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

Ethereum Transaktionen

Jannes Neemann und Ture Claussen

Seminar-Arbeit im Studiengang „Angewandte Informatik"

1. April 2020

Autor 1: Jannes Neemann
1530893
jannes.neemnann@stud.hs-hannover.de
Verfasste Seiten/Abschnitte: ...

Autor 2: Ture ClauSSen
1531067
ture.claussen@stud.hs-hannover.de
Verfasste Seiten/Abschnitte: ...

Prüfer: M.Sc.Jussi Salzwedel
Abteilung Informatik, Fakultät IV
Hochschule Hannover
jussi.salzwedel@hs-hannover.de

Selbständigkeitserklärung

Mit der Abgabe der Ausarbeitung erklären wir, dass wir die eingereichte Seminar-Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die von uns angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Werken wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht haben.

Hannover, den 1. April 2020

Inhaltsverzeichnis

Zusammenfassung. Schlüsselwörter:

1 Einführung

2 Struktur und technische Umsetzung einer Transaktion

2.1 Komponenten von Transaktionen

2.2 Typen von Transaktionen

2.3 Serialisierung

3 Aufbau einer Transaktion

3.1 Nonce

3.2 Gas

Gas ist ein zentraler konzeptioneller Lösungsansatz im Rahmen von Ethereum. Da Ethereum turing-vollständig ist [3, S. 1], ergibt sich unter anderem das sogenannte "Halteproblem". Dieses besagt, dass im Voraus nicht vorhergesagt werden kann, ob das Programm einer Turing-Maschine jemals zu einem Ende kommt. [1, S.70] Um die Funktionalität des Netzwerks zu gewährleisten, wird die Laufzeit einer jeden Zustandsveränderung der Blockchain, sprich Transaktion, durch Gas begrenzt.

Gas ist eine eigenständige Währung innerhalb von Ethereum, dessen Einheit einen Rechenschritt in der EVM bemisst [2, S. 9:3], wobei für jeden Opcode die Kosten in Gas spezifiziert werden. [3, S. 25 ff.] Gas ist also eine Gebühr für Rechnenaufwand. Vor jeder Transaktion muss der externe Akteur festlegen, welchen Rechenaufwand er zu zahlen bereit ist.

Das Datenfeld *gasPrice* definiert bei Transaktionen welcher Preis pro Einheit Gas gezahlt werden soll. Dem entsprechend bezeichnet das Feld einen skalaren Wert in Wei. Gas kann bewusst nur mit Ether erworben werden, da die Gas-Preise möglichst unabhändig von den Preisschwankungen (von Ether) sein sollen. [3, S. 7]

Das *gasLimit* wiederrum gibt an, wie viel Gas für diese Transaktion maximal aufgewendet werden darf. Somit gilt es im Voraus abzuschätzen wie hoch der Rechenaufwand sein wird. Gerade wegen des Halteproblems kann dies aber nur grob vorgenommen werden. Eine GröSSe sind zunächst die intrinsischen Kosten einer Transaktion. Das ist der Overhead der allein durch die Transaktion und deren Inhalt betsteht. Diese intrinsischen Kosten lassen sich schon vor Ausführung mit folgendem Algorithmus validieren.

Preis und Latenz

Anreiz und Spieletheorie

3.3 Value und Data

3.4 Signatur

ECDSA

Multisignaturen

4 Transaktionsabwicklung

4.1 Propagation

4.2 Speicherung

5 Ausblick

Literatur

1. Davis, M.: Computability and Unsolvability. Courier Corporation (Apr 2013)
2. M.Spain, M.Foley: OASIcs-Tokeneconomics. Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany (2019)
3. Wood, G.: Ethereum/yellowpaper. 2019-10-20 (Oct 2019)