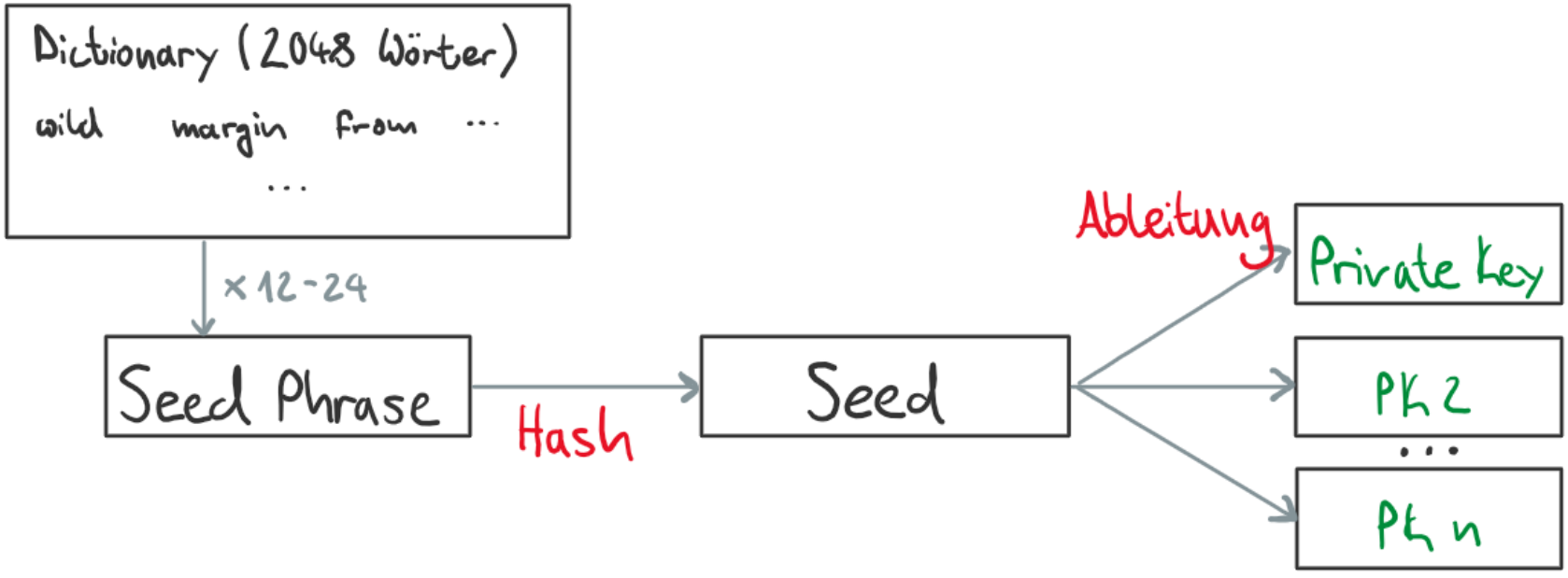


Abbildung: Erstellung eines Key-Pairs

# Anwendung

## Wallets Teil III

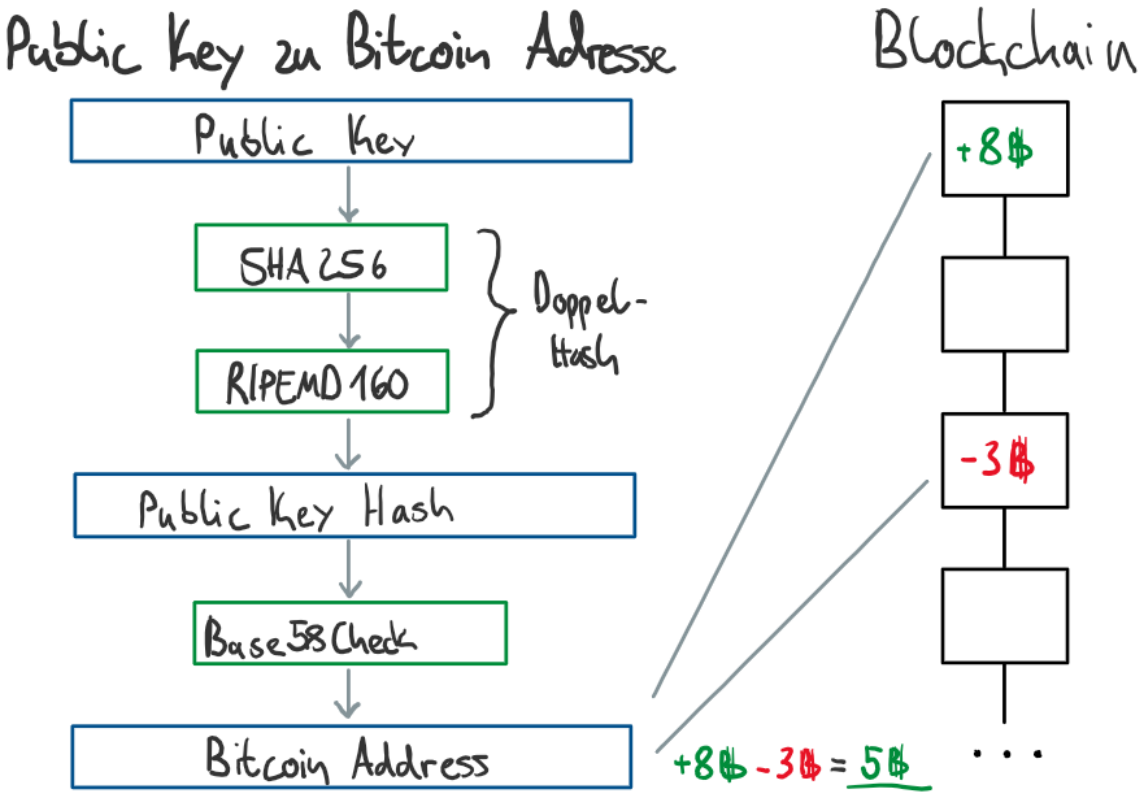


Abbildung: Erstellung einer Adresse

# Anwendung

## Transaktionen

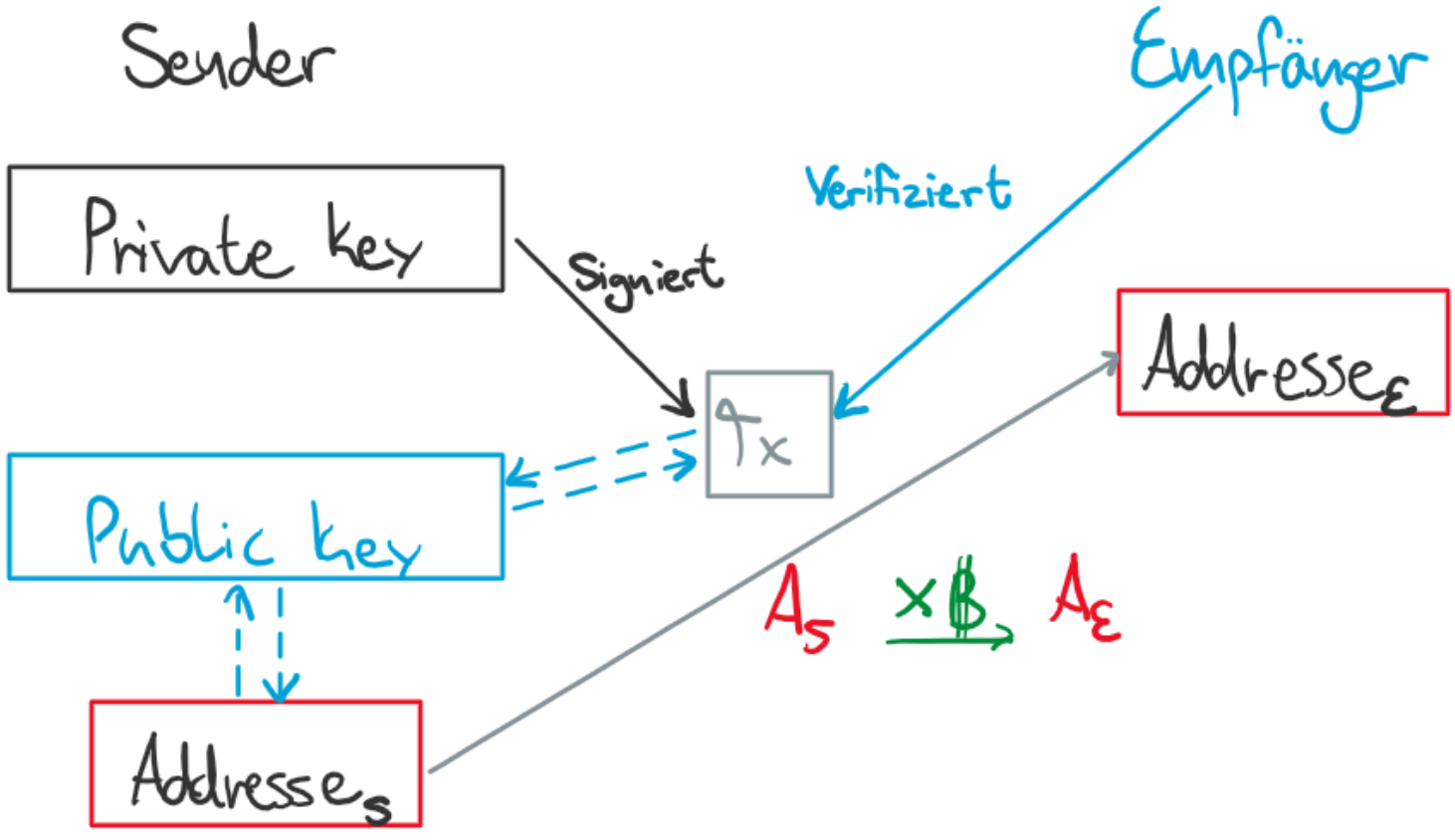


Abbildung: Transaktionsablauf

# Anwendung

## Wallets Teil IV

- Wie sehen konkrete Implementierungen von Wallets aus?

| **Hot Wallets** | | **Cold Wallets** | |
|---|---|---|---|
| Web-Anwendung<br>Mobile-Anwendung<br>Desktop-Anwendung | | Hardware<br>Digital<br>Papier | |
| + | einfach<br>kostenfrei | + | sehr sicher |
| − | unsicher | − | teuer<br>schwerer Einstieg |

# Anwendung

## Konkrete Kryptowährungen

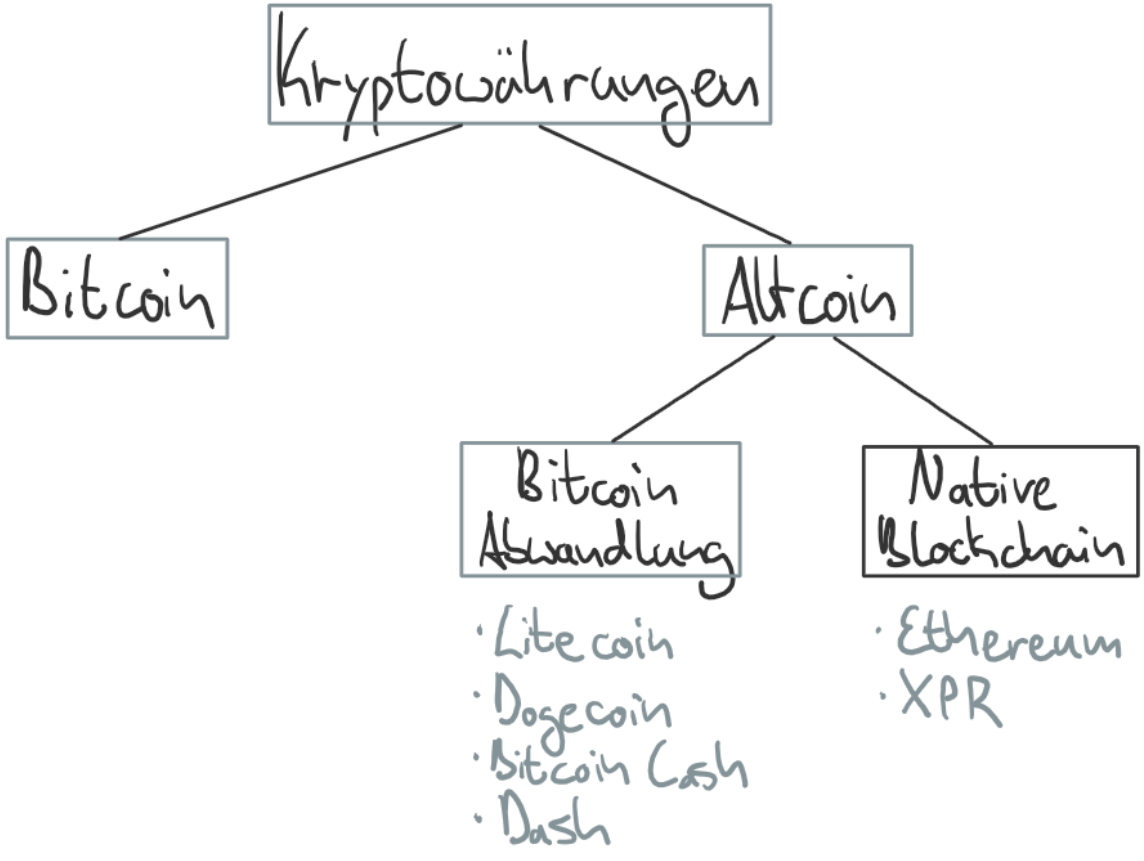


Abbildung: Kryptowährungen

# Zwischenstand

# Fazit

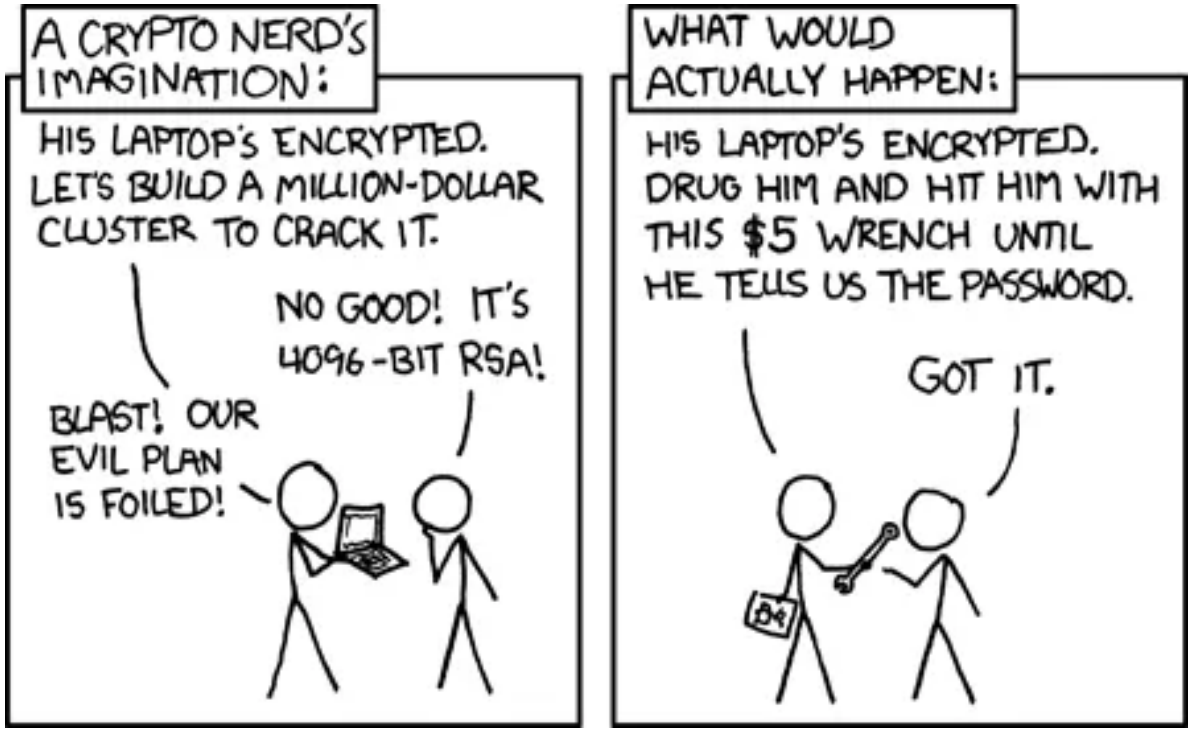


Abbildung: 5 Dollar Schraubschlüssel Angriff [3]

# Quellen I


[1] Prof. Dr. Oliver Bendel. Definition: Was ist Kryptowährung. [Online; aufgerufen 15.10.2021]. 2021. URL: https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160/version-384589.

[2] bitcoin.org. Wie funktioniert Bitcoin? [Online; aufgerufen 26.11.2021]. URL: https://bitcoin.org/de/wie-es-funktioniert.

[3] coindiligent.com. Five Dollar Wrench Attack. [Online; aufgerufen 25.11.2021]. 2021. URL: https://nitrocdn.com/RRxvRrLqWvYnbMLxaKtfoREJNlVTTpII/assets/static/optimized/rev-15a4122/wp-content/uploads/2018/12/xkcd-security.png.

[4] Bitcoin cummunity. Bitcoin Wiki. [Online; zuletzt aufgerufen 30.11.2021]. URL: https://en.bitcoin.it/wiki.

# Quellen II

[5] Satoshi Nakamoto.
Bitcoin open source implementation of P2P currency.
[Online; aufgerufen 09.11.2021]. 2009. URL: https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

[6] Satoshi Nakamoto.
Bitcoin: A Peer-to-Peer Electronic Cash System. [Online; aufgerufen 12.10.2021]. 2009. URL: https://bitcoin.org/bitcoin.pdf.

[7] Yan Pritzker. Bitcoin entdecken. Aprycot Media - Held & Troendle GbR, 2020.

# Quellen III

[8] Maarten Zuidhoorn.
The Journey from Mnemonic Phrase to Address. [Online; aufgerufen 25.11.2021]. 2020. URL: https://medium.com/mycrypto/the-journey-from-mnemonic-phrase-to-address-6c5e86e11e14.