

Thum, Marcel

Article

Die ökonomischen Kosten des Bitcoin-Mining

ifo Schnelldienst

Provided in Cooperation with:

Ifo Institute – Leibniz Institute for Economic Research at the University of Munich

Suggested Citation: Thum, Marcel (2018) : Die ökonomischen Kosten des Bitcoin-Mining, ifo Schnelldienst, ISSN 0018-974X, ifo Institut - Leibniz-Institut für Wirtschaftsforschung an der Universität München, München, Vol. 71, Iss. 02, pp. 18-20

This Version is available at:

<https://hdl.handle.net/10419/175155>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Marcel Thum*

Die ökonomischen Kosten des Bitcoin-Mining

Bitcoins werden in der Öffentlichkeit momentan vor allem unter den Aspekten des »staatsfernen« Geldes und der Gefahr einer spekulativen Blase diskutiert. In der Euphorie über die neue Form digitaler Währung wird häufig übersehen, dass Bitcoins und andere Kryptowährungen im Gegensatz zum traditionellen Geld erhebliche reale Kosten bei der Erzeugung verursachen. Allein die Erzeugung von Bitcoins dürfte seit 2010 mehr als 5 Mrd. US Dollar gekostet haben.

Noch vor zwei oder drei Jahren waren Bitcoins im Wesentlichen nur ein Thema für Computernerds. Aktuell sind Bitcoins und andere Kryptowährungen in aller Munde. Bitcoins werden als Zahlungsmittel wie auch als Anlageobjekte ernsthaft in den Massenmedien diskutiert. Auch die ökonomische Fachliteratur hat sich in den letzten Jahren mehr und mehr mit Kryptowährungen befasst. Unter anderem wurde untersucht, ob es sich bei Bitcoins überhaupt um Geld im üblichen Sinne handelt (vgl. Yermack 2013) und ob Kryptowährungen einer staatlichen Regulierung bedürfen.¹ Angesichts des exponentiellen Kurswachstums (und rapiden Kursverfalls) wird auch die Gefahr der Blasenbildung vermehrt diskutiert. Der Aspekt der gesellschaftlichen Kosten der Kryptowährungen ist dabei bislang kaum beleuchtet worden. Häufig wird noch immer das idyllische Bild einer dezentralen, von vielen »Freiwilligen« erstellten Währung gezeichnet. Leider ist es aber komplett irreführend. Während das von den Zentralbanken hergestellte Bargeld nur relativ wenige Ressourcen verschlingt – einen Geldschein zu drucken, kostet eben fast nichts –, hat das Erzeugen der Bitcoins trotz seiner jungen Historie bis heute bereits rund 5 Mrd. US-Dollar gekostet.

Um die gesellschaftlichen Kosten der Bitcoinerzeugung zu verstehen, ist eine kurze, zugegebenermaßen sehr schematische Darstellung der Funktionsweise des Bitcoin-Mining vonnöten.² Dabei geht es im Folgenden nicht um den Handel von Bitcoins, sei es zu Transaktionszwecken oder aus Anlagegründen. Denn die gesellschaftlichen Kosten der Kryptowährung ent-

stehen beim Mining, also bei der Entstehung neuer Bitcoins. Wie kommen neue Bitcoins in die Welt? Bitcoins sind letztendlich eine lange Zeichenkette bzw. eine Textdatei. Jede Überweisung eines Bitcoins von einer Person an eine andere Person wird in dieser Textdatei (»Blockchain«) unveränderlich festgeschrieben. Um diese Textdatei gegen Manipulationen zu sichern, wird ein Prüfwert (»Hash«) erzeugt. Diesen Prüfwert zu ermitteln, ist rechentechnisch aufwendig. Tausende, inzwischen meist hochspezialisierte Computerfarmen weltweit konkurrieren darum, als erste den nächsten gültigen Prüfwert zu erzeugen. Das Bitcoinsystem ist dabei so angelegt, dass der Schwierigkeitsgrad für die Ermittlung des Prüfwertes steigt, je mehr Rechenkapazität weltweit auf die Ermittlung des Prüfwertes verwandt wird. Im Mittel wird die Blockchain sechs Mal pro Stunde verlängert, so dass sechs Prüfwerte pro Stunde erzeugt werden müssen.³

Welchen Anreiz haben die Miner – also alle, die versuchen einen solchen Prüfwert zu finden –, Arbeitszeit, Energie und Kapital in Form leistungsstarker Rechnerfarmen in diesen Suchprozess zu investieren? Der erste Miner, dem es gelingt, einen neuen Prüfwert zu erzeugen und damit der Blockchain einen neuen Block hinzuzufügen, erhält eine Entlohnung in Form von Bitcoins. Alle anderen Miner, die zeitgleich ebenfalls auf der Suche nach dem neuen Prüfwert waren, gehen leer aus. Diese Entlohnung sinkt im Zeitverlauf. Für die ersten 210 000 Blöcke betrug die Entlohnung jeweils 50 Bitcoins pro Block, für die nächsten 210 000 Blocks war die Entlohnung 25 Bitcoins usw., d.h. nach 210 000 Blöcken halbiert sich jeweils die Entlohnung.

* Prof. Dr. Marcel Thum ist Leiter der ifo Niederlassung Dresden und Inhaber des Lehrstuhls für Finanzwissenschaft an der Technischen Universität Dresden.

¹ Siehe hierzu, aber auch zur Frage der Geldeigenschaften von Bitcoins diverse Beiträge im ifo Schnelldienst 22/2017 (Thiele et al. 2017).

² Für weiterführende Darstellungen, bei denen es z.B. auch um Fragen der Kryptosicherheit und des Betrugs geht, vgl. Velde (2013) oder Kroll et al. (2013).

³ Hierfür muss aus der neuen Blockchain ein Hashwert gebildet werden, der unter einem festgelegten Grenzwert liegen muss. Der Grenzwert wird immer so angepasst, dass bei gegebener Zahl von Rechenkapazität aller Miner (also alle, die versuchen, einen solchen Hashwert zu finden), im Durchschnitt pro Stunde sechs neue Blocks erfolgreich hinzugefügt werden können.

Die Entlohnung eines zum Zeitpunkt t erfolgreichen Miners beträgt in Bitcoins $R(t)$. Diese Entlohnung hat zum Zeitpunkt t einen Marktwert von $p(t) \cdot R(t)$, wobei p den aktuellen Bitcoinpreis in Dollar angibt. Die Intensität des Minings lässt sich durch die durchgeführten Rechenoperationen ausdrücken, mit denen die Miner versuchen, einen passenden Prüfwert zu ermitteln. Sei m_i die Zahl der Rechenoperationen, die Miner i in einer Periode durchführt. Dann lässt sich die Wahrscheinlichkeit für den Miningenerfolg von Miner i schreiben als $\frac{m_i}{m_i + \sum_{j \neq i} m_j}$. Damit ergibt sich der erwartete Gewinn eines Miners als

$$E\pi_i = \frac{m_i}{m_i + \sum_{j \neq i} m_j} \cdot p \cdot R - c \cdot m_i - C,$$

wobei c die variablen Kosten je Rechenoperation (z.B. Energiekosten) und C die Fixkosten des Mining sind.

Gewinnmaximierung des Miners i bei gegebenem Verhalten der übrigen Miner verlangt

$$\frac{\partial E\pi_i}{\partial m_i} = \frac{\sum_{j \neq i} m_j}{(m_i + \sum_{j \neq i} m_j)^2} \cdot p \cdot R - c = 0.$$

Befinden sich insgesamt n Miner im Markt, ergibt sich bei Symmetrie ($m_i = m_j$) als gleichgewichtige Aktivität jedes einzelnen Miners:

$$m_i^* = \frac{n-1}{n^2} \cdot \frac{p \cdot R}{c}.$$

Damit lässt sich der gleichgewichtige Gewinn eines repräsentativen Miners mit

$$E\pi_i^* = \frac{p \cdot R}{n^2} - C,$$

schreiben. Da der Marktzutritt frei ist, sollten so lange Unternehmen in den Markt eintreten, bis die Gewinne wegkonkurriert sind ($E\pi_i^* = 0$). Die Zahl der Miner beträgt damit

$$n^* = \sqrt{\frac{p \cdot R}{C}};$$

Die Zahl der Miner steigt im Wert der Entlohnung und sinkt mit den Fixkosten. Der entscheidende Punkt ist: Da jeder Miner im Erwartungswert Nullgewinn erzielt, entsprechen die Kosten des Mining zu jedem Zeitpunkt dem Wert der neu geschaffenen Bitcoins, egal wie sich der Wert der Bitcoins entwickelt.

Die gesellschaftlichen Kosten des weltweiten Mining lassen sich unter Zuhilfenahme ökonomischer Theorie ermitteln. Der Wettbewerbsprozess unter den Minern ähnelt einem Rent-Seeking-Wettbewerb, wie ihn Tullock (1967) in die Literatur eingeführt hat.⁴ Beim Rent Seeking müssen alle Teilnehmer am Wettbewerb echte Ressourcen aufwenden, um eine Chance auf den Gewinn eines Preises zu haben. (Im üblichen Marktwettbewerb werden dagegen langfristig nur diejenigen Hersteller Ressourcen aufwenden, die ihre Produkte auch am Markt absetzen können; die weniger erfolgreichen Unternehmen scheiden dagegen aus und wenden auch keine Ressourcen mehr auf.) Letztendlich ist Rent Seeking verschwenderisch, weil die Aufwendungen der Verlierer im Wettbewerb umsonst waren.

Das Tullock'sche Modell des Rent Seeking zeigt nun, dass die gesamten Aufwendungen mit der Zahl der Teilnehmer am Wettbewerb steigen und dass – bei freiem Markteintritt – der Aufwand aller Teilnehmer dem zu gewinnenden Preis entspricht. Der Preis, um den die Miner konkurrieren, ist der aktuelle Wert der Bitcoins, die für den ersten erfolgreich gebildeten Prüf-

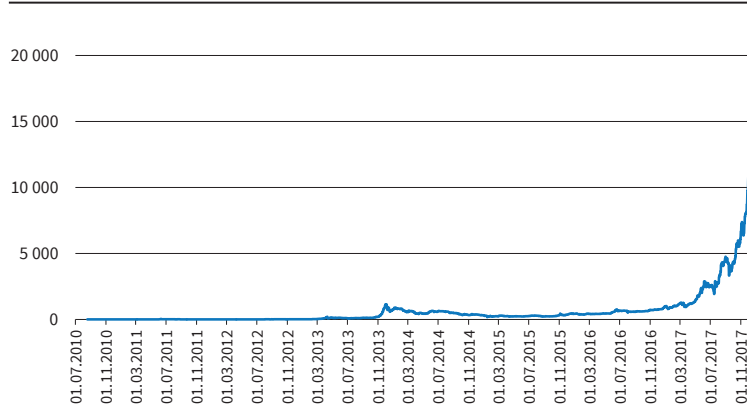
wert ausgezahlt werden. Das Tullock-Modell impliziert, dass man die Kosten des Bitcoin-Mining über den Wert der neu geschaffenen Bitcoins ermitteln kann. Egal wie sich der Wert der Bitcoins entwickelt, entsprechen die Kosten des Mining zu jedem Zeitpunkt dem Wert der neu geschaffenen Bitcoins. Jeder einzelne Miner kann zwar versuchen, seine Kosten zu senken, z.B. indem er seine Rechnerfarm in Regionen mit niedrigem Energiepreis wie z.B. in Island ansiedelt. Am Gesamtergebnis ändert das aber nichts, weil die gesunkenen Energiekosten gesamtwirtschaftlich von den erhöhten Rechenaktivitäten und neuen Konkurrenten aufgefressen werden. (Eine Skizze des formalen Modells findet sich in der Box.)

Um die Gesamtkosten des Bitcoin-Mining zu errechnen, ermitteln wir für jeden Tag den Wert der neugeschöpften Bitcoins. Dieser Wert ergibt sich aus dem aktuellen Bitcoinpreis multipliziert mit der Zahl der neu geschaffenen Bitcoins. Abbildung 1 zeigt die Preisentwicklung der Bitcoins seit August 2010 in laufenden US-Dollar. Das Bitcoinsystem wurde zwar schon im Januar 2009 ins Leben gerufen, konsistente Preisdaten liegen aber erst später vor. (Angesichts des anfänglich geringen Preises dürfte der Fehler durch die fehlenden Preisdaten gering sein.) Für Tage ohne Preisnota-

⁴ Für einen Überblick zu Rent-Seeking-Wettbewerben (vgl. Nitzan 1994).

Abb. 1

Bitcoinkurs
In US-Dollar



Quelle: <https://blockchain.info>.

© ifo Institut

tion ab August 2010 wurde immer der letzte verfügbare Preis konstant gehalten.

Wie die Abbildung zeigt, verharrte der Bitcoinkurs lange Zeit auf beinahe konstant niedrigem Niveau. Erst Mitte 2016 setzte der rapide Kursanstieg ein.

Wie bereits erwähnt bekamen die Miner für jeden der ersten 210 000 geschaffenen Blöcke jeweils 50 Bitcoins als Entlohnung. Am 28. November 2012 sank die Entlohnung auf 25 Bitcoins. Seit dem 10. Juli 2016 werden nur noch 12,5 Bitcoins als Entlohnung bezahlt. Durch die Kombination aus Entlohnung und tagesak-

Tab. 1

Barwertkosten des Bitcoin-Mining in Mrd. US-Dollar

Diskontierungssatz	2 %	4 %	6 %
Barwertkosten	5,123	5,267	5,417

Quelle: Berechnungen des ifo Instituts.

tuellem Bitcoinkurs lassen sich für jeden Tag bis zum 31. Dezember 2017 die Werte der neu geschöpften Bitcoins und damit die Kosten der Bitcoin-Generierung ermitteln.⁵ Diese Werte werden dann auf den 1. Januar 2018 aufdiskontiert und aufsummiert.

Tabelle 1 zeigt den Barwert dieser Kosten für alternative Diskontierungssätze. Bei einem Zins von 4% entspricht der Gegenwartswert aller Kosten für die Schaffung von Bitcoins 5,3 Mrd. US-Dollar. Zwar erzielen einzelne Miner einen Gewinn, weil sie erfolgreich Hashes erzeugen konnten und der Wert der erhaltenen Bitcoins die eigenen Kosten übersteigt. Aber dafür hatten andere Miner kein Glück, tragen aber die Kosten, weil

⁵ Außer der hier diskutierten Honorierung für erfolgreiche Prüfwerte gibt es auch eine Entlohnung in Form von Transaktionsgebühren, die hier aber für die Kalkulation der Kosten des Bitcoin-Mining ignoriert werden.

sie erfolglos Rechenkapazität installiert und dafür Strom, Arbeitskraft, Rohstoffe etc. verbraucht haben. Allein der Energieverbrauch, der nur einen Teil der Kosten ausmacht, beträgt 259 KWH pro Bitcointransaktion – genug um einen US-Haushalt mehr als eine Woche lang mit Strom zu versorgen (vgl. <https://digiconomist.net/bitcoin-sustainability-report-12-2017>).

Wie die Tabelle auch zeigt, spielt die Höhe des Diskontierungssatzes für den Barwert der Kosten keine allzu große Rolle. Der Ressourcenverbrauch liegt in allen Szenarien im einstelligen

Milliardenbereich. Neben den jüngst umfangreich diskutierten Problemen wie den Angriffen auf Bitcoin-Speicher und der Gefahr der Blasenbildung leidet das Bitcoin-System auch unter einer massiven Ressourcenverschwendung.

LITERATUR

Kroll, J.A., I.C. Davey und E.W. Felten (2013), »The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries«, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC, 11.–12. Juni 2013.

Nitzan, S. (1994), »Modelling Rent-Seeking Contests«, *Public Choice* 10, 41–60.

Thiele, C.-L., M. Diehl, Th. Mayer, D. Elsner, G. Pecksen, V. Brühl und J. Michaelis (2017), »Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?«, *ifo Schnelldienst* 70(22), 2017, 3–20.

Tullock, G. (1967), »The Welfare Costs of Tariffs, Monopolies, and Theft«, *Western Economic Journal* 5, 224–232.

Velde, F.R. (2013), »Bitcoin: A Primer«, *Chicago Fed Letter* No.317, Dezember.

Yermack, D. (2013), »Is Bitcoin a Real Currency? An Economic Appraisal«, NBER Working Paper 19747, Cambridge, MA.