

Was bedeutet eigentlich „Kryptowährung“?¹

Ingolf G. A. Pernice und Brett Scott

1. Definition

Eine Kryptowährung kann als System verstanden werden, das zur Ausgabe von Wertmarken („Token“) bestimmt ist, die als allgemeines oder begrenztes Tauschmittel verwendet werden sollen, und die über ein oft kollektiv geführtes digitales Verzeichnis unter Verwendung von Kryptographie verbucht werden, um das Vertrauen in Institutionen in unterschiedlichem Maße zu ersetzen. Vor diesem Hintergrund kann der singuläre Begriff Kryptowährung für eine Wertmarke stehen, die als allgemeines oder begrenztes Tauschmittel verwendet werden soll und über ein Kryptowährungssystem ausgegeben wird.

2. Ursprung und Entwicklung des Begriffs

Im öffentlichen Sprachgebrauch kam der Begriff Kryptowährung 2008 mit der Entwicklung von Bitcoin – ein Protokoll, das ein Netzwerk von Menschen, die über eine digitale Peer-to-Peer-Kommunikationsinfrastruktur miteinander verbunden sind, in die Lage versetzt, digitale Wertmarken auszugeben und sie untereinander zu übertragen, während der Prozess durch Kryptographie gesichert wird (Nakamoto 2008) – auf.

Während der ursprüngliche Vorschlag den Begriff Kryptowährung nicht verwendete, präsentierte Nakamoto das Projekt als Peer-to-Peer-„Währung“ in einer Netzwerk- und Kryptographie-Mailingliste (Nakamoto 2009). Der Begriff „Kryptowährung“ gewann jedoch bald in online-Unterhaltungen (vgl. HXN 2009) und Printmedien (z.B. Davis 2011) an Bedeutung.²

Früh wurde zwischen dem Protokoll – mit dem großgeschriebenen Begriff „Bitcoin“ – und den Wertmarken – mit dem kleingeschriebenen Begriff „bitcoin“ – unterschieden. Neue bitcoins werden von einem Netzwerkmitglied (einem so genannten „Schürfer“ oder „miner“) erzeugt, dem es gelungen ist, das Format eines Bündels („block“) von eingegangenen Überweisungsaufträgen bzw. Transaktionen (von zuvor ausgegebenen bitcoins; zusammen mit einer Anforderung auf Erhalt einer festgelegten Summe neu erzeugter bitcoins als Belohnung) zu ändern, so dass das Bündel („block“) an eine Kette („chain“) von zuvor bestätigten Bündeln angehängt werden kann („blockchain“).

Der Rest dieses Abschnitts versucht zu erklären, wie dieses Protokoll und unmittelbare Nachkommen den Begriff Kryptowährung geprägt haben könnten.

2.1. Die Rolle der Kryptographie in frühen Kryptowährungen

Der Wortstamm „Krypto“ innerhalb des Begriffs Kryptowährung könnte als Surrogat für Kryptographie angesehen werden, könnte aber auch aus der Cypherpunk-Bewegung hervorgegangen sein, die „anonymes Bargeld und andere privatsphäresichernde Zahlungssysteme“ (De Filippi & Wright 2018, S. 19) als wichtiges Werkzeug innerhalb einer Krypto-Anarchie betrachtete (Ludlow 2001, S. 4). Diese Zielsetzung hallt in der Mission Bitcoins, „kryptographische Beweise statt Vertrauen“ zu nutzen (Nakamoto 2008, S. 1) wider. Die genauen Protokollspezifikationen von Bitcoin und seinen Nachkommen sind in Tschorsch und Scheuermann (2016) zusammengefasst. Kryptographie taucht auf verschiedene Weise in ihrer Architektur auf. Einige Beispiele sind Integrität von und Konsens über eine(r) gemeinsame(n) Transaktions-Historie sowie die Autorisierungsprozedur für das Senden von Wertmarken. Die Verwendung des Surrogats „Krypto“ für Bitcoin ist jedoch insofern etwas willkürlich, als frühere Versuche zur Schaffung digitaler Formen offizieller Währungen (z.B. Chaum 1988) ebenfalls stark auf kryptographischen Techniken beruhten. Dennoch mag es gerechtfertigt erscheinen, da die Kryptographie für Bitcoin eine weitaus zentralere Rolle spielt als für nationale Währungen.

2.2. Monetäre Merkmale früher Kryptowährungen

Moderne Geldsysteme offizieller Landeswährungen bestehen, abstrakt gesprochen, aus physischen und digitalen Krediten – ausgegeben von staatlichen Zentralbanken, Münzämtern und privaten Geschäftsbanken als Emittentinnen – die unter einem Rechtssystem zirkulieren, das ihre Einlösung garantiert. Die Anzahl der Kredite erweitert sich durch deren Emission, danach können sie im Zuge ihres Umlaufs zwischen den Benutzer:innen übertragen werden, bevor sie bei der Kreditrückzahlung an die Emittentinnen wieder eingezogen werden. Dieses zusammengesetzte System aus expansions- und kontraktionsfähigen Krediten nennen wir im alltäglichen Sprachgebrauch „Geld“. In diesem Zusammenhang ist der Begriff Kryptowährung umstritten, da der Name von Anfang an die Annahme trifft, dass es sich bei den Wertmarken um Geld handelt. Die Kontroverse wird durch die Tatsache verstärkt, dass Enthusiast:innen den Begriff auch performativ verwenden, um normativ klarzustellen, dass Krypto-Wertmarken „Geld sein sollten“ oder – alternativ – um zu leugnen, dass das, was wir derzeit „Geld“ nennen, tatsächlich Geld ist.

Eine Strategie, diese Sprachpolitik zu entschärfen, besteht darin, die Annahme, die Wertmarken seien Geld, zunächst wegzulassen, indem man ihnen den generischen Namen Krypto-Wertmarken gibt und dann ihre unumstrittenen Eigenschaften auflistet, um sie mit Geld in offizieller Landeswährung zu vergleichen.

Wertmarken früher Kryptowährungen sind Datenobjekte, die durch Buchführung erstellt wurden, ähnlich wie das Eintippen der Zahl „1“ das mentale Bild eines „Dings“ erzeugt. Diese werden als „Wertmarken“ bezeichnet, aber es sind „leere Wertmarken“. Ein Beispiel für eine leere Wertmarke in der physischen Welt könnte ein durchsichtiger Plastik-Chip ohne Beschriftung oder Rechte sein. Bitcoin-Wertmarken sind in ähnlicher Weise leere Zeichen, ähnlich wie das digitale Äquivalent von leeren physischen Wertmarken, jedoch mit strengen Angebotsbeschränkungen.³

Diese leeren digitalen Wertmarken werden jedoch mit einem Namen und einem Markenlogo beworben, das ihnen als geistiges Bild dient, ohne welches sie fast vollständig funktionslos wären. Die Wertmarken können als digitale Inhaberpapiere bezeichnet werden, in dem Sinne, dass Übertragungen nur durch Besitz eines privaten Schlüssels initiiert werden können, der einen „noch nicht verbrauchten Transaktionsoutput“ freischalten kann. Ihre „Inhaberpapier-ähnliche“ Eigenschaft ist ein Grund, warum Kryptowährungen manchmal als „digitales Bargeld“ bezeichnet werden (physisches Bargeld ist die Form eines Inhaberpapiers in offizieller Landeswährung). Die Wertmarken können zirkulieren – Bitcoin und einige seiner Nachkommen verarbeiten täglich Hunderttausende von Wertmarken-Transfers (vgl. Hileman und Rauchs 2017). Darüber hinaus haben sie einen in der offiziellen Landeswährung gemessenen Marktpreis und ihre Wertmarken können in kleinere Stücke geteilt oder zu größeren zusammengefasst werden. Die Tatsache, dass teilbare und kumulierbare Wertmarken mit einem Kurs in offizieller Landeswährung bewegt werden können, verleiht dem System ein „geldähnliches“ Gefühl und – unter Annahme einer weiten Definition von Geld als „etwas, das im Zusammenhang mit dem Handelsverkehr ausgegeben und bewegt wird“ – fühlt sich der Begriff Kryptowährung im Alltagsgebrauch vage plausibel an.

Die meisten „Käufe“ mit Bitcoin- Wertmarken erfolgen jedoch in Form von Kompensationsgeschäften. Die Wertmarke, die in offizieller Landeswährung bewertet wird, wird mit einer Ware oder Dienstleistung verglichen, die in offizieller Landeswährung bewertet wird, und aus diesem Vergleich zweier Preise in offizieller Landeswährung ergibt sich ein Umtauschverhältnis zwischen der Wertmarke und dem Gut oder der Dienstleistung. Dies ist das konzeptionelle Äquivalent der Überlagerung eines Paares von Zwei-Weg-Transaktionen in offizieller Landeswährung und der Aufhebung der Geldströme, wodurch im Ergebnis der Eindruck entsteht, dass das Krypto-Wertzeichen als „Geld“ verwendet wird, um ein Gut oder einen Dienst zu „bezahlen“.

Nichtsdestotrotz wird Bitcoin hauptsächlich für Spekulationszwecke verwendet (Baur et al. 2018) – der Kauf der Wertmarke in offizieller Landeswährung geschieht mit der Absicht, sie bei Kursanstieg gegen die offizielle Landeswährung wieder zu verkaufen – und nicht für den Gegenhandel („Bezahlen“) von Waren und Dienstleistungen. Diese Spekulation (vgl. u.a. Yermack 2015; Glaser et al. 2014; oder Cheah 2015) treibt die Volatilität des in offizieller Landeswährung bemessenen Preises der Wertmarke an, was – wenn man sie durch die von ökonomischen Lehrbüchern favorisierte Betrachtung der konventionellen „Funktionen des Geldes“ analysiert (Geld als Tauschmittel, Wertaufbewahrungsmittel und Recheneinheit) – Probleme für die „Geld-heit“ der Wertmarken aufwirft. Ihnen fehlt nicht nur die allgemeine Akzeptanz im Austausch für Waren und Dienstleistungen, sie werden auch nicht häufig verwendet, um Dinge zu bepreisen, und Versuche, Preise in Krypto anzugeben, sind nicht intuitiv (Yermack 2015).⁴

Darüber hinaus haben Kryptowährungen Schwächen, anhaltend „Wert zu speichern“, wenn wir dies so interpretieren, dass die Wertmarken „eine stabile Kaufkraft behalten“ sollen (was im Fall von Bitcoin bedeutet, einen unveränderten Preis in offizieller Landeswährung und im Waren-Gegenwert zu behalten). Einfach ausgedrückt, während eine Person im Allgemeinen abschätzen kann, wie viele Päckchen Zucker sich für 100 US-Dollar in einem Monat kaufen lassen, wird sie sich unsicher sein, wie viel Zucker sie in einem Monat durch Bitcoin-Kompensationsgeschäfte erwerben kann.

3. Derzeit mit dem Begriff verbundene Fragen

Neben den obigen Debatten über die Gültigkeit der ursprünglichen Verwendung des Begriffs Kryptowährung wurde der Begriff durch Weiterentwicklungen bei neueren Generationen von Kryptowährungssystemen aufgeweicht. Die Rolle der Kryptographie und der „Geld-heit“, die durch die verschiedenen Wertmarken-Designs impliziert wird, variiert erheblich und wird im Rest des Abschnitts erörtert.

3.1. Die Rolle der Kryptographie in heutigen Kryptowährungen

Eine aus technischer Sicht sinnvolle Klassifizierung von Projekten bezieht sich auf die Zuordnung der Rechte zum Schreiben und Lesen von Transaktions-Aufzeichnungen. Peters et al. (2016) haben eine beliebte Kategorisierung eingeführt, mit der sich die zugrunde liegende Infrastruktur von Kryptowährungssystemen entlang der Dimensionen „public vs. private“ und „permissioned vs. permissionless“ (i.e. mit bzw. ohne Zugriffsbeschränkung) klassifizieren lässt. In public, permissionless-Systemen kann im Prinzip jeder:r Teilnehmer:in (Knoten) im Netzwerk Transaktionen lesen und in das Register schreiben. Bei public permissioned Systemen können nur autorisierte Knoten schreiben. In private permissioned Systemen ist sogar das Lesen auf autorisierte Knoten beschränkt. Je stärker ein System in seiner zugrunde liegenden Infrastruktur privat und an Erlaubnis geknüpft ist, desto weiter ist es von der Cypherpunk-Vision entfernt.

Ein Beispiel für einen Entwicklungstrend, der dem archetypischen Krypto-Ziel treu bleibt, Vertrauen durch kryptographische Beweise zu ersetzen (vgl. Nakamoto 2008; Genkin et al. 2018), sind auf Schutz der Privatsphäre ausgerichtete so genannte „Privacy Coins“ (z.B. Zcash, o.J.; Monero, o.J.). Sie sind eng mit archetypischen Kryptowährungen verwandt und übernehmen ihren öffentlichen beschränkungsfreien Aufbau von Lese- und Schreibrechten auf dem Register. Als „alternative Kryptowährungen, die mit dem Ziel entwickelt wurden, stärkere Datenschutzgarantien als Bitcoin zu bieten“ (Genkin et al. 2018), erhöhen sie den Einsatz von Kryptographie sogar noch, um Anonymität besser gewährleisten zu können. Als Folge ihrer Fokussierung auf die Privatsphäre führen sie jedoch zu zunehmenden Bedenken in Bezug auf Geldwäschebekämpfung und Strafverfolgung (vgl. Tziakouris 2020; Ferrari 2020).

Der wesentliche Trend bestand jedoch eher darin, die zentrale Rolle der Kryptographie in den jeweiligen Implementierungen zu verringern. Es kamen sogar Zahlungssysteme auf, die zwar von Konzernen betrieben aber immer noch als Kryptowährungen bezeichnet werden.⁵

Eyal (2017, S. 39) kommt zu dem Schluss: „wenn die Teilnehmenden der jüngsten Blockchain-Veranstaltungen auch nur in irgendeiner Weise als Indikator gelten können, haben Kryptowährungen die Aufmerksamkeit des Mainstream-Finanztechnologiesektors (FinTech) auf sich gezogen“. Als traditionelle Unternehmen begannen, mit der von Bitcoin inspirierten Technologie zu experimentieren, änderten sich die Systemanforderungen – und damit auch die jeweiligen Sicherheitsaspekte und die Verwendung von Kryptographie. Das wirtschaftliche Design dieser stärker zentralisierten Zahlungssysteme führte zu einem gewissen Grad zur Wiedereinsetzung vertrauenswürdiger Drittparteien oder Vermittlungsinstanzen für die Wertmarken-Schaffung.

Während sich viele neuartige Kryptowährungen weit von den krypto-anarchistischen Wurzeln archetypischer Wertmarken-Designs entfernt haben, spielt die allgemeine Idee, das Vertrauen in Institutionen oder deren interne Steuerungsmechanismen durch Kryptographie zu ersetzen, immer noch eine Rolle bei allen Kryptowährungs-Designs. Da jedoch selbst bei Banküberweisungen in offizieller Landeswährung aus Sicherheitsgründen Kryptographie verwendet wird, sollte der bloße Einsatz von Kryptographie nicht allein zur Definition von Kryptowährungen herangezogen werden.⁶

3.2. Monetäre Eigenschaften heutiger Kryptowährungen

Frühe Kryptowährungen hatten die erklärte Absicht, „digitales Bargeld“ oder eine Währung zu schaffen (siehe Abschnitt 1.1.). Das Aufkommen verschiedenster Formen von Krypto-Wertmarken hat dieses Verständnis jedoch aufgeweicht. Nicht alle Entwicklungsstränge zielen auf Allzweck-Geldzeichen ab.

First-Layer-Wertmarken (z.B. Ether), die so genannten „Smart Contract“-Plattformen⁷ (z.B. Ethereum) zugrunde liegen, und informell sogar Second-Layer-Wertmarken (Wertmarken, die an die jeweilige Plattform gebunden sind) werden zwar als Kryptowährungen bezeichnet, existieren allerdings vorrangig um die jeweiligen Smart Contracts zu aktivieren, anstatt eine allgemeine Zahlungslösung für Waren und Dienstleistungen bereitzustellen (siehe Bartoletti 2017). Als Smart Contract wird ein ausführbarer Computercode bezeichnet, der z.B. auf einer Blockchain läuft, um Vereinbarungen zwischen zwei Parteien zu schließen und zu vollstrecken, ohne Beteiligung vertrauenswürdiger Vermittlungsinstanzen oder wechselseitiges Vertrauen (Alharby et al. 2017). Nichtsdestotrotz kann dieser Fokus auf einen „eingeschränkten Zweck“ insofern eine Stärke sein, als dass die Aktivierung von Smart Contracts als echte Dienstleistung angesehen werden kann, die über den Besitz der Wertmarke zugänglich ist, Hierdurch werden die Wertmarken in der „realen Wirtschaft“ „verankert“, wenn auch im Cyberspace.

Aber auch die Klasse der Allzweck-Wertmarken ist durch Veränderungen gekennzeichnet. Eine Reaktion auf die inhärente Instabilität der Kurse⁸ ursprünglicher Kryptowährungen war das Aufkommen von so genannten „Stable Coins“, die versuchen, das Problem der hohen Kaufkraftvolatilität von Bitcoin und seinen Nachkommen zu lösen (Pernice 2019). Stable Coins sind wertmäßig an offizielle(n) Landeswährungen gekoppelt oder in irgendeiner Weise mit Vermögenswerten „gedeckt“, die in der offiziellen Landeswährung bepreist sind. Sie sind somit keine „leeren“ Zeichen mehr und weisen einen Bezugspunkt auf, der leichter einzuschätzen und zu kommunizieren ist. Es gibt sehr unterschiedliche Arten von Stable Coins, und verschiedenste Klassifizierungsversuche, um verschiedene Stabilisierungstechniken auf einen abstrakten Nenner zu bringen (z.B. Bullmann et al. 2019; Pernice et al. 2019; Moin et al. 2020; Sidorenko 2019; Clark et al. 2020). Eine nationale Währung kann „tokenisiert“ (also als digitale Wertmarke auf einer Blockchain abgebildet) werden, indem ein digitales Versprechen dafür auf einem Blockchain-System emittiert wird. Solche tokenisierten Gelder könnten tatsächlich als „neue Form von elektronischem Geld“ (Blandin et al. 2019) gesehen werden, die unter die entsprechenden Vorschriften für E-Geld, Anti-Geldwäsche- und Anti-Terrorfinanzierungsvorschriften fallen. Dies könnte „Geldeigenschaft“ zumindest aus rechtlicher Sicht gewährleisten. Bei komplexeren Stable Coin-Designs ist die Rechtslage nicht immer klar. Aus wirtschaftlicher Sicht könnte ihre Kaufkraftstabilität dazu beitragen, dass sie in

Zukunft als Geld genutzt werden könnten. Stable Coins haben jedoch vorerst noch keine allgemeine Akzeptanz im Einzelhandel erfahren (Bullmann et al. 2019).

5. Schlussfolgerungen

Viele wissenschaftliche Veröffentlichungen gehen davon aus, dass der Begriff Kryptowährung allgemein bekannt ist oder skizzieren ihn allenfalls grob.⁹

Unserer Studie hingegen folgt der Begriffsentwicklung beginnend mit Bitcoin, um zu definieren, was heute unter Kryptowährungen verstanden wird. Der Neologismus „Kryptowährung“ ist in seiner Bedeutung unstetig und wird auf Systeme mit unterschiedlichen technischen Architekturen und Steuerungssystemen angewendet. Dennoch besteht eine Vereinheitlichungsmöglichkeit für die unterschiedlichen Begriffsverwendungen darin, ihn durch eine gemeinsame Absicht derjenigen zu definieren, die ihn beanspruchen, und nicht durch die verschiedenen Mittel, mit denen diese Absicht umgesetzt wird, und unabhängig davon, ob die Absicht in der Praxis erreicht wird. Wir stellen fest, dass Kryptowährungssysteme die Absicht gemeinsam haben, ein allgemeines oder begrenztes Tauschmittel, eine Kryptowährung, bereitzustellen, wobei eine Infrastruktur verwendet wird, die das Vertrauen in Institutionen in unterschiedlichem Maße durch Kryptographie ersetzt.

Um den Begriff im öffentlichen Diskurs nützlicher zu machen, sollte der Begriff „Kryptowährung“ mit spezifizierenden Angaben zu den jeweiligen wirtschaftlichen (z.B. Bullmann et al. 2019; Pernice et al. 2019; Moin et al. 2020; Clark et al. 2020), steuerungstechnischen (z.B. Ziolkowski et al. 2020; Beck et al. 2018; Hacker 2019) und technologischen (z.B. Cachin und Vukoli 2017; Peters et al. 2016) Merkmalen des jeweiligen Systems gekoppelt werden.

Anmerkungen

- 1 Eine frühere Version dieses Artikels erschien ursprünglich in englischer Sprache in Internet Policy Review, DOI: 10.14763/2021.2.1561
- 2 Eine online-Suche bei Google Trends und Google Ngrams ergab, dass der Begriff Kryptowährung vor der Einführung von Bitcoin nicht verwendet wurde.
- 3 Es gilt dabei zu beachten, dass sich der Begriff einer „leeren Wertmarke“, eines Tokens, eines Chips oder einer Münze hier eher auf die wirtschaftliche Intuition als auf die technische Umsetzung bezieht. In Bitcoin und seinen Nachkommen existieren keine „Münzen“, sondern nur Transaktionsoutputs, Datenketten, die übertragbar und beliebig teilbar sind.
- 4 Umrechnung der Preise üblicher Konsumgüter in z.B. Bitcoin führt zu Angaben in kleinen Dezimalzahlen.
- 5 Vgl. z.B. Facebooks Projekt „Diem“ (o.J.) und sein Echo in den Medien (Popper und Isaac 2020).
- 6 Man hätte sich auch auf das einende Element „Blockchain-Technologie“ stützen können (das für die kryptographischen Werkzeuge einer Kryptowährung stehen könnte). Da dieser Begriff jedoch ähnlich unklar und vage ist wie der zu definierende Begriff, haben wir dies unterlassen.
- 7 Eine Zusammenfassung der Forschung zu Smart-Contract-Plattformen findet sich in Macrinici et al. (2018), während Bartoletti et al. (2017) und Alharby et al. (2017) verschiedene Plattformen untersuchen.
- 8 Denn im Gegensatz zu offiziellen Währungen fehlt dezentralen Kryptowährungen in der Regel eine Instanz oder ein Mechanismus, der für die erforderliche Anpassung des Angebots an Wertmarken bzw. der Zugangsbedingungen an die veränderliche Nachfrage verantwortlich ist, um ihren Marktwert zu stabilisieren.
- 9 Die Bedeutung des Begriffs „Kryptowährung“ wird kurz angerissen in White (2014), Lansky (2018), Aggarwal (2018), Chu et al. (2017), Sovbetov (2018) und Härdle et al. (2020).

Literatur

- Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017): Quantum attacks on Bitcoin, and how to protect against them. ArXiv. <https://arxiv.org/abs/1710.10377>
- Alharby, M., & Van Moorsel, A. (2017): Blockchain-based smart contracts: A systematic mapping study. *Computer Science & Information Technology*, 7(10), 1-6. <https://doi.org/10.5121/csit.2017.71011>
- Bartoletti, M., & Pompianu, L. (2017): An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns. In: M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, & M. Jakobsson (Hg.), *Financial Cryptography and Data Security* (pp. 494–509). Springer International Publishing. https://doi.org/10.1007/978-3-319-70278-0_31
- Baur, D. G., Hong, K., & Lee, A. D. (2018): Bitcoin: Medium of exchange or speculative assets? *Journal of International Financial Markets, Institutions and Money*, 54, 177–189. <https://doi.org/10.1016/j.intfin.2017.12.004>
- Beck, R., Müller-Bloch, C., & King, J. L. (2018): Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems*, 19(10). <https://aisel.aisnet.org/jais/vol19/iss10/1>
- Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., & Cloud, K. (2019): Global cryptoasset regulatory landscape study [Report]. Cambridge Centre for Alternative Finance, University of Cambridge. <https://econpapers.repec.org/RePEc:jbs:altfin:201904-gcrls>
- Bullmann, D., Klemm, J., & Pinna, A. (2019): In search for stability in crypto-assets: Are stablecoins the solution? (Paper No. 230; Occasional Paper Series). European Central Bank. <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf>
- Cachin, C., & Vukolić, M. (2017): Blockchain Consensus Protocols in the Wild (Keynote Talk). In: 31st International Symposium on Distributed Computing (DISC 2017) (pp. 1:1–1:16). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. <https://doi.org/10.4230/LIPIcs.DISC.2017.1>
- Chaum, D., Fiat, A., & Naor, M. (1988): Untraceable Electronic Cash. In S. Goldwasser (Ed.), *Advances in Cryptology—CRYPTO’88* (pp. 319–327). Springer. https://doi.org/10.1007/0-387-34799-2_25
- Cheah, E. T., & Fry, J. (2015): Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, 130, 32–36. <https://doi.org/10.1016/j.econlet.2015.02.029>
- Chu, J., Chan, S., Nadarajah, S., & Osterrieder, J. (2017): GARCH modelling of cryptocurrencies. *Journal of Risk and Financial Management*, 10(4), 17. <https://doi.org/10.3390/jrfm10040017>
- Clark, J., Demirag, D., & Moosavi, S. (2020): Demystifying Stablecoins: Cryptography meets monetary policy. *Queue*, 18(1), 39–60. <https://doi.org/10.1145/3387945.3388781>
- Davis, J. (2011, October 3): The crypto-currency. *The New Yorker*, 87. <https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>
- De Filippi, P., & Wright, A. (2018): *Blockchain and the law: The rule of code*. Cambridge, Massachusetts: Harvard University Press. <https://doi.org/10.2307/j.ctv2867sp>
- Diem. (o.J.): Retrieved 3 May 2021, from <https://www.diem.com/en-us/>
- Eyal, I. (2017): Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. *Computer*, 50(9), 38-49. <https://doi.org/10.1109/MC.2017.3571042>
- Ferrari, V. (2020): The regulation of crypto-assets in the EU – investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law*, 27(3), 325–342. <https://doi.org/10.1177/1023263X20911538>
- Genkin, D., Papadopoulos, D., & Papamanthou, C. (2018): Privacy in Decentralized Cryptocurrencies. *Communications of the ACM*, 61(6), 78–88. <https://doi.org/10.1145/3132696>
- Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014, June 7): Bitcoin-asset or currency? Revealing users’ hidden intentions. ECIS 2014 Proceedings. European Conference on Information Systems. <https://aisel.aisnet.org/ecis2014/proceedings/track10/15>
- Hacker, P. (2019): Corporate Governance for Complex Cryptocurrencies?: A Framework for Stability and Decision Making in Blockchain-Based Organizations. In P. Hacker, *Regulating Blockchain* (pp. 140–166). Oxford University Press. <https://doi.org/10.1093/oso/9780198842187.003.0008>
- Härdle, W. K., Harvey, C. R., & Reule, R. C. G. (2020): Understanding Cryptocurrencies. *Journal of Financial Econometrics*, 18(2), 181–208. <https://doi.org/10.1093/jfinc/nbz033>
- Hileman, G., & Rauchs, M. (2017): Global cryptocurrency benchmarking study [Report]. Cambridge Centre for Alternative Finance, University of Cambridge. <https://ideas.repec.org/b/jbs/altfin/201704-gcbs.html>
- HXN [B3AR]. (2009, September 24): This is really interesting: Bitcoin, the p2p cryptocurrency. [Http://bitcoin.sourceforge.net/](http://bitcoin.sourceforge.net/) [Tweet]. @hxn. <https://twitter.com/hxn/status/4334116324>

- Lansky, J. (2018): Possible state approaches to cryptocurrencies. *Journal of Systems Integration*, 9(1), 19–31. <https://doi.org/10.20470/jsi.v9i1.335>
- Ludlow, P. (Ed.) (2001): *Crypto anarchy, cyberstates, and pirate utopias*. Cambridge, Massachusetts: MIT Press. <https://doi.org/10.7551/mitpress/2229.001.0001>
- Macrinici, D., Cartofeanu, C., & Gao, S. (2018): Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35(8), 2337–2354. <https://doi.org/10.1016/j.tele.2018.10.004>
- Moin, A., Sekniqi, K., & Sirer, E. G. (2020): SoK: A Classification Framework for Stablecoin Designs. In J. Boneau & N. Heninger (Eds.), *Financial Cryptography and Data Security* (pp. 174–197). Springer International Publishing. https://doi.org/10.1007/978-3-030-51280-4_11
- Monero. (o.J.): Monero Research Lab. Monero. <https://web.getmonero.org/resources/research-lab/>
- Nakamoto, S. (2008): Bitcoin: A peer-to-peer electronic cash system [White Paper]. <https://bitcoin.org/bitcoin.pdf>
- Nakamoto, S. (2009, February 11): Bitcoin open source implementation of P2P currency [Forum post]. P2P Foundation Post. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>
- Peters, G. W., & Panayi, E. (2016): Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In P. Tascia, T. Aste, L. Pelizzon, & N. Perony (Eds.), *Banking Beyond Banks and Money: A Guide to Banking Services in the Twenty-First Century* (pp. 239–278). Springer International Publishing. https://doi.org/10.1007/978-3-319-42448-4_13
- Pernice, I. G., Henningsen, S., Proskalovich, R., Florian, M., Elendner, H., & Scheuermann, B. (2019, June): Monetary stabilization in cryptocurrencies—design approaches and open questions. In 2019 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 47–59). IEEE. <https://doi.org/10.1109/CVCBT.2019.00011>
- Popper, N., & Isaac, M. (2020, April 16): Facebook-Backed Libra Cryptocurrency Project Is Scaled Back. *The New York Times*. <https://www.nytimes.com/2020/04/16/technology/facebook-libra-cryptocurrency.html>
- Sidorenko, E. L. (2019): Stablecoin as a New Financial Instrument. In S. I. Ashmarina, M. Vochozka, & V. V. Mantulenko (Eds.), *Digital Age: Chances, Challenges and Future* (pp. 630–638). Springer International Publishing. https://doi.org/10.1007/978-3-030-27015-5_75
- Sovbetov, Y. (2018): Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero. *Journal of Economics and Financial Analysis*, 2(2), 1–27. <https://mp.ra.uni-muenchen.de/85036/>
- Tschorsch, F., & Scheuermann, B. (2016): Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084–2123. <https://doi.org/10.1109/COMST.2016.2535718>
- Tziakouris, G. (2018): Cryptocurrencies—A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective. *IEEE Security & Privacy*, 16(4), 92–94. <https://doi.org/10.1109/msp.2018.3111243>
- White, L. H. (2015): The Market for Cryptocurrencies. *Cato Journal*, 35(2), 383–402. <https://ideas.repec.org/a/cto/journal/v35y2015i2p383-402.html>
- Yermack, D. (2015): Is Bitcoin a Real Currency? An Economic Appraisal. In D. Lee Kuo Chen (Ed.), *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 31–43). Academic Press. <http://doi.org/10.1016/b978-0-12-802117-0.00002-3>
- Zcash (o.J.): How it works. Zcash. <https://z.cash/technology/>
- Ziolkowski, R., Miscione, G., & Schwabe, G. (2020): Decision problems in blockchain governance: Old wine in new bottles or walking in someone else’s shoes? *Journal of Management Information Systems*, 37(2), 316–348. <https://doi.org/10.1080/07421222.2020.1759974>