



HOCHSCHULE OSNABRÜCK

UNIVERSITY OF APPLIED SCIENCES

Institut für Duale Studiengänge

PRÜFUNGSLEISTUNG

IM STUDIENGANG WIRTSCHAFTSINFORMATIK

Blockchain als verteiltes Datenbankmanagementsystem

Eingereicht von:

Matthias Fischer (700643)
Fabian Hagengers (701292)

Studiengruppe:

15DWF1

Betreuer:

Prof. Dr. Heiko Tapken

Modul:

Datenbank-Engineering

Abgabedatum:

30.03.2018

Inhaltsverzeichnis

Abbildungsverzeichnis	II
Tabellenverzeichnis	III
Listings	IV
Abkürzungsverzeichnis	V
1 Einleitung	1
2 Blockchain in der Theorie	1
2.1 Transaktionsablauf	1
2.2 Blockaufbau	2
2.3 Proof-Of-Work	2
3 Blockchain in der Praxis am Beispiel Multichain	3
3.1 Installation	3
3.2 Erstellung von Transaktionen	3
3.3 Erstellung von Transaktionen mit Daten	3
4 Kritische Reflexion	3
5 Fazit	3
Literaturverzeichnis	4
Eidesstattliche Erklärung	4

Abbildungsverzeichnis

1	Vereinfachter Transaktionsablauf. Quelle: Fraunhofer FIT	1
---	--	---

Tabellenverzeichnis

Listings

Abkürzungsverzeichnis

1 Einleitung

Seit der Schöpfung der ersten Bitcoins 2009 wächst die Popularität der Kryptowährungen und der Blockchain-Technologie stetig an.¹ Besonders die Industrie beschäftigt sich intensiv mit dem Thema Blockchain, da diese Technologie die Möglichkeit bietet Dokumente fälschungssicher, irreversible und dezentral zu speichern.² Satoshi Nakamoto veröffentlichte 2008 ein Artikel mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“, indem eine Währung ohne zentrale Entität erläutert wurde.³ Dieser Artikel von Satoshi Nakamoto stellt die Basis jeder Blockchain.

Innerhalb dieser Ausarbeitung sollen zwei Ziele verfolgt werden. Zunächst soll das theoretische Grundwissen der Blockchain-Technologie als Datenbank erläutert werden. Aufbauend auf diesem Wissen verfolgt diese Ausarbeitung das Ziel eine Blockchain mit der Software Multichain⁴ zu erstellen und anschließend Transaktionen durchzuführen.

Das nachfolgende Kapitel erläutert die theoretischen Hintergründe der Blockchain-Technologie. In Kapitel 3 wird eine Blockchain mit der Software Multichain erstellt und anschließend erläutert wie Transaktionen durchgeführt werden können. In Kapitel 4 folgt eine kritische Reflexion dieser Ausarbeitung. Abschließend wird ein Fazit der Ausarbeitung gebildet.

2 Blockchain in der Theorie

Die Blockchain ist eine verkettete Liste von Blöcken, welche mithilfe von kryptographischen Verfahren irreversible und manipulationsfrei verbunden sind. Ein Block enthält Transaktionen in denen Daten gespeichert sind. Eine Blockchain besteht nicht aus einer zentralen Datenbank, sondern wird in einem dezentralen Peer-To-Peer Netzwerk gespeichert. In einem Peer-To-Peer Netzwerk werden die Netzwerkteilnehmer als Nodes bezeichnet.⁵

2.1 Transaktionsablauf

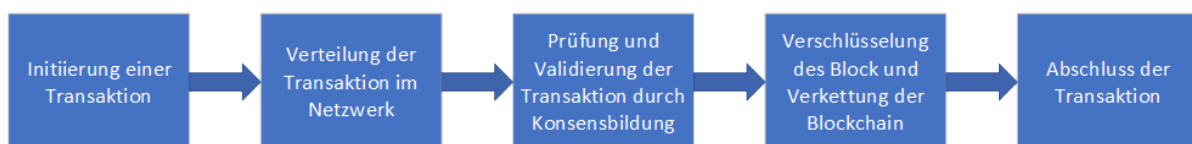


Abbildung 1: Vereinfachter Transaktionsablauf. Quelle: Fraunhofer FIT

¹[Neugebauer, 2018, S. 312]

²[Neugebauer, 2018, S. 312]

³[Satoshi Nakamoto, 2008, S. 1]

⁴<https://www.multichain.com/>

⁵[Korzun and Gurtov, 2013, S. 5]

Zunächst wird die durchzuführende Transaktion im Netzwerk verteilt. Anschließend fassen die Netzwerkteilnehmer mehrere Transaktionen zu einem Block zusammen und versuchen durch eine Konsensbildung die Transaktionen zu validieren. Die Validierung findet bei der Blockchain-Technologie mit dem sogenannten Proof-Of-Work statt, welche es fordert das aus den Transaktionen und dem vorherigen Block ein Hash-Wert mit einer bestimmten Voraussetzung gebildet wird. Nachdem ein Netzwerkteilnehmer ein validen Hash-Wert ermittelt hat, werden der Block an die Kette angehängen und im Netzwerk verteilt. Alle anderen Teilnehmer überprüfen die Erweiterung der Kette. Falls die neue Blockchain nicht den Ansprüchen der Voraussetzung entspricht, wird die Erweiterung abgelehnt und die vorherige Kette zurückgegeben, andernfalls wird die erweiterte Blockchain übernommen. Anschließend ist die Transaktion erfolgreich durchgeführt.

2.2 Blockaufbau

Hash eines Blockes besteht aus

- Hash des vorherigen Blockes
- Merkle-Root = Hash-Tree aus mehrere Transaktionen
- Nonce = frei wählbarer Wert, um die Anforderung der Blockchain zu bewerkstelligen
- Transaktionen

2.3 Proof-Of-Work

- Eigenschaften einer Blockchain
- dezentralität
- Blockaufbau
-

3 Blockchain in der Praxis am Beispiel Multichain

3.1 Installation

3.2 Erstellung von Transaktionen

3.3 Erstellung von Transaktionen mit Daten

4 Kritische Reflexion

5 Fazit

Literaturverzeichnis

Dmitry Korzun and Andrei Gurtov. *Structured peer-to-peer systems: Fundamentals of hierarchical organization, routing, scaling, and security*. Springer, New York, NY, 2013. ISBN 978-1-4614-5482-3.

Reimund Neugebauer, editor. *Digitalisierung: Schlüsseltechnologien für Wirtschaft und Gesellschaft*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1. auflage edition, 2018. ISBN 978-3-662-55889-8.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. URL <https://bitcoin.org/bitcoin.pdf>.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich meine Hausarbeit

Blockchain als verteiltes Datenbankmanagementsystem

selbstständig und ohne fremde Hilfe angefertigt habe und dass ich alle von anderen Autoren wörtlich übernommenen Stellen wie auch die sich an die Gedankengänge anderer Autoren eng anlehnenden Ausführungen meiner Arbeit besonders gekennzeichnet und die Quellen zitiert habe.

Ort, Datum

Unterschrift