Konsens-Algorithmen von Blockchain

Eine Betrachtung der Nachhaltigkeit der Konsensfindung

Felix Eigelshoven, André Ullrich und Norbert Gronau, Lehrstuhl für Wirtschaftsinformatik, Universität Potsdam

Neben dem enormen Kursanstieg des Bitcoins in den Jahren 2017/2018, stieg im gleichen Maß auch die benötigte Rechenleistung und der damit verbundene Elektrizitätsbedarf, um Blöcke innerhalb der Bitcoin-Blockchain zu verifizieren. Aus diesem Problem ableitend beschäftigt sich dieser Beitrag mit der Fragestellung, welchen Beitrag unterschiedliche Konsens-Algorithmen innerhalb einer Blockchain zur Nachhaltigkeit liefern. Im Ergebnis liegt ein Überblick über die meist genutzten Konsens-Algorithmen und deren Beitrag zur Nachhaltigkeit vor.

Consensus Algorithms in Blockchain

Alongside to the enormous rise in Bitcoin value in 2017/2018, there was also a tremendous rise in required Hashpower and electricity to verify blocks of the Bitcoin-Chain. Deriving from this problem, this article investigates different consensus algorithms and their impact on sustainability. Furthermore this article proposes an extensive comparison of the most used Blockchain algorithms with a focus on their contribution to sustainability.

Keywords:
consens-algorithms, blockchain, proof of work, proof of stake, delegated proof of stake, sustainability

Allgemein kann eine Blockchain als ein verteiltes und dezentrales Register beschrieben werden, in dem Daten in Form von Blöcken vollständig zusammengefasst werden [1, 2]. Diese Blöcke werden anschließend mittels kryptographischer Verfahren miteinander verkettet. Jeder Block besitzt genau einen Elternblock und besteht aus einem Block Header und einem Block Body. Der Header enthält unter anderem die aktuelle Blockversion, einen auf den Elternblock verweisenden Hashwert, den Hashwert aller Transaktionen eines Blocks (Merkle Tree Root Hash), einen Zeitstempel, eine kompakte Form des aktuellen Hashziels (nBits) und ein 4-Byte-Nonce-Feld zur Beeinflussung der Hash-Schwierigkeit. Die Hash-Schwierigkeit definiert die Anforderungen an den zu findenden Hashwert in der Konsensfindung. Der Body hingegen enthält die Anzahl der Transaktionen (Transaction Counter) und die Transaktionen selbst [1, 3]. Eine Besonderheit innerhalb der Blockchain stellt der erste Block dar, der Genesis Block. Dieser ist fest im Quellcode verankert, speichert die ersten Transaktionen in einer Blockchain und besitzt keinen Elternblock [1]. Bild 1 zeigt den schematischen Aufbau einer Blockchain.

Die Blockchain-Technologie zeichnet sich dabei vor allem durch die vier Merkmale Dezentralität, Persistenz, Anonymität und Nachvollziehbarkeit aus [1, 3].

Dezentralität bedeutet in diesem Zusammenhang, dass eine Transaktion zwischen zwei Parteien nicht von einer zentralisierten dritten Partei verifiziert werden muss, sondern innerhalb des Netzwerkes selbst verifiziert werden kann. Hierdurch können anfallende Kosten gesenkt und die Performance verbessert werden [1]. Weiterhin wird das Netzwerk robuster, da kein zentraler Angriffspunkt existiert und bei einem Knotenausfall die Transaktion über eine alternative Strecke übermittelt werden kann. Dies ist möglich, da jede Partei als gleichwertig betrachtet wird [5]. Um eine Transaktion zwischen verschiedenen Teilnehmern zu authentifizieren, werden asymmetrische kryptographische Verfahren in Form von digitalen Signaturen verwendet. Jeder Nutzer erhält einen privaten und einen öffentlichen Schlüssel. Der private Schlüssel wird dabei für die Signierung der Transaktion genutzt und kann mit dem öffentlichen Schlüsselpaar anschließend verifiziert werden [1, 3].

Blockchain-Anwendungen lassen sich in die Typen privat, öffentlich, halbprivat und Konsortium unterteilen: Öffentliche Blockchain-Anwendungen können von jedem gelesen und für Transaktionen genutzt werden. Jeder Netzwerkteilnehmer kann an der Konsensfindung partizipieren. Private Blockchain-Anwendungen hingegen werden von einer zentralen Organisation gesteuert, welche über die Rechtevergabe entscheidet. Halbprivate Anwendungen stellen Mischformen dar. Konsortium Blockchain-Anwendungen können nur von

B. Sc. Felix Eigelshoven arbeitet als studentischer Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik, insb. Prozesse und Systeme an der Universität Potsdam.

Dr. André Ullrich arbeitet im Rahmen der Nachwuchsforschergruppe ProMUT als Post-Doktorand am Lehrstuhl für Wirtschaftsinformatik, insb. Prozesse und Systeme an der Universität Potsdam.

Prof. Dr.-Ing. habil. Norbert Gronau ist Inhaber des Lehrstuhls für Wirtschaftsinformatik, insb. Prozesse und Systeme sowie Direktor des Forschungs- und Anwendungszentrums Industrie 4.0 an der Universität Potsdam.

felix.eigelshoven@lswi.de
www.lswi.de

https://doi.org/10.30844/I40M_20-1_S29-32

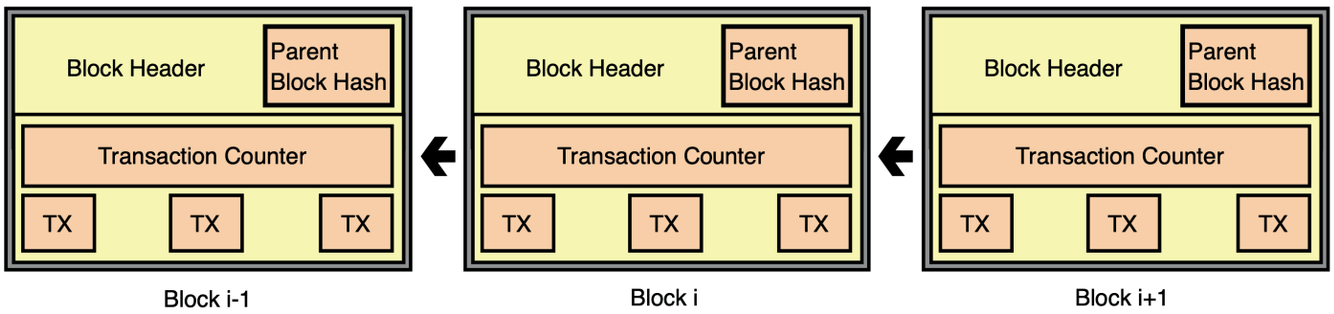

Bild 1: Schematische Architektur einer Blockchain [4].

vorab definierten Parteien verwendet werden und unterliegen diversen Restriktionen [1, 6].

Zur Notwendigkeit von Konsens in der Blockchain

Konsensfindung beschreibt den dynamischen Prozess der Einigung auf einen Zustand innerhalb einer Gruppe oder eines Netzwerks [1, 7]. Aufgrund dezentraler und verteilter Architektur stehen Blockchain-Anwendungen bei der Findung eines gemeinsamen Konsenses vor zwei Problemen [2, 7]: (1.) Das Byzantine General Problem. Hierbei handelt es sich um ein Szenario, in dem eine Gruppe von Generälen den Angriff auf eine Stadt koordiniert. Der Angriff kann dabei nur gelingen, wenn alle Generäle die Stadt gleichzeitig angreifen. Dabei gilt es jedoch zu beachten, dass die einzelnen Generäle auch Verrat begehen können und diese sich somit gegenseitig nicht trauen [8]. Auf Blockchain übertragen existiert eine Vielzahl an unbekannten Teilnehmern innerhalb eines Netzwerks, die sich unabhängig voneinander über die Richtigkeit eines Blocks einigen müssen. (2.) Kann Guthaben in einer Währung für zwei Transaktionen gleichzeitig genutzt werden, so wird dies als Double-Spending-Problem bezeichnet. Dies ist theoretisch in der Blockchain möglich, da im Vergleich zu klassischen Währungen wie dem Dollar weder ein physisches Underlying noch eine zentrale Partei, die alle Transaktionen verifiziert, existieren [2, 7, 9]. Zur Lösung dieser Probleme bedarf es Algorithmen zur Konsensfindung innerhalb des Netzwerks. Die im folgenden vorgestellten Algorithmen gewährleisten hierbei, dass nur ein Block an die vorhandene Kette gehangen wird. Dieser beinhaltet ausschließlich gültige Transaktionen [7]. So wird gewährleistet, dass alle Nutzer innerhalb des Netzwerks auf die gleiche Datenbasis zurückgreifen können und keine doppelten Ausgaben möglich sind [7]. Weiterhin reduzieren Konsens-Algorithmen den Anreiz ungültige bzw. schädliche Blöcke parallel anzubieten und so das Netzwerk zu manipulieren [1, 2, 10].

Proof of Work - POW

Die Grundidee des Proof-of-Work-Algorithmus beruht darauf, dass jeder Netzwerkteilnehmer die Transaktionen eines Blocks prüfen kann, indem er mittels Rechenleistung komplexe mathematische Probleme löst. Die Durchführung dieser mathematischen Funktion wird als Mining und die durchführenden Teilnehmer als Miner bezeichnet. Möchte ein Miner einen neu erstellten Block an eine bestehende Kette anfügen, so muss dieser einen bestimmten Grad an Arbeit verrichten [3], wodurch diesem Kosten in Form von Zeit und Ressourcen entstehen. Ein neu erstellter Block wird verifiziert, indem der Header des neuen Blocks mit dem Wert des Nonce-Felds kombiniert und anschließend mittels einer Hash-Funktion transformiert wird [3, 11].

Eine Hash-Funktion ist eine Funktion, die eine Folge an Zeichen mit beliebiger Länge in eine Zeichenfolge mit fester länge transformiert (Hashwert) [11, 12]. Die eigentliche Schwierigkeit liegt hierbei darin, dass der zu findende Hashwert bestimmte Eigenschaften aufweisen muss, bspw. eine vorab definierte Nullfolge am Anfang des Werts. Dies wird im Nonce-Feld definiert [9]. Ein verifizierender Hashwert muss dabei kleiner-gleich dem Ziel-Hashwert sein. Im Fall Bitcoin wird die Hashfunktion SHA-256 genutzt [10].

Der Miner, der als erstes den passenden Hashwert findet, darf den Block an die bestehende Kette anheften und wird für seinen Aufwand vergütet. Die anderen Miner gehen in diesem Fall leer aus. Wurde ein Block erfolgreich verifiziert, muss dieser anschließend vom restlichen Netzwerk bestätigt werden, indem diese den Wert erneut per Hashfunktion prüfen [1, 3, 11]. Die Vergütung besteht aus einer vorab im Pro-

tokoll definierten Summe an neu generierten Token sowie den Transaktionsgebühren des neuen Blocks. Hierbei muss jedoch beachtet werden, dass die Schwierigkeit der Hashfunktion, sowie die Prämie sich über den Lauf der Zeit anpassen. Aktuell erhalten Bitcoin-Miner eine Belohnung in Höhe von 12.5 Bitcoin, welche sich alle 210.000 Blöcke halbiert [9, 13].

Proof of Stake – POS

Im direkten Vergleich steht beim Proof of Stake nicht das Verrichten von Arbeit in Form von Rechenleistung im Vordergrund, sondern die Anzahl an Token, die ein Netzwerkteilnehmer (Stakeholder) bereit ist, für einen bestimmten Zeitraum wegzuschließen. Während dieses Zeitraums können die weggeschlossenen Token weder gehandelt noch verkauft werden. Dieser Anteil an Token, den ein Teilnehmer wegschließt, wird als Stake bezeichnet, das Wegschließen als Staken. POS verfolgt die grundlegende Idee, dass Teilnehmer, die eine große Anzahl an Token wegschließen, weniger dazu tendieren, das Netzwerk in Form von falsch verifizierten Blöcken anzugreifen. Folglich können nur Stakeholder an der Konsensfindung teilnehmen [9, 12, 14].

In einem Netzwerk, das zur Konsensfindung einen POS-Algorithmus nutzt, bspw. das NXT-Netzwerk, wird für jede Blockverifizierung eine Partei per Zufall ausgewählt. Je größer der Stake einer Partei ist, desto höher ist die Wahrscheinlichkeit, dass diese Partei ausgewählt wird, um den nächsten Block zu verifizieren. Je nach Ausführung des Algorithmus spielen weitere Variablen eine Rolle. Diese zusätzlichen Bedingungen werden implementiert, damit die Entscheidungsfindung nicht alleine vom Vermögen abhängig ist und auch Nutzer mit einem geringen Stake die Möglichkeit erhalten, Blöcke zu verifizieren. Nach erfolgreicher Auswahl wird der Netzwerkteilnehmer, der den Block verifiziert hat, in Form einer vorab definierten Prämie vergütet. In POS-Algorithmen werden keine neuen Token generiert. Die Prämie entspricht daher den Transaktionsgebühren eines Blocks [9].

Da Stakeholder jedoch keine Ressourcen bei der Verifikation von Blöcken verbrauchen, stehen POS-Algorithmen aufgrund ihres Designs vor einem sogenannten Nothing-at-Stake-Problem. Da es zu keinen Opportunitätskosten bei der Verifizierung von legitimen Blöcken kommt, besteht für verifizierende Stakeholder im Falle einer Teilung in zwei Ketten, (wie im Fall Ethereum und Ethereum Classic) der Anreiz darin, mehrere Blöcke parallel zu verifizieren und so die Menge an erhaltenen Transaktionsgebühren zu maximieren [14].

Delegated Proof of Stake – DPOS

Der Konsens-Algorithmus Delegated Proof of Stake stellt eine erweiterte Version des Proof of Stake dar und verbindet Reputation innerhalb des Netzwerks mit einem Echtzeit-Wahlsystem. Bei dieser Variante wählen die Stakeholder mittels Stimmrechten delegierte Validatoren, welche die Verifikation von Blöcken und Transaktionen verantworten. Die Stimmrechte werden hierbei proportional zur Anzahl vorhandener Token vergeben. Hierbei können Abstimmungssystem und Vergütungssystem von Netzwerk zu Netzwerk variieren. In der Regel wird jedoch der Validierer für die Verifikation der Transaktionen prozentual vergütet. Diese Vergütung kann anschließend proportional mit den Wählern geteilt werden [2, 10]. Aufgrund der geringeren Anzahl beteiligter Parteien können Blöcke schneller verifiziert und somit Transaktionen schneller durchgeführt werden. Weiterhin können unehrliche Validatoren schnell vom Netzwerk abgewählt und durch eine vertrauenswürdige Partei ersetzt werden [1, 7].

Nachhaltigkeit in der Blockchain

Wie beschrieben setzt der POW-Algorithmus auf das Verrichten von Arbeit in Form von Rechenleistung. Dies hat Auswirkungen auf die Nachhaltigkeit von Blockchain-Anwendungen und wird im Folgenden anhand der Bitcoin-Blockchain diskutiert: Das Ausführen der Hashfunktionen ist sehr rechenintensiv und mit enormem Stromverbrauch verbunden. Allein die Konsensfindung von Bitcoins verbraucht mindestens 2.55 GWh jährlich, Tendenz stark steigend [14]. Bei einem Stromverbrauch von 2.55 GWh (Stand 2018; zum Vergleich: der Jahresverbrauch Irlands entsprach 3.1 GWh) kostet eine Transaktion innerhalb des Bitcoin-Netzwerks ca. 300 kWh [10, 15].

Je mehr Rechenleistung ein Miner besitzt, desto schneller können Inputs in einen Hashwert umgewandelt werden. Folglich haben die Miner mit der meisten Rechenleistung auch die höchste Wahrscheinlichkeit den nächsten Block zu verifizieren und die Prämie einzustreichen [10, 16]. Im Fall von Bitcoin liefern die Investitionskosten in Form von Hardware und Ressourcenbedarf zusätzlichen Schutz und stellen eine Hürde für potenzielle Angreifer da [5]. Aufgrund der ansteigenden Schwierigkeit in POW-Algorithmen, müssen Teilnehmer technisch aufrüsten, um weiterhin erfolgreich

Literatur

[1] Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H.: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. (2017), S. 557–564.

[2] Alsunaidi, S. J.; Alhaidari, F. A.: A Survey of Consensus Algorithms for Blockchain Technology. In: Int. Conf. Comput. Inf. Sci. (2019), S. 1–6.

[3] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, Abrufdatum: 5.7.2019

[4] Nofer, M.; Gomber, P.; Hinz, O.; Schiereck, D.: Blockchain. In: Business & Information Systems Engineering: Vol. 59, No. 3. 2017, S. 183-187. DOI: 10.1007/s12599-017-0467-3

[5] Berentsen, A.; Schäfer, F.: Bitcoin, Blockchain und Kryptoassets. Auflage 1., Norderstedt 2017.

[6] SAP: Was ist eigentlich eine Blockchain? URL: www.sap.com/germany/products/leonardo/blockchain/what-is-blockchain.html, Abrufdatum 3.7.2019.

[7] Chaudhry, N.; Yousaf, M. M.: Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. In: ICOSST 2018 - 2018 Int. Conf. Open Source Syst. Technol. Proc. (2019), S. 54–63.

[8] Lamport, L.; Shostak, R.; Pease, M.: The Byzantine Generals Problem. In: ACM Trans. Program. Lang. Syst. 4 (1982) 3, S. 382–401.

[9] Seang, S.: Torre, D.: Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies. Working Papers, HAL. 2018.

	Proof of Work	Proof of Stake	Delegated Proof of Stake
Sozial	+ Jeder Teilnehmer kann an der Konsensfindung partizipieren - Zentralisierung durch Mining Pools	- Höhe des Stakes hat direkten Einfluss auf Entscheidungsmacht der Teilnehmer - Konsensfindung nur durch Stakeholder	+ Faire Prämiendistribution möglich - Zentralisierung durch Validierer - Konsensfindung nur durch gewählte Validierer
Ökonomisch	+ Prämien bei Blockverifikation - teure Hardware Investitionen - Skalierbarkeit und Effizienz	+ Prämien bei Blockverifikation + Keine teuren Hardware Investitionen - Nothing at Stake Problem	+ Prämien bei Blockverifikation + Keine teuren Hardware Investitionen + Skalierbarkeit und Effizienz
Ökologisch	- Hoher Energieverbrauch	+ Energieeffizient	+ Energieeffizient

Bild 2: Verortung der Algorithmen in die drei Säulen der Nachhaltigkeit.

an der Konsensfindung teilnehmen zu können. Dieses Wettrüsten führt zum Zusammenschluss der einzelnen Parteien, zu sogenannten Mining-Pools, in denen Rechenleistung zusammengelegt wird, um mathematischen Probleme gemeinsam zu lösen. Nach erfolgreichem Minen eines Blocks wird die Prämie innerhalb des Pools aufgeteilt. Aktuell besitzen die vier größten Mining Pools mehr als 50 % der gesamten Rechenleistung innerhalb des Bitcoin-Netzwerks. Durch die Bildung von Mining Pools und der Zusammenlegung von Rechenleistung verliert das Bitcoin-Netzwerk stetig an Dezentralität [2, 10].

Im direkten Vergleich bieten der POS- als auch der DPOS-Algorithmus eine weitaus umweltfreundlichere und nachhaltigere Alternative zur Konsensfindung. Teilnehmer benötigen keine rechenstarke Hardware, somit kann der Bedarf von Elektrizität sowie das Anschaffen teurer Hardware um ein Vielfaches verringert werden [1, 14].

Aufgrund der geringeren Anzahl an Validierungsmöglichkeiten, können Blöcke eines DPOS-Algorithmus schneller verifiziert und folglich Transaktionen schneller ausgeführt werden. Im Gegenzug zur gewonnen Effizienz verliert das Netzwerk jedoch durch die beschränkte Anzahl an Validierern an Dezentralität [1, 10]. Die folgende Tabelle ordnet die vorgestellten Algorithmen in die drei Säulen der Nachhaltigkeit ein.

Wie Zheng u. a. [1] zeigen, sind alle drei Algorithmen anfällig für einen 51%-Angriff.

Dabei versucht der Angreifer die Konsensfindung zu seinen Gunsten zu beeinflussen, indem er einen Großteil der Entscheidungsgewalt selbst stellt [1, 2, 5]. Für einen effektiven Angriff auf ein Netzwerk das POS oder DPOS nutzt, benötigt der Angreifer mehr als 50% der Coins oder mehr als 50% der Validatoren. Hervorzuheben ist jedoch, dass solch ein Angriff hier aufgrund des Algorithmus-Designs als sehr unwahrscheinlich zu bewerten ist [2]. In einem Netzwerk das POW zur Konsensfindung nutzt, reichen bereits mehr als 25% der Gesamtrechenleistung, um das Netzwerk zu manipulieren und die Wahrscheinlichkeit einer Belohnung zu erhöhen (vgl. selfish mining strategy) [1, 2, 11]. Wird das Mining jedoch aus einer spieltheoretischen Sicht betrachtet, so stellt ehrliches Verhalten ein Nash-Gleichgewicht dar, solange die Miner nur über eine geringe Rechenleistung verfügen [17].

Das dynamische Wahlsystem des DPOS Algorithmus bietet eine mögliche Lösung für das Nothing-at-Stake Problem. Betrügerische Validatoren können problemlos abgewählt und anschließend durch einen Validator mit besserer Reputation ersetzt werden [1, 2].

Zusammenfassung

Blockchain-Technologien stehen aufgrund ihrer dezentralen und verteilten Architektur vor dem Problem einer einheitlichen Konsensfindung. Die in diesem Beitrag vorgestellten Konsens-Algorithmen bieten verschiedene Möglichkeiten, um innerhalb des Netzwerks einen einheitlichen Konsens zu erreichen. Proof-of-Work-Algorithmen, wie im Fall von Bitcoin, weisen einen hohen Elektrizitätsverbrauch auf. Proof-of-Stake- sowie Delegated-Proof-of-Stake-Algorithmen stellen im direkten Vergleich zu Proof of Work eine ressourcenschonendere Alternative zur effektiven Konsensfindung innerhalb eines Netzwerks dar.

Dieser Beitrag entstand im Rahmen der Nachwuchsforschungsgruppe ProMUT „Nachhaltigkeitsmanagement 4.0 – Transformative Potentiale digital-vernetzter Produktion für Mensch, Umwelt und Technik" (Kennzeichen 01UU1705B), das vom Bundesministerium für Bildung und Forschung in Rahmen der Förderinitiative „Sozial-ökologische Forschung" gefördert wird.

Schlüsselwörter:
Konsens-Algorithmen, Blockchain, Proof of Work, Proof of Stake, Delegated Proof of Stake, Nachhaltigkeit

[10] Mingxiao, D.; Xiaofeng, M.; Zhe, Z.; Xiangwei, W.; Qijun, C.: A review on consensus algorithm of blockchain. In: IEEE Int. Conf. Syst. Man, Cybern. SMC 2017, vol. 2017-Janua (2017), S. 2567–2572.
[11] Bhaskar, N. D.; Chuen, D. L. K.: Bitcoin Mining Technology. Amsterdam 2015.
[12] Siim, J.: BlackCoin's Proof-of-Stake Protocol v2. https://courses.cs.ut.ee/MTAT.07.022/2017_fall/uploads/Main/janno-report-f17.pd, Abrufdatum: 5.7.2019.
[13] Coingecko: When is Bitcoin Halving. 2019. URL: www.coingecko.com/de/explain/bitcoin_halving, Abrufdatum: 5.7.2019.
[14] Saleh, F.: Blockchain Without Waste: Proof-of-Stake. SSRN Electron. https://ssrn.com/abstract=3183935, Abrufdatum 5.07.2019.
[15] Vries, A.: Bitcoin's Growing Energy Problem. In: Joule 2 (2018) 5, S. 801–805.
[16] Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C.: Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. Sustainability 2017, 9, 2214.
[17] Kiayias, A.; Koutsoupias, E.; Kyropoulou, M; Tselekounis, Y.: Blockchain Mining Games. http://arxiv.org/abs/1607.02420, Abrufdatum: 27.9.2019