Löst das Chainweb das Blockchaintrilemma?

Name

25. Oktober 2022

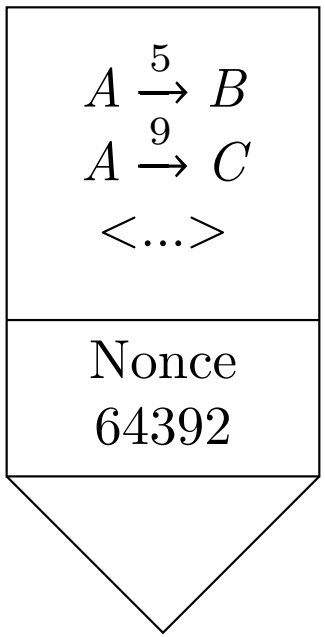
Inhaltsverzeichnis

Grundlagen

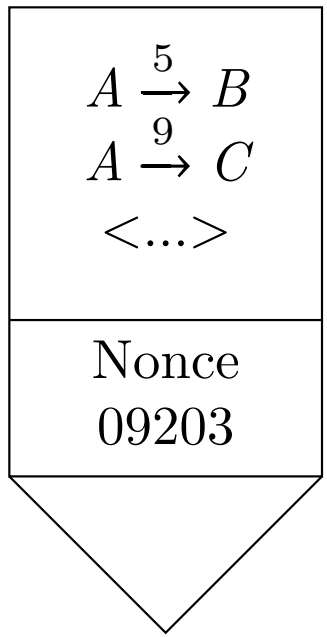
- Hashfunktion: $h : \{0,1\}^* \rightarrow \{0,1\}^l$
  - h für Computer einfach zu berechnen
  - Es gilt für alle x und x': $h(x) \neq h(x')$
- Bestätigung von Transaktionen durch Rechenleistung: Proof of Work
- Limitierter Durchfluss (TPS) von etwa 5 Transaktionen pro Sekunde

Proof of Work

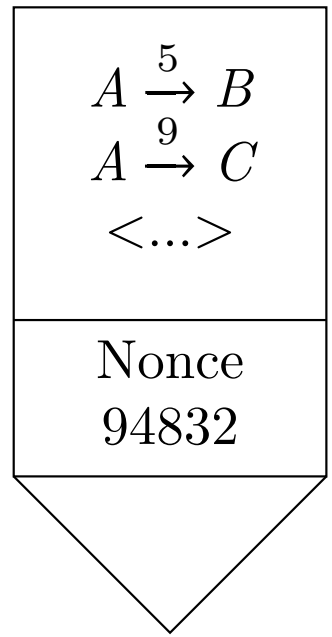
- Berechnen des Hashwertes mit verschiendenen Werten für die Nonce



383625362367312 4



0303948571920435



0000000023673124

Proof of Work

- Einreihen gefundener Blöcke in die Blockchain

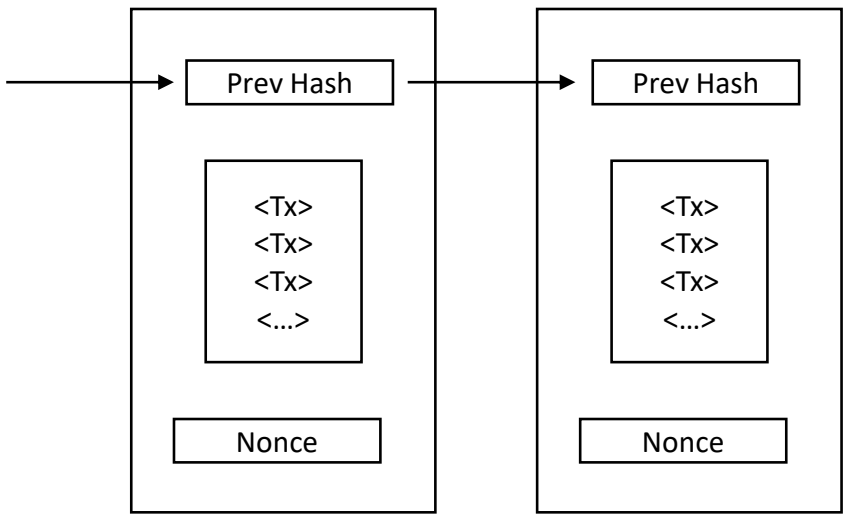


Abbildung: Vereinfachte Darstellung einer Blockchain. [1]

Blockchaintrilemma

Vereinen dreier wünschenswerter Faktoren einer Blockchain:

- Dezentral
- Skalierbarkeit
- Sicher

Funktionsweise des Chainwebs

- Proof of Work
- Mehrere parallele, unabhängige Ketten
- Jede Kette referenziert neben Vorgängerblock auch auf andere Ketten

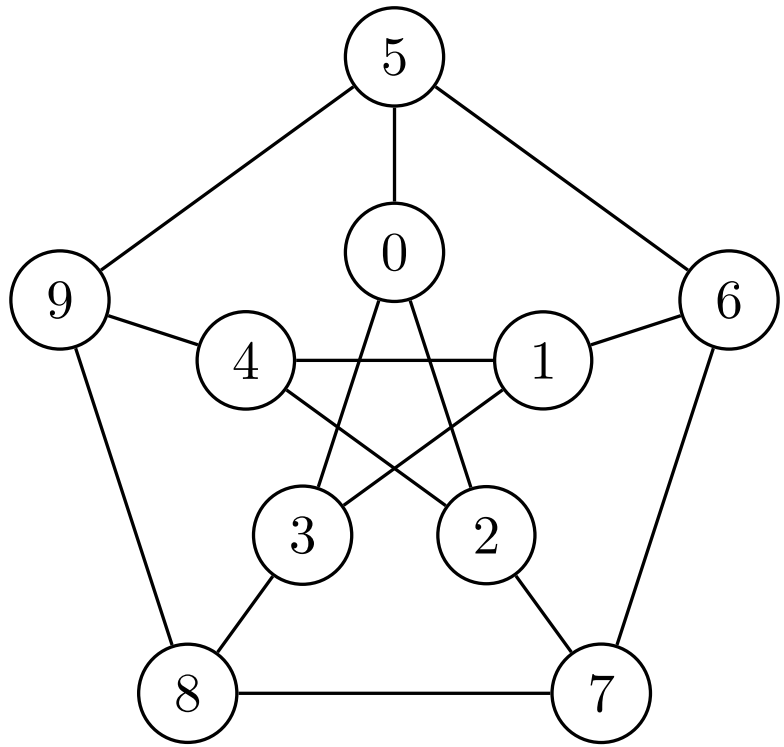


Abbildung: Petersen-Graph der Ordnung 10, Grad 3 und Durchmesser 2. [2]

Durchfluss des Chainwebs

- Durchfluss von einer Kette $TPS_1 = 8$ experimentell bestimmt
- Gesammtdurchfluss mit C Ketten: $TPS_C = C \cdot 8$

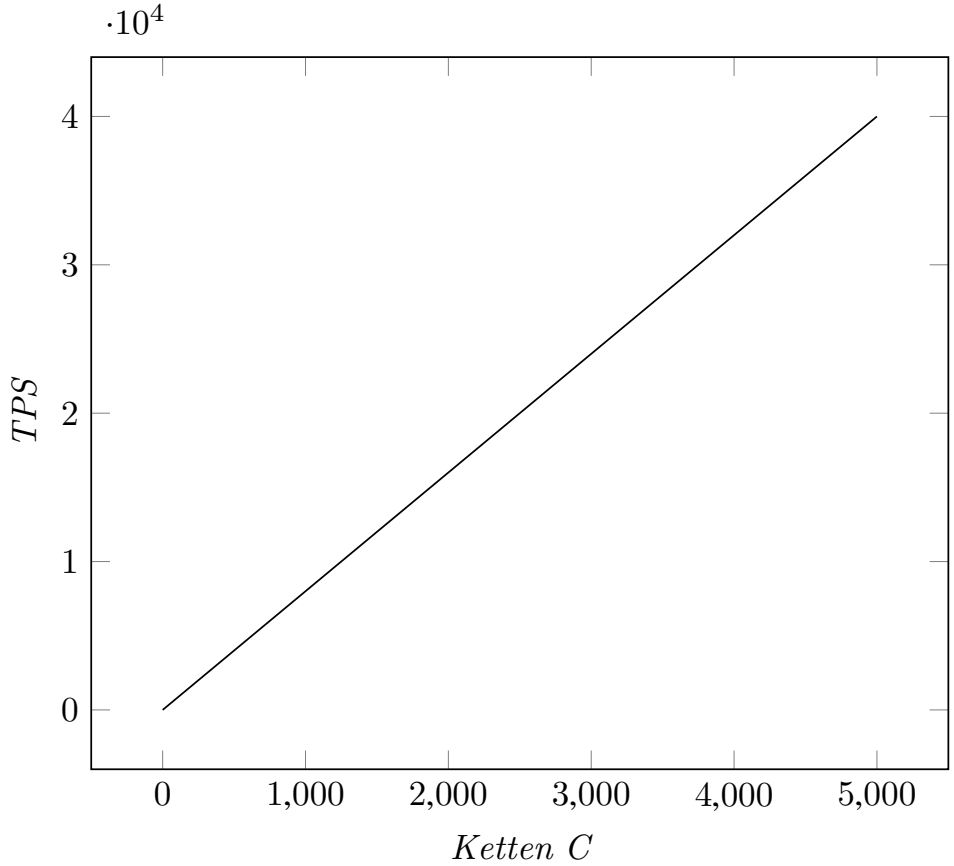


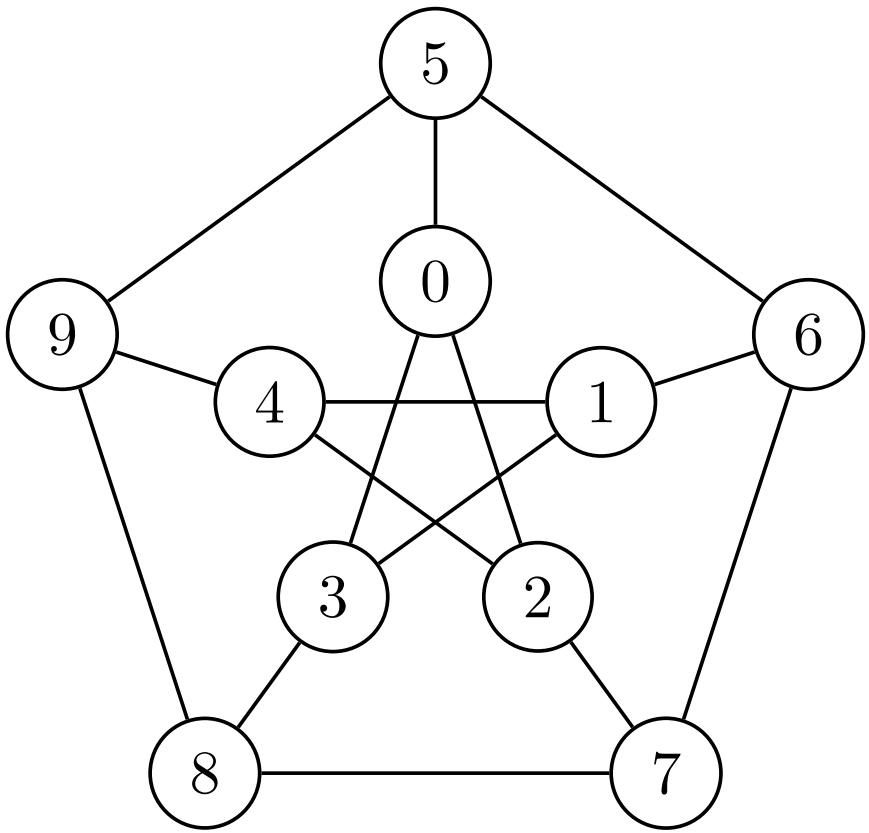
Abbildung: Darstellung des Durchflusses in Abhängigkeit der Ketten.

Zusammenfassung

- Skalierbar ✓
- Theoretisch dezentral ✓
- Sicher ✓

Petersen-Graph

```
\usetikzlibrary{
  graphs,graphs.standard
}
\tikzgraphsset{
  edges={draw,semithick},
  nodes={circle,draw,semithick}
}
\centering
\tikz
\graph[math nodes, clockwise]
{ subgraph I_n [V={0,1,2,3,4}]
    --
  subgraph C_n [V={5,6,7,8,9},
  radius=1.25cm];
{[cycle] 0,2,4,1,3} };
```



Kreisdiagramm

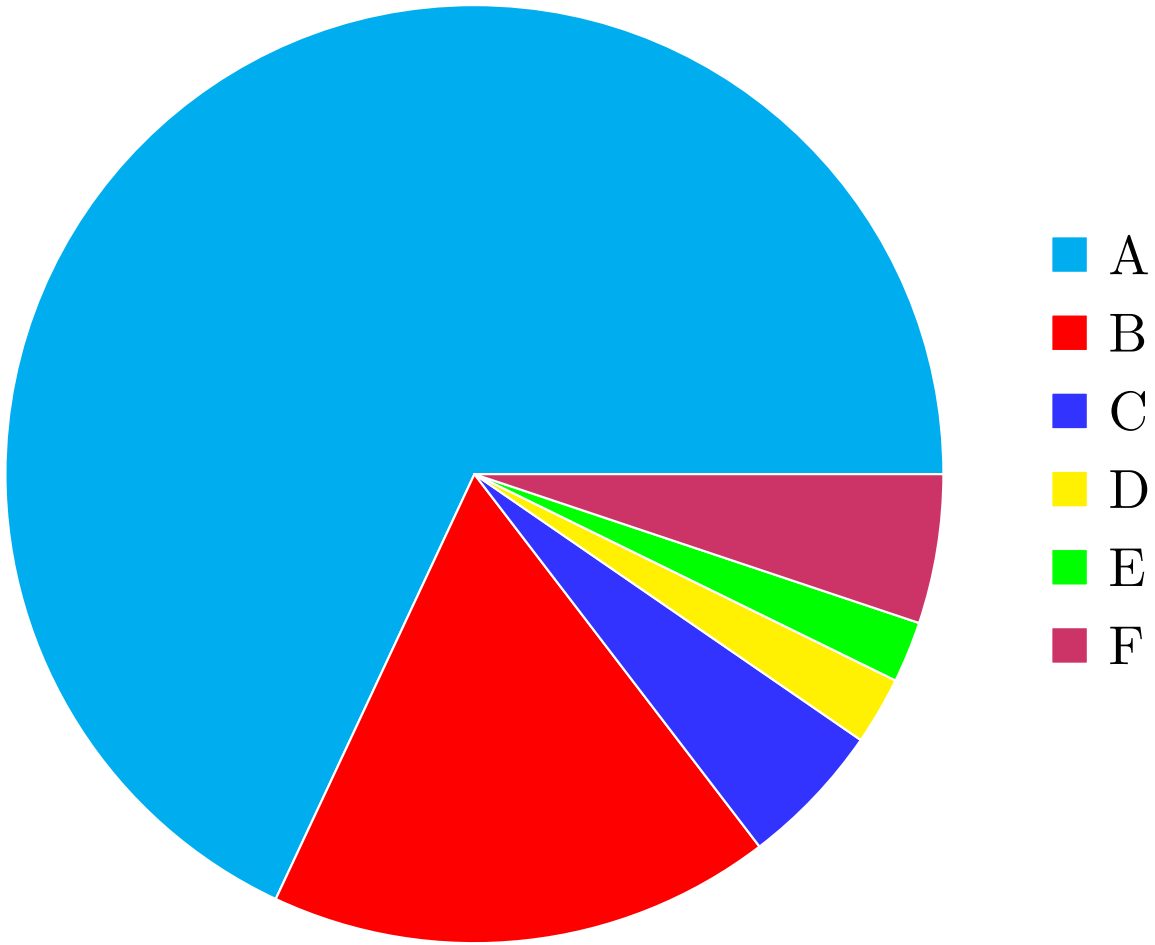


Abbildung: Kreisdiagramm in LaTeX.

Kreisdiagram

- Modifizieren des Pakets *pgf – pie* durch *etoolbox*

```
% Präambel
\usepackage{pgf-pie}
\usepackage{etoolbox}
\newtoggle{showpct}
\makeatletter
\patchcmd{\pgfpie@slice}%
{\pgfpie@scalefont{#3}\pgfpie@numbertext{#3}}%
{\iftoggle{showpct}{\pgfpie@scalefont{#3}
\pgfpie@numbertext{#3}}{}}%
{}{}
\makeatother
```

Schlussbemerkung

- Zu jedem Problem gab es irgendwo eine passende Lösung

Schlussbemerkung

- Zu jedem Problem gab es irgendwo eine passende Lösung
- Effiziente Nummerierung von Bildern, Formeln und Abschnitten

Schlussbemerkung

- Zu jedem Problem gab es irgendwo eine passende Lösung
- Effiziente Nummerierung von Bildern, Formeln und Abschnitten
- LaTeX hat mich überzeugt

Literatur I

[1] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Techn. Ber. 2009.
URL: https://bitcoin.org/bitcoin.pdf (besucht am 10. 06. 2022).

[2] William Martino, Monica Quaintance und Stuart Popejoy. *Chainweb: A Proof-of-Work Parallel-Chain Architecture for Massive Throughput.* Techn. Ber. 2018.
URL: https://d31d887a-c1e0-47c2-aa51-c69f9f998b07.filesusr.com/ugd/86a16f_029c9991469e4565a7c334dd716345f4.pdf (besucht am 10. 06. 2022).

[3] Joseph Abadi und Markus Brunnermeier. *Blockchain Economics.* National Bureau of Economic Research, 2018.

[4] William Martino und Monica Quaintance. *Chainweb Protocol Security Calculations.* Techn. Ber. 2018.
URL: https://d31d887a-c1e0-47c2-aa51-c69f9f998b07.filesusr.com/ugd/86a16f_26d87f20cf8548d2927e28152babf533.pdf (besucht am 10. 06. 2022).

Literatur II

[5] William Martino, Stuart Popejoy und Monica Quaintance. „Parallel-chain architecture for blockchain systems“. 10938567. 2019. URL: https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=10938567.PN.&OS=PN/10938567 (besucht am 10. 06. 2022).

[6] Eyal Loz und Pineda-Villavicencio Guillermo. „New Benchmarks for Large-Scale Networks with Given Maximum Degree and Diameter“. In: *The Computer Journal* 53.7 (2010), S. 1092–1105. DOI: 10.1093/comjnl/bxp091.

[7] Kadena LCC. *Kadena Block Explorer*. URL: https://explorer.chainweb.com/mainnet (besucht am 28. 05. 2022).

[8] Stuart Haber und W. Scott Stornetta. „How to time-stamp a digital document“. In: *Journal of Cryptology* 3.2 (1991), S. 99–111. ISSN: 0933-2790. DOI: 10.1007/bf00196791.

Literatur III

[9] Arthur Gervais u. a.
„On the security and performance of proof of work blockchains“.
In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016). DOI: 10.1145/2976749.2978341.

[10] Thomas Espitau, Pierre-Alain Fouque und Pierre Karpman.
Higher-Order Differential Meet-in-The-Middle Preimage Attacks on SHA-1 and BLAKE. Techn. Ber. 2015.
URL: https://eprint.iacr.org/2015/515.

[11] Shubin Cai u. a.
„A TPS model of block-generating method based on POW“. In: *2019 IEEE International Conference on Smart Cloud (SmartCloud)* (2019).
DOI: 10.1109/smartcloud.2019.00024.

Literatur IV

[12] Bundesamt für Sicherheit in der Informationstechnik. *Blockchain sicher gestalten: Konzepte, Anforderungen, Bewertungen.* 2019. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3 (besucht am 10. 06. 2022).

[13] Blake2. *BLAKE2 — fast secure hashing.* 2017. URL: https://www.blake2.net/ (besucht am 10. 06. 2022).

[14] Doug Beardsley. *How to Scale a Proof of Work Blockchains.* 2021. URL: https://medium.com/kadena-io/how-to-scale-a-proof-of-work-blockchain-9233e5b4b62 (besucht am 06. 06. 2022).

[15] Anedak. *Kadena Statistics.* URL: https://anedak.com/beta (besucht am 05. 06. 2022).

[16] Michael Nielsen. *How the Bitcoin protocol actually works.* 2013. URL: https://michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/ (besucht am 10. 06. 2022).

Literatur V

[17] Xinle Yang, Yang Chen und Xiaohu Chen.
„Effective scheme against 51% attack on proof-of-work blockchain with history weighted information“. In: *2019 IEEE International Conference on Blockchain (Blockchain)* (2019).
DOI: 10.1109/blockchain.2019.00041.