Lennart Völler

Archetypen von Konsensalgorithmen in Blockchain

Projektarbeit

GRIN

Bibliografische Information der Deutschen Nationalbibliothek:

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

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 Verlag

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

Abbildungsverzeichnis

Abkürzungsverzeichnis/Glossar

Abkürzung	Bedeutung
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

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 Kernkernkomponente 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).

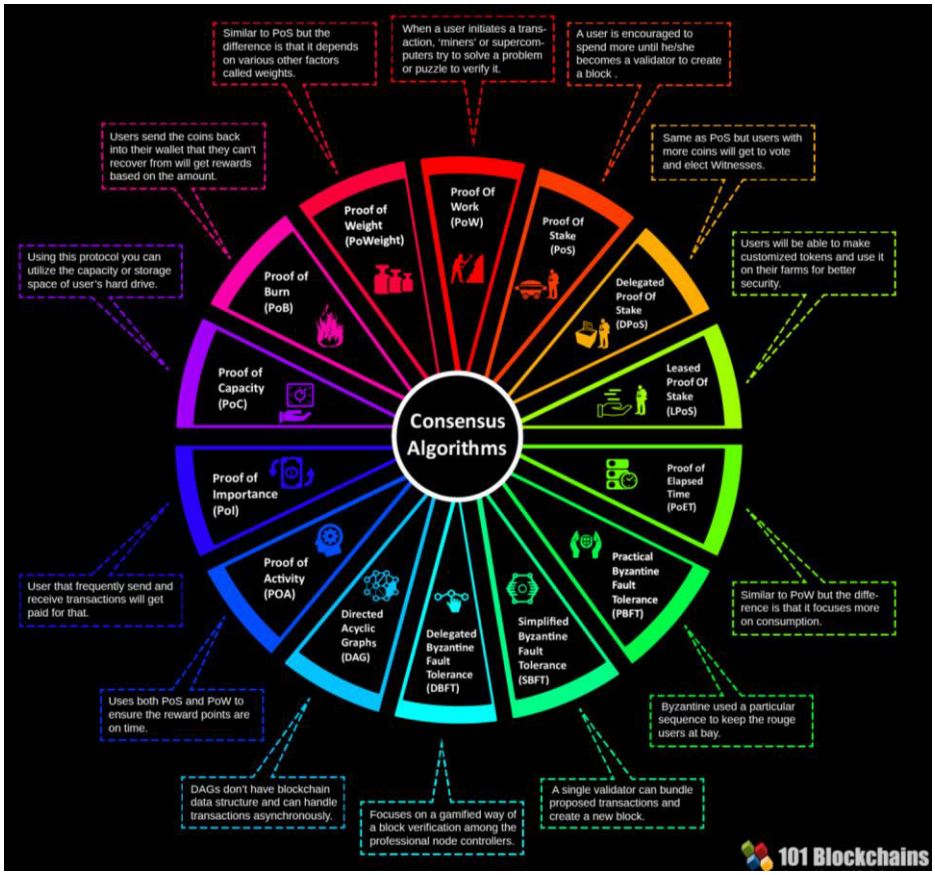

Abb. 1: Typen von Konsensalgorithmen in Blockchains (Anwar 2018)