

**Lennart Völler**

# Archetypen von Konsensalgorithmen in Blockchain

**Projektarbeit**

# BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei [www.GRIN.com](http://www.GRIN.com) hochladen  
und kostenlos publizieren



## **Bibliografische Information der Deutschen Nationalbibliothek:**

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

## **Impressum:**

Copyright © 2018 GRIN Verlag  
ISBN: 9783668858008

## **Dieses Buch bei GRIN:**

<https://www.grin.com/document/451969>

**Lennart Völler**

# **Archetypen von Konsensalgorithmen in Blockchain**

## **GRIN - Your knowledge has value**

Der GRIN Verlag publiziert seit 1998 wissenschaftliche Arbeiten von Studenten, Hochschullehrern und anderen Akademikern als eBook und gedrucktes Buch. Die Verlagswebsite [www.grin.com](http://www.grin.com) ist die ideale Plattform zur Veröffentlichung von Hausarbeiten, Abschlussarbeiten, wissenschaftlichen Aufsätzen, Dissertationen und Fachbüchern.

### **Besuchen Sie uns im Internet:**

<http://www.grin.com/>

<http://www.facebook.com/grincom>

[http://www.twitter.com/grin\\_com](http://www.twitter.com/grin_com)

# **Archetypen von Konsensalgorithmen in Blockchains**

Archetypes of consensus algorithms in Blockchain

---

## **Projektarbeit**

Im Virtuellen Weiterbildungsstudiengang Wirtschaftsinformatik

---

Verfasser: **Lennart Völler**

4. Fachsemester

Abgabe: 07.11.2018  
Wintersemester 2018 / 2019

<b>ABBILDUNGSVERZEICHNIS</b> .....	<b>A</b>
<b>ABKÜRZUNGSVERZEICHNIS/GLOSSAR</b> .....	<b>B</b>
<b>FORMELVERZEICHNIS</b> .....	<b>C</b>
<b>1. EINLEITUNG</b> .....	<b>1</b>
<b>2. METHODEN</b> .....	<b>3</b>
2.1    QUALITATIVE INHALTSANALYSE.....	6
2.2    QUANTIFIZIERUNG .....	9
2.3    PARTITIONIERENDE CLUSTERANALYSE MITTELS K-MEANS CLUSTER ALGORITHMUS.....	11
<b>3. ANALYSE</b> .....	<b>14</b>
3.1    QUALITATIVE INHALTSANALYSE.....	14
3.1.1    Materialauswahl.....	14
3.1.2    Kategorie Bildung.....	14
3.1.3    Konsensalgorithmen.....	16
3.1.4    Kategorien.....	19
3.1.5    Merkmalsausprägungen.....	23
3.2    QUANTIFIZIERUNG .....	25
3.3    CLUSTERANALYSE .....	27
3.4    GENERIERUNG VON ARCHETYPEN.....	29
3.4.1    Archetyp c1: The Rocket.....	32
3.4.2    Archetyp c2: The Democrat.....	32
3.4.3    Archetyp c3: The Undecided .....	33
3.4.4    Archetyp c4: The Wonderchild.....	33
<b>4. FAZIT</b> .....	<b>34</b>
<b>LITERATURVERZEICHNIS</b> .....	<b>37</b>
<b>APPENDIX</b> .....	<b>46</b>
APPENDIX A – EINORDNUNG UNTERSUCHTER MATERIALIEN.....	46
APPENDIX B – INDUKTIVE BILDUNG VON KATEGORIEN.....	48
APPENDIX C – BESTIMMUNG VON MERKMALSAUSPRÄGUNGEN VON KONSENSALGORITHMEN .....	60
APPENDIX D – DARSTELLUNG DER MERKMALSAUSPRÄGUNGEN .....	84
APPENDIX E – PROGRAMMCODE FÜR K-MEANS CLUSTERING .....	85
APPENDIX F – ERGEBNISSE DER CLUSTERANALYSE .....	97
APPENDIX G – GEGENÜBERSTELLUNG QUALITATIVER MERKMALSAUSPRÄGUNGEN VON KONSENSALGORITHMEN EINES CLUSTERS .....	99
G.1 Cluster c1: {BFT, RPCA}.....	99
G.2 Cluster c2: {PoW, PoC}.....	101
G.3 Cluster c3: {PoA, PoET, Stellar}.....	103
G.4 Cluster c4: {PoS, DPoS}.....	104

---

## Abbildungsverzeichnis

Abb. 1: Typen von Konsensalgorithmen in Blockchains.....	2
Abb. 2: Abstraktionsebenen von Blockchains .....	5
Abb. 3: Ablauf der qualitativen Inhaltsanalyse .....	7
Abb. 4: Ergebnis der induktiven Kategorie Bildung .....	14
Abb. 5: Vergleich von induktiv gebildeten Kategorien und im Material verwendeten Kategorien.....	23
Abb. 6: Quantifizierte Merkmalsausprägungen der Analysedaten.....	25
Abb. 7: Normierte Merkmalsausprägungen .....	26
Abb. 8: Distanzmatrix aller untersuchten Konsensalgorithmen .....	27
Abb. 9: Ergebnisse des K-Means Algorithmus.....	28
Abb. 10: Persistente Cluster über verschiedene Werte von K.....	28
Abb. 11: Steigerung der Abdeckung der Merkmalsausprägungen durch Centroide mit abnehmender Clustergröße.....	30
Abb. 12: Lage der Centroidefür $k=4$ und relative Abdeckung der Kategorien der Clusterelemente .....	31
Abb. 13: Konsensalgorithmus Archetypen mit charakterisierenden Symbolen.....	34

---

## Abkürzungsverzeichnis/Glossar

<b>Abkürzung</b>	<b>Bedeutung</b>
ASIC	Application-specific integrated circuit
BFT	Byzantine fault tolerance
BTC	Bitcoin
DPoS	Delegated Proof of Stake
ETH	Ethereum
LPoS	Leased Proof of Stake
LTC	Litecoin
PoA	Proof of Authority
PoBa	Proof of Bandwidth
PoBu	Proof of Burn
PoC	Proof of Capacity
PoET	Proof of Elapsed Time
PoR	Proof of Retrievability
PoS	Proof of Stake
PoS	Proof of Storage
PoV	Proof of Velocity
PoW	Proof of Work
RPCA	Ripple Protocol Consensus Algorithm
TX	Transaction

---

## Formelverzeichnis

Formel 1: Normierung von Merkmalsausprägungen .....	10
Formel 2: Gower Koeffizient .....	12
Formel 3: Distanzfunktion für nominale Attribute .....	12
Formel 4: Distanzfunktion für ordinale Attribute .....	12
Formel 5: Gemittelte quadratische Distanz aller Punkte eines Clusters .....	13

---

# 1. Einleitung

Als Satoshi Nakamoto 2008 das Bitcoin Whitepaper veröffentlichte, interessierte das zunächst niemanden. Es dauerte einige Zeit, bis sich zumindest eine kleine Gruppe von Menschen fand, die die Reichweite seiner Erfindung erahnen konnten. Diese Gruppe tauschte sich zunächst auf dem von Nakamoto gegründeten Bitcointalk Forum aus. In den folgenden Jahren nahmen das Thema dann auch Medien, die einer breiteren Öffentlichkeit zugänglich sind, auf – nicht unwesentlich mit der Wertsteigerung von Bitcoin korreliert – und befassten sich mit dem neuen Phänomen: „Blockchain“. Auch nach zehn Jahren kann das Thema Blockchain noch als neu bezeichnet werden. Bitcoin als Urvater der Blockchain und von vielen synonym für die Technologie herangezogenes Beispiel hat es längst in die Massenmedien geschafft und den ein oder anderen Hype in der Finanztechnologie ausgelöst. Dennoch scheint ein tiefergehendes Verständnis der Technologie hinter Bitcoin und Blockchain nach wie vor der kleinen Gruppe an Enthusiasten vorbehalten zu bleiben, die auch schon vor zehn Jahren das Potenzial der Technologie erkannte. Wenn in nicht-technischen Kreisen davon gesprochen wird, man habe Bitcoin und Blockchain verstanden, dann ist dieses Verständnis oft auf einem ähnlich oberflächlichen Niveau wie das Verständnis von Kernspaltung zur Energiegewinnung; man weiß, wie es schematisch funktioniert, ist jedoch trotzdem noch kein Atomphysiker.

Nun wird kaum jemand behaupten, der Aufbau der Blockchain reiche in seiner Komplexität an einen Atomreaktor heran. Warum stoppt der Prozess des Verstehens dennoch so oft an der Oberfläche des Themas oder bleibt bei Bitcoin stehen, wo es doch mittlerweile über 2000 sogenannte Altcoins gibt (Coinmarketcap 2018)? Die Blockchain Technologie hat sich in den vergangenen Jahren – ebenfalls nicht unwesentlich mit der Wertsteigerung von Bitcoin korreliert – rasant weiterentwickelt, was zu einer wuchernden Diversifizierung von Anwendungsgebieten, Implementierungen, Protokollen und Algorithmen geführt hat. Den Überblick angesichts der vielen möglichen Anwendungsgebiete dieser Technologie zu behalten oder als Neuling auf dem Gebiet Fuß zu fassen, erscheint zunehmend schwierig. Dies liegt nach Sicht des Autors daran, dass bisher alles, was mit Blockchain zutun hat, unter ebendiesem Begriff subsummiert wird. Weder wird zwischen verschiedenen Anwendungsbereichen noch zwischen verschiedenen, fundamental unterschiedlich verwendeten Algorithmen unterschieden. Niemand käme auf die Idee, bei dem Begriff „Kraftfahrzeug“ Straßenfahrzeuge und Landfahrzeuge in eine Kategorie einzuteilen. Auf dem Blockchain

Feld passiert genau das. Diese Arbeit löst das Problem in einem Teilbereich der Blockchain Technologie: den Konsensalgorithmen.

Diese Arbeit entwickelt vier Archetypen von Konsensalgorithmen, die wesentliche Charakteristiken zusammenfassen und so die Orientierung zwischen den mittlerweile über zwei dutzend Konsensalgorithmen in Blockchains erleichtern.

### Was sind Konsensalgorithmen?

Konsensalgorithmen sind nicht neu. Sie werden seit Jahrzehnten in verteilten Systemen eingesetzt, um sicherzustellen, dass alle Systemteile stets über eine aktuelle bzw. korrekte Kopie der Daten verfügen. Sie schließen somit Speicherkonflikte aus und legen fest, welcher Zustand der Daten im ganzen System als wahr anerkannt wird (vgl. Metzger 2018). Konsensalgorithmen sind die Kernkomponente von Blockchains, da sie in verschiedensten Konstellationen von sich vertrauenden oder nicht vertrauenden Parteien, unter Verwendung verschiedenster Mechanismen, dafür sorgen können, dass stets Einigkeit darüber besteht, was der aktuelle Zustand des Netzwerkes ist. Dieser Zustand kann – in Kryptowährungen – die Information darüber sein, wer zu welchem Zeitpunkt über welche Gelder verfügen darf oder – in verteilten Datenbanken – die Information darüber, wer zu welchem Zeitpunkt welche Zugriffsrechte hat oder hatte. Konsensalgorithmen sind die Kernkomponente der Blockchain (vgl. Bano et al. 2017, p. 1).

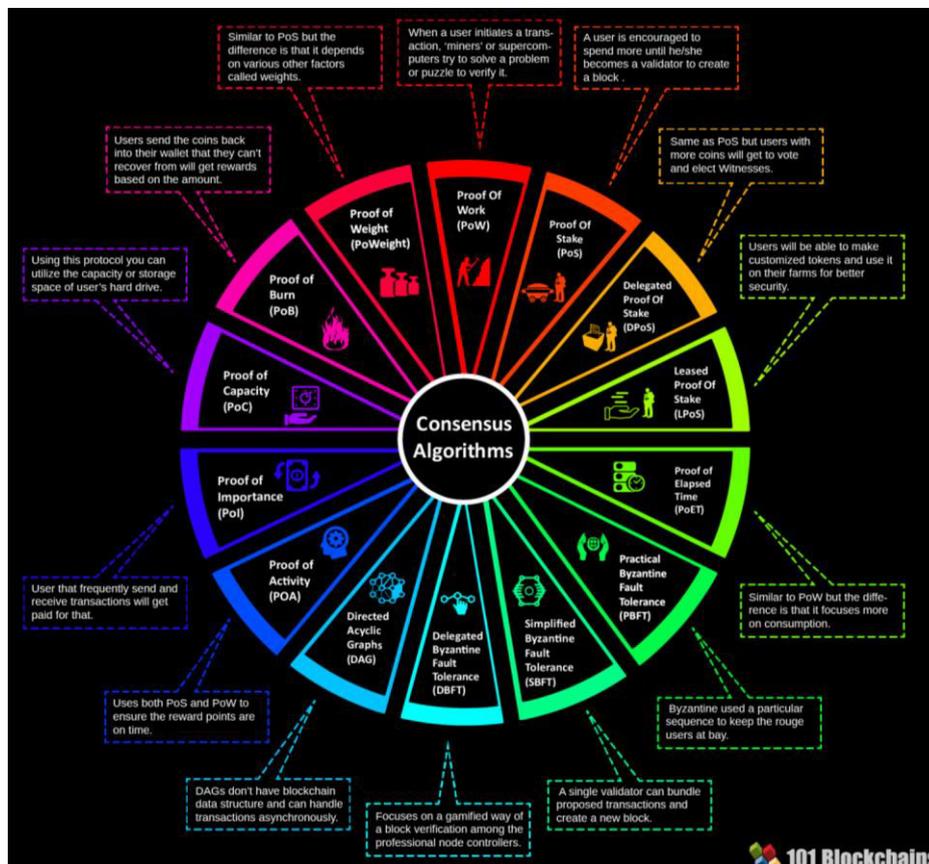


Abb. 1: Typen von Konsensalgorithmen in Blockchains (Anwar 2018)