HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Ethereum

Transaktionen

Jannes Neemann, Ture Claußen
26. Mai 2020

1 Gas

2 Signatur

3 Propagation

4 Ausblick

Definition

- konzeptioneller Lösungsansatz für das Halteproblem
- bemisst einen Ressourcenverbrauch des Weltcomputers
- Kosten einer Transaktion: $gasPrice \times gasLimit$ bzw. $gasPrice \times gasUsed$

Intrinsische Kosten g_0

$$g_0 \equiv \sum_{i \in T_i, T_d} \begin{cases} G_{txdatazero} \text{ if } i = 0 \\ G_{txdatanonzero} \text{ otherwise} \end{cases} + \begin{cases} G_{txcreate} \text{ if } T_t = \emptyset \\ 0 \text{ otherwise} \end{cases} + G_{transaction}$$

Intrinsische Kosten von T_x

- T_x mit $G_{\text{txdatazero}} \times 4$ und $G_{\text{txdatanonzero}} \times 68 \rightarrow$ intrinsische Kosten : 3524 *gas* + 21000 *gas*
- Abschätzung: Wie viel Rechenleistung wird zusätzlich gebraucht?

gasPrice von T_x

- Am 20.04.2020 aktzeptieren ungefähr 84% der letzten 200 Blöcke den Preis von 9GWei

Preis und Latenz

- Korrelation zwischen gasPrice und Latenz?
- Eskalation von Transaktionskosten?

Durchsatzfähigkeit

$$T_{max} = \frac{\mathit{blockGasLimit}}{\mathit{transactionMedianGas}} = \frac{9817880}{80000} = 122.72$$

blockGasLimit

um maximal $\frac{P(H)_{H1}}{1024}$ des alten Limits $P(H)_{H1}$ erhöht oder verringert werden darf

Entwicklung gasPrice

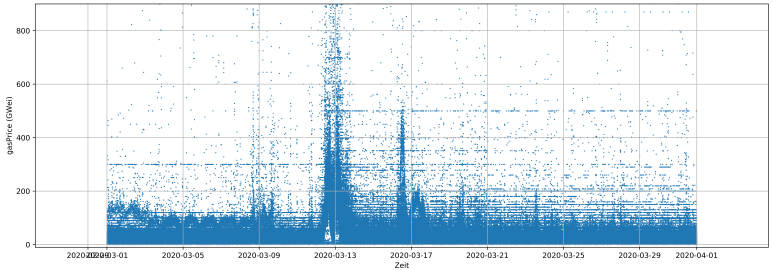

Abbildung: gasPrice nach Tag im Monat März [2]

Preis und Latenz

- Hohe Auslastung in kleinem Zeitintevall problematisch
- ICOs und DOS Angriffe verringern Zuverlässigkeit

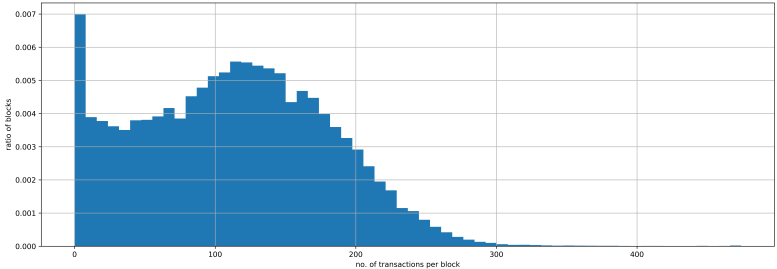

Abbildung: Verteilung der Zahl an Transaktionen pro Block (60 konstante Klassen) [2]

- Leere Blöcke lassen sich schneller Veröffentlichen
- Wirtschaftliche Interessen gehen vor

Anreiz und Spieletheorie

- Warum sollte ich Ressourcen für das System zur Verfügung stellen?
  $\rightarrow$Cryptoeconomics
- Formalisierung des menschlichen Verhaltens durch Spieletheorie
- *utility payoff* Nützlichkeitsfunktion $u(x, t)$ möglichst maximieren

1 Gas

2 Signatur

3 Propagation

4 Ausblick

Bedeutung

belegt den Besitz eines Schlüssels, der aktuell die *Authenzität* und die *Integrität* der Nachricht beweisen

Funktion

$$v, r, s = F_{sig}(F_{keccak256}(m), k)$$

- serialisierte Form aller Datenfelder + ChainID

Signatur der Transaktion T_x

v: 26

r:
dade772f31d20b4ed1c7f63ae035c0cc83fd7b786ca9339eb01763138877a6d4

s:
13e16f7a55d261e504e27ea4fecc174a1a46c87d804b9a3917aebde665c1ddb1

1 Gas

2 Signatur

3 Propagation

4 Ausblick

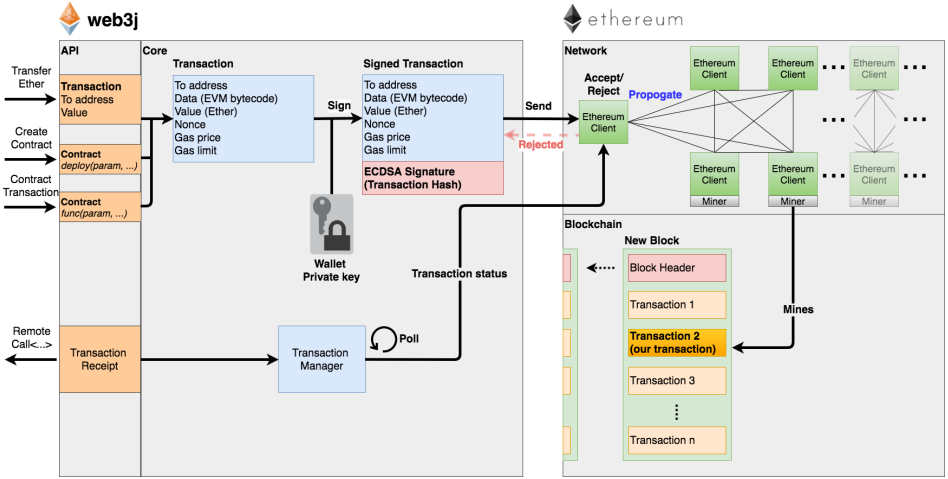

Abbildung: Propagation von Client [1]

Speicherung

- Inkludierung im Block
- Erstellung eines Receipts *receipt* besteht aus dem Zustand R_σ nach der Transaktion, dem kumulierten, verbrauchten Gas nach der Transaktion R_u und den Logs R_l
- *bloom filter* R_b von den Logs
- nach Konsens über Block unveränderlicher Teil der Blockchain

1 Gas

2 Signatur

3 Propagation

4 Ausblick

Ausblick

- homomorphische Verschlüsselung und Zero-knowledge-proofs
- $\rightarrow$ Ethereum 2.0

Web3j_transaction.png (PNG Image, 1747 × 955 pixels).
https://web3j.readthedocs.io/en/latest/_images/web3j_transaction.png

Neemann, J., Claussen, T.: Appendix: Scripts.
https://github.com/campfireman/SEM-ethereum-transactions