Karlsruher Institut für Technologie

SS 2020 Proseminar: Bitcoin & Blockchain
Segregated Witness

Stefan Krieg

FORSCHUNGSGRUPPE DEZENTRALE SYSTEME UND NETZDIENSTE (DSN)
INSTITUT FÜR TELEMATIK, FAKULTÄT FÜR INFORMATIK

Bildquelle: https://en.bitcoin.it/w/images/en/4/49/Segwit.png

Gliederung

- Motivation
- Ziel der Arbeit
- Grundlagen
  - Transaktion
  - Merkle Tree
- Probleme
  - Transaction Malleability
  - Scaling Problem
- Lösung durch SegWit
  - Konzept
  - Umsetzung
  - Weitere Feature
- Evaluierung
- Fazit

Motivation

- SegWit eines der größten Bitcoin-Protokoll Updates
- Löst große Probleme
- Legt Grundstein für zukünftige Updates

Forschungsgruppe DSN
Institut für Telematik, Fakultät für Informatik

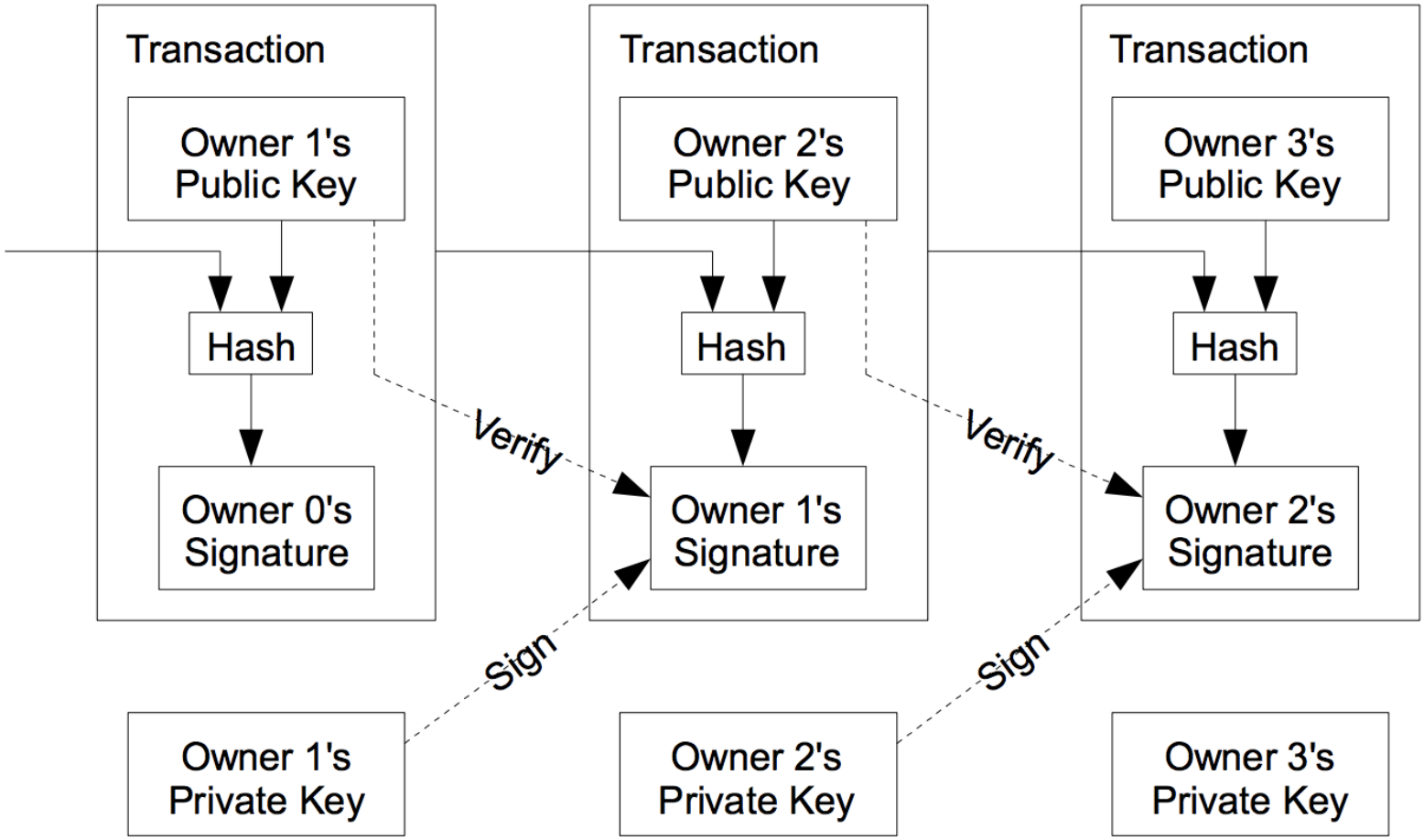
Ziel der Arbeit

- Probleme von Bitcoin erläutern
- Erklärung der Funktionsweise von SegWit
- Ob und wie damit Probleme gelöst werden können
- Erfolg in der Praxis

GRUNDLAGEN

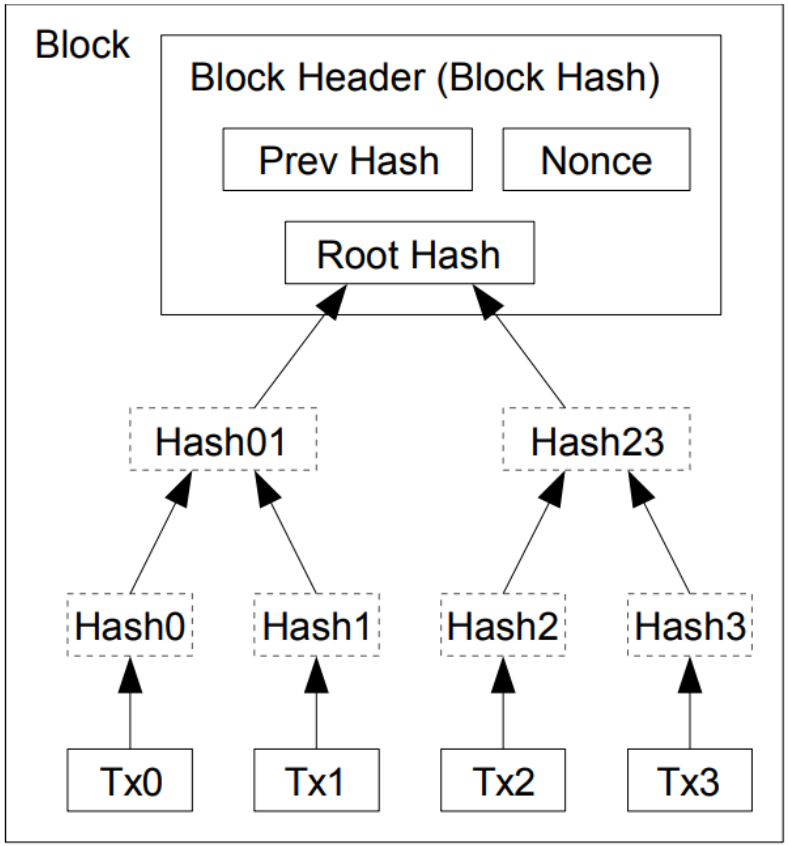
Forschungsgruppe DSN
Institut für Telematik, Fakultät für Informatik

Transaktionen

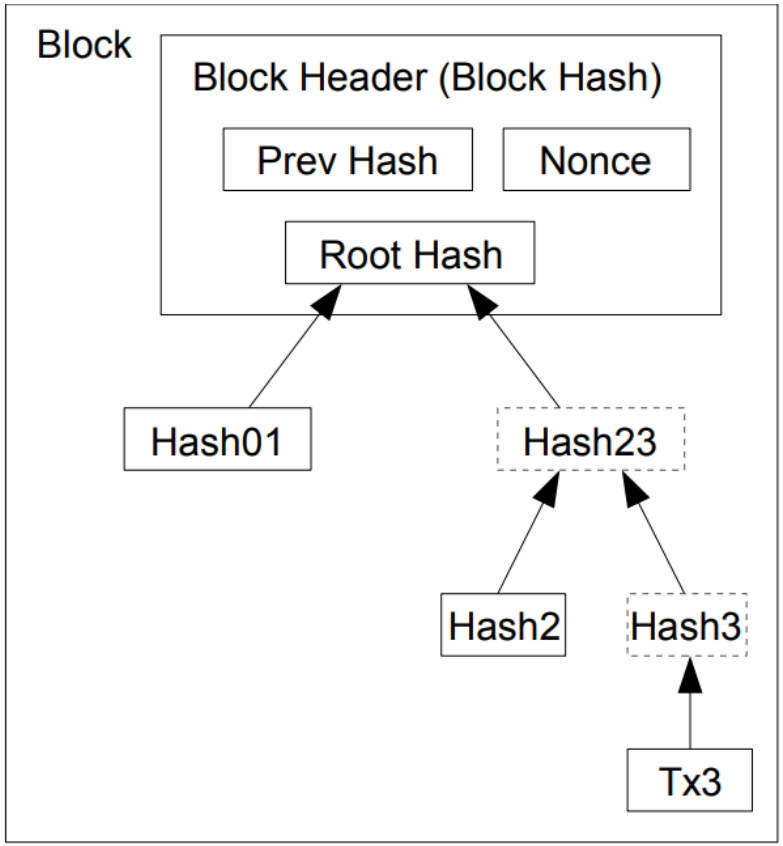


Bildquelle: https://i.stack.imgur.com/YXguz.png

Merkle Tree



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Bildquelle: https://bitcoin.org/bitcoin.pdf

PROBLEME

Forschungsgruppe DSN
Institut für Telematik, Fakultät für Informatik

Transaction Malleability

- Beispiel:
  1. Transaktion A wird gesendet
  2. Gleiche Transaktion A‘ mit anderer ID wird gesendet
  3. A‘ zuerst in Block aufgenommen → A abgelehnt
  4. Transaktion B mit gleichem Wert wird gesendet

- Angriff ermöglicht Double-Spend

Skalierbarkeit

- Blockgröße begrenzt auf 1 MB

- Ein Block alle ca. 10 Minuten

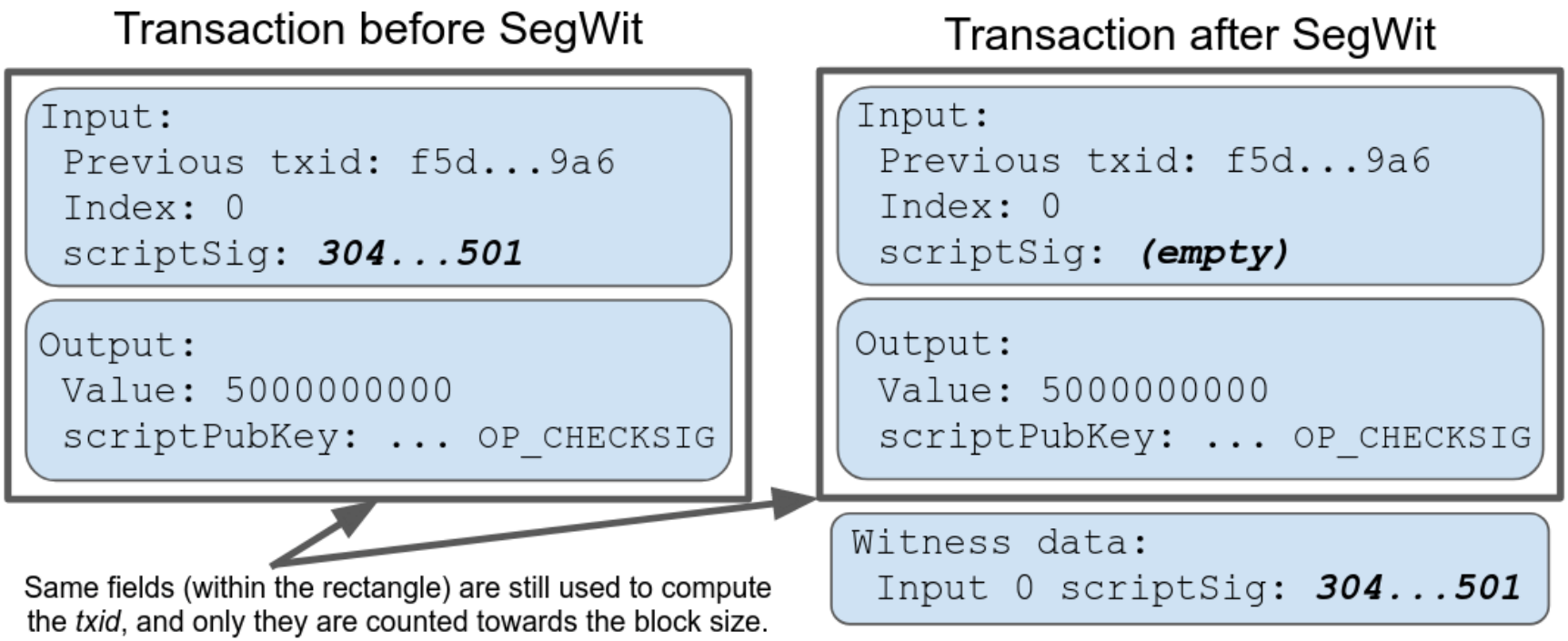
→ Durchschnittlich ca. 7 Transaktionen pro Sekunde
→ Maximal ca. 27 Transaktionen pro Sekunde möglich
(Vergleich: Visa 1700/s)

- Zu Bemerken: Großer Teil jeder Transaktion ist die Signatur

LÖSUNG

Konzept zur Behebung

- Neue Struktur namens „Witness“

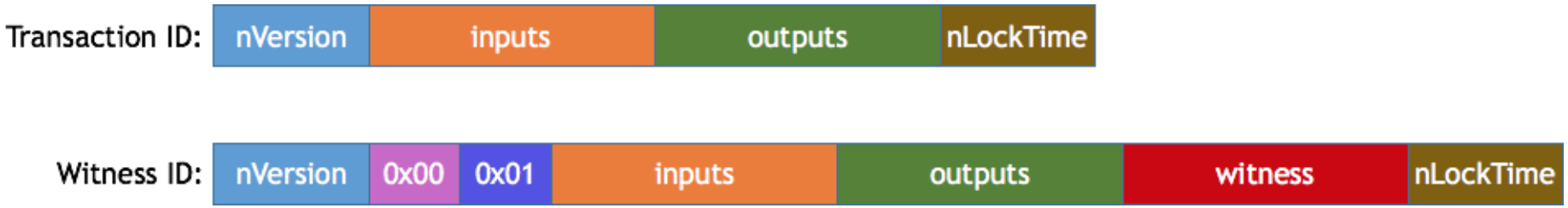


Bildquelle: https://www.buybitcoinworldwide.com/pages/info/img/segwit-v-legacy.png

Umsetzung

- 2 IDs statt einer
- Berechnung TXID über serialisierte Transaktion
  - Signatur-Daten dabei leer
- Berechnung WTXID über serialisierte Witness-Daten
  - Enthält Signatur-Daten

→ TXID nicht mehr veränderbar



Bildquelle: https://raw.githubusercontent.com/bitcoin/bips/master/bip-0144/witnesstx.png

Block-Gewicht

- Basis Größe:
  - Summe der Größe aller Transaktionen (ohne Witness) eines Blocks
- Gesamte Größe:
  - Summe der Größe aller Transaktionen (mit Witness) eines Blocks

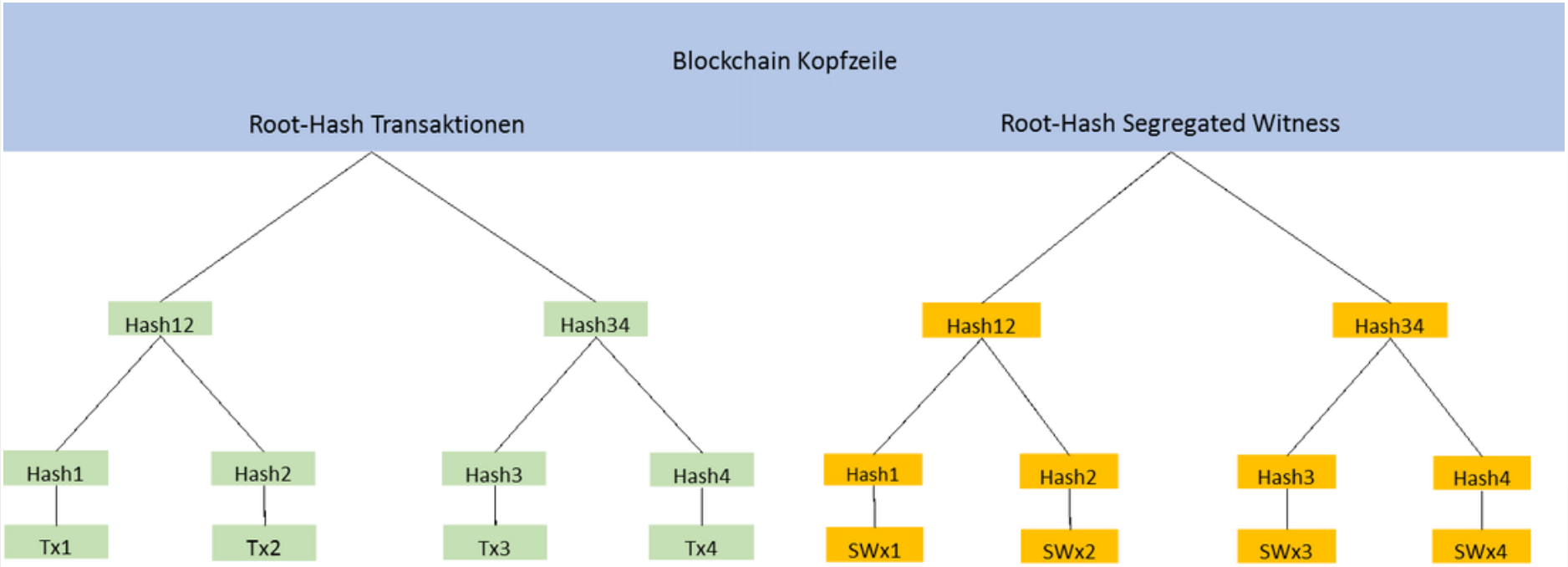
- Block-Gewicht: 3 * Basis Größe + Gesamt Größe

- Neue Regel: Block-Gewicht ≤ 4,000,000 Byte

- Maximale Blockgröße auf fast 4 MB erhöht

Witness Merkle Tree

- Eigener Merkle Tree für Witness-Block
- Witness Root Hash in coinbase Transaktion



Bildquelle: https://blockchain-nachrichten.com/uploads/8/2/2/6/82265992/segwit-merkle-tree_orig.png

Soft Fork

- Protokoll-Update rückwärts kompatibel
  - Alte Knoten erkennen neue Transaktionen als gültig
  - Alte Transaktionen müssen nicht unbedingt valide sein
  - Update empfehlenswert

→ Verhindert Spaltung des Netzwerks

- Alte Knoten können nicht:
  - SegWit Transaktionen validieren

- Wurde am 24. August 2017 aktiviert
  - Am 8. August schon Zustimmung aller Miner

Evaluierung

- Einführung von SegWit sehr sinnvoll
  - Ermöglicht neue Technologien wie Lightning Network
  - Erhöht Blockgröße zu heute besser geeignetem Wert

- Heute von Transaktionen ca. 50% SegWit
- Durchschnittliche Blockgröße von ca. 1.3 MB, Tendenz steigend

- Transaktionen pro Sekunde nicht deutlich gestiegen
  - Andere Lösung benötigt

Fazit

- Neue Witness Struktur
  - Signaturen ausgelagert
  - Eigene ID für jede Transaktion
  - Eigenen Merkle Tree zur Validierung
- Neue Regel zur Blockgrößenbeschränkung
- Scaling Problem nur teilweise gelöst
- Transaction Malleability nicht mehr möglich

→ Ermöglicht Lightning Network

Quellen

- Buch: Computer Security - ESORICS 2014 (Seiten 313-326)
- https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
- https://github.com/bitcoin/bips/blob/master/bip-0144.mediawiki
- https://www.mycryptopedia.com/what-is-segregated-witness/
- https://petertodd.org/2016/segwit-consensus-critical-code-review
- https://www.coindesk.com/one-year-later-whats-holding-back-segwit-adoption-on-bitcoin
- https://blockchair.com/bitcoin/charts/transactions-per-second?interval=3m
- https://nchain.com/app/uploads/2017/07/SegWit-and-the-illusion-of-scale.pdf
- https://eprint.iacr.org/2019/416
- https://tradeblock.com/blog/analysis-of-bitcoin-transaction-size-trends
- https://en.bitcoin.it/wiki/Softfork