1. Jg. | 29.10.2020 | Seiten 145–216 | www.rdz-online.de

Recht der Zahlungsdienste

3 . 2020

Betriebs-Berater Geldverkehr

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Von Bitcoin zu Libra und dem digitalen Euro: Technische Fortschritte von Blockchains und deren Implikationen auf digitale Währungen

Seit der Erfindung von Bitcoin im Jahr 2008 hat die Blockchain-Technologie eine bemerkenswerte Entwicklung zu verzeichnen. Spätestens durch die enormen Wertsteigerungen von Kryptowährungen Ende 2017 gibt es im privaten und öffentlichen Sektor intensive Bemühungen, ihre Potenziale zu verstehen und zu nutzen. Der nachfolgende Beitrag geht speziell auf den technischen Fortschritt von Blockchain-Technologie in den vergangenen Jahren ein und zeigt Implikationen für die Umsetzbarkeit digitaler Währungen auf.

Johannes Sedlmeir

Einleitung

Blockchain-Technologie ermöglicht eine Art dezentraler Buchführung. Im Falle von Kryptowährungen wie Bitcoin bedeutet dies, dass nicht eine zentrale Instanz, wie etwa eine Bank, die aktuellen Eigentumsverhältnisse an einer Sache dokumentiert, sondern dass stattdessen alle Teilnehmer an dem Währungssystem die Möglichkeit haben, eine synchronisierte Kopie des entsprechenden Kontenbuchs auf ihrem Rechner (node) zu führen und dabei über alle Veränderungen (Transaktionen) abzustimmen (Konsens) sowie diese selbst nachzurechnen und damit die Änderungen des Status quo zu prüfen (*Butijn/Tamburri/van den Heuvel*, ACM Computing Surveys 3/2020, 1–37). Dadurch ist Blockchain-Technologie auch jenseits des Finanzsektors relevant: Blockchain-Technologie kann technisch gesehen alle Funktionalitäten einer digitalen Plattform bereitstellen, ohne dabei jedoch auf einen einzelnen Betreiber dieser Plattform angewiesen zu sein. Die Abwicklung von Programmierlogik, die über eine einfache Bezahlung hinausgeht, nennt man dabei oft „Smart Contracts". Eine blockchainbasierte digitale Plattform ermöglicht die Nutzung der bekannten Vorteile digitaler Plattformen, wie bspw. Standardisierung, Kollaboration über Organisationsgrenzen hinweg und Netzwerkeffekte, ohne dass dabei eine Aggregation von Marktmacht bei einem Betreiber befürchtet werden muss (*Glaser/Hawlitschek/Notheisen*, in: Treiblmaier/Beck (Hrsg.), Business Transformation through Blockchain, 2019, S. 121–143).

Im Folgenden wird in erster Linie auf Anwendungen von Blockchain-Technologie für digitale Währungen eingegangen. Digitale Währungen kann man hinsichtlich vieler unterschiedlicher Dimensionen unterscheiden. Besonders im Fokus steht dabei der Grad an Dezentralität: Die Kontenbücher der bekanntesten Kryptowährungen, wie etwa Bitcoin oder Ether, werden mit Hilfe einer sog. öffentlichen, nicht zugangsbeschränkten Blockchain geführt. Dies bedeutet, dass jeder ohne Zustimmung einer dritten Partei das Kontenbuch synchronisieren und sich unter einem Pseudonym am Konsens beteiligen kann. Die Konsensfindung kann man sich wie eine Abstimmung darüber vorstellen, welche Transaktionen neu in das Kontenbuch aufgenommen werden. Da in einem nicht zugangsbeschränkten System aber keinerlei Kontrolle besteht, wer wie viele Pseudonyme anlegt, sollten die Stimmen nicht alle gleich gewichtet sein. Demnach muss das Gewicht der Stimme bei der Abstimmung an eine knappe Ressource gekoppelt werden – bei den ersten Blockchains wie Bitcoin war dies die aufzuwendende Rechenleistung (proof of work) bzw. elektrische Energie (daher auch der bekanntlich enorme Energiebedarf). Mittlerweile gibt es jedoch auch Verfahren, das Stimmgewicht an den Kapitalanteil, welchen man an der jeweiligen Kryptowährung besitzt, zu koppeln (proof of stake). Daneben existieren auch zugangsbeschränkte Netzwerke, die oft in Konsortien oder föderalen Strukturen eingesetzt werden. Da für zugangsbeschränkte Blockchains eine Registrierung nötig ist, können hier wahlbasierte Abstimmungsverfahren, in denen bspw. jede Organisation oder jeder Teilnehmer genau eine Stimme hat, verwendet werden (*Sedlmeir u. a.,* Business & Information Systems Engineering, 2020, S. 1–10). Als Beispiel ist hier Libra zu nennen; dort werden Unternehmen wie etwa Facebook selbst, Kreditkartenanbieter oder Banken die entsprechenden Nodes betreiben.

Eine besondere Art von digitalen Währungen sind sog. Stablecoins. Damit wird versucht, eine Alternative für volatile Kryptowährungen zu etablieren. Dies wird i. d. R. durch das Hinterlegen von Fiat-Währungen (wie bspw. US-Dollar für den Stablecoin Tether) oder einer anderen Kryptowährung (dann wegen deren zu erwartenden Wertschwankungen i. d. R. verbunden mit Über-

besicherung) erreicht. Hier stellt sich die Frage, ob eine dezentrale digitale Plattform angesichts des benötigten Vertrauens in eine Bank, die die entsprechenden Sicherheiten hält, noch sinnvoll ist (man denke an die Glaubwürdigkeit von Kontoauszügen im Fall von Wirecard). Aufgrund der steigenden Nachfrage nach Stablecoins und des damit verbundenen Ziels einer wertstabilen digitalen Währung untersuchen aktuell weltweit viele Zentralbanken, ob sie Einheiten ihrer jeweiligen Währung digital auf einer Blockchain verfügbar machen wollen. Digitale Zentralbankwährungen (central bank digital currencies – CBDC) stellen eine Verbindlichkeit der jeweiligen Zentralbanken (oder Geschäftsbanken) in Form von Einheiten einer Kryptowährung dar und vereinen somit den sicheren und wertstabilen Charakter einer von der Zentralbank emittierten Währung. Hier werden bereits ökonomische Implikationen von CBDC auf den Bankensektor und die Wirkungsweise klassischer Geldpolitik, gesellschaftliche Implikationen wie Governance, Inklusion und Risikoverteilung, sowie rechtliche Fragestellung, besonders hinsichtlich des Datenschutzes, Geldwäsche oder Terrorismusfinanzierung, analysiert (*Dell'Erba*, NYUJ Legis. & Pub. Pol'y 2019, 1).

Dieses Technikschlaglicht hat zum Ziel, die in den vergangenen Jahren erzielten technischen Fortschritte der Blockchain-Technologie näher vorzustellen. Es soll damit deutlich machen, dass aus technischer Sicht verschiedene Möglichkeiten bestehen, Kryptowährungen, private Stablecoins wie Libra und auch CBDC umzusetzen. Dies soll dem Leser die Möglichkeit geben, sich Gedanken über potenzielle rechtliche Fragestellungen für ein Kontinuum von Lösungen, von vollkommen zentral zu vollkommen dezentral und von vollkommen transparent hin zu hohem Datenschutz, machen zu können.

Bitcoin und die ersten Kryptowährungen

Die für die ersten Kryptowährungen wie Bitcoin oder Ether zugrunde liegenden Blockchains weisen – besonders hinsichtlich ihres Durchsatzes, d. h. der größtmöglichen Anzahl an Transaktionen pro Sekunde – eine überaus schlechte Performanz auf. Dafür verantwortlich sind der jeweilige Konsensmechanismus und die für Blockchains charakteristische redundante Ausführung aller Transaktionen: Der Einigungsprozess, welche Transaktionen neu hinzugefügt werden, ist für die Nodes mit Aufwand und Wartezeiten verbunden. Zum anderen erfordern das Prüfen, Verarbeiten und Speichern aller Transaktionen auf allen Nodes Rechenkapazität, Bandbreite und Speicherplatz. Gerade Letzteres ist in der Praxis eine starke Limitation – während bspw. ein Bitcoin-Node nur wenige Megabytes pro zehn Minuten an Downloadgeschwindigkeit erfordert und damit vergleichsweise wenig Bandbreite benötigt, ist die Bitcoin-Blockchain mittlerweile bereits mehrere hundert Gigabyte groß. Entsprechend benötigt ein Bitcoin-Node bereits so viel Speicherplatz, wie ein handelsüblicher Laptop zur Verfügung hat. In einem nicht zugangsbeschränkten System ist zudem üblicherweise ein hoher Grad an Dezentralisierung erwünscht – entsprechend dürfen die technischen Anforderungen an Nodes nicht allzu hoch sein. Daher können die Bitcoin- und Ethereum-Blockchain sowie allgemein Kryptowährungen zugrunde liegende Blockchains grundsätzlich nur einen geringen Durchsatz erreichen. Einige Blockchains, wie etwa Bitcoin Cash, haben die Blockgröße und damit auch den Durchsatz der Transaktionen in der Vergangenheit erhöht. Diskussionen zu dem Konflikt zwischen hohem Grad an Dezentralisierung und hohem Durchsatz werden seit Jahren kontrovers geführt (https://en.bitcoin.it/wiki/Block_size_limit_controversy, Abruf: 18.9.2020).

Die Redundanz der Operationen führt zudem zu Problemen hinsichtlich vertraulicher Daten. Zwar sind die Teilnehmer in Kryptowährungen üblicherweise pseudonymisiert; mit Zusatzinformationen, bspw. einem durchlaufenen KYC-Prozess bei einer Krypto-Börse, systematischen Untersuchungen von IP-Adressen oder anderen Informationsquellen gelingt es aber, vielen Pseudonymen die sich dahinter befindlichen Personen oder Organisationen zuzuordnen und entsprechend auch all deren Transaktionen inklusive Zeitpunkt, Absender, Empfänger und Betrag auszulesen (*Zhang*, ACM Computing Surveys 3/2019, 1–34). Dies ist nicht nur regulatorisch, sondern auch nach unserem gesellschaftlichen Verständnis hinsichtlich der Vertraulichkeit finanzieller Daten problematisch und führt dazu, dass Transaktionen mit Hilfe von Kryptowährungen auch für Unternehmen wenig attraktiv sind. Aus diesem Grund wurden Kryptowährungen entwickelt, bei denen mit Hilfe von kryptographischen Verfahren Kontostände und Beträge nicht offengelegt werden müssen, um die Korrektheit von Transaktionen zu überprüfen. Beispiele hierfür sind etwa Monero und Z-Cash. Diese stellen technisch gesehen zwar einen erheblichen Fortschritt dar, die Vertraulichkeit-Features werden aber wegen verbreiteter Unkenntnis über die Datenschutz-Problematik und auch Bedenken hinsichtlich krimineller Nutzungszwecke aktuell kaum eingesetzt. Zudem waren Performanz und Nutzerfreundlichkeit dieser Art von Transaktionen zunächst noch einmal deutlich schlechter als die normaler Transaktionen in gängigen Kryptowährungen.

Erste Ansätze zur Verbesserung von Performanz und Datenschutz

Aufgrund der genannten Hürden hinsichtlich Performanz und Datenschutz sowie weiterer regulatorischer Bedenken haben für viele Anwendungen von Blockchain-Technologie in Unternehmen oder dem öffentlichen Sektor zugangsbeschränkte Blockchains Einzug gehalten. Technologisch waren die Fundamente hierfür bereits Ende der 1990er Jahre gelegt, aber erst durch die Verbreitung von Kryptowährungen entstand eine Wahrneh-

mung für die Potenziale solcher Architekturen. Grundsätzlich können die Konsensmechanismen zugangsbeschränkter Blockchains bereits eine höhere Performanz als die der o. g. Kryptowährungen erreichen. Viel entscheidender ist aber, dass an von Unternehmen oder öffentlichen Einrichtungen betriebene Nodes wesentlich höhere Hardware- und Bandbreiteanforderungen gestellt werden dürfen. Entsprechend können mit zugangsbeschränkten Blockchains bis zu mehrere tausend Transaktionen pro Sekunde erreicht werden, was von der Größenordnung bereits der Anforderung an ein großes Zahlungsnetzwerk entspricht. Auch die Problematik der oft langen Bestätigungsdauer (Latenz/Finalität) kann in zugangsbeschränkten Blockchains wesentlich entschärft werden. Durch vertragsbasiertes Aufsetzen der Netzwerke und im Konsortium gesteuerte Governance sind diese zudem auch rechtlich einfacher einzuordnen. Zugangsbeschränkte Blockchains weisen darüber hinaus oft auch bereits in beschränktem Umfang zusätzliche Datenschutz-Features wie die integrierte Unterstützung von Off-Chain-Speicherung auf und sind schon durch die Beschränkung des Zugriffs nur durch registrierte Teilnehmer weniger problematisch für vertrauliche Daten von Nutzern oder Unternehmen. All diese Gründe haben vermutlich auch dazu geführt, dass etwa Libra trotz der ursprünglichen Ankündigung, langfristig ein nicht zugangsbeschränktes Blockchain-Netzwerk aufzubauen, von diesem Ziel zurückgetreten ist.

Zero-Knowledge Proofs für Vertraulichkeit und Durchsatz in nicht zugangsbeschränkten Blockchains

In den vergangenen Jahren gab es auf dem Gebiet der sog. Zero-Knowledge Proofs (ZKP), die theoretisch bereits seit den 1980er Jahren in der Informatik untersucht werden, auch aufgrund der durch Kryptowährungen entstandenen praktischen Anwendungspotenziale und des resultierenden ökonomischen Innovationsdrucks, enorme Fortschritte. ZKP erlauben es, die Korrektheit einer Berechnung zu beweisen, ohne alle Inputs, Outputs oder Zwischenschritte dokumentieren bzw. die Berechnung wiederholen zu müssen. Dies erklärt ihre Vorteile für das Ausführen vertraulicher und zugleich überprüfbarer Berechnungen auf einer Blockchain (*Zhang*, a. a. O.). Zudem haben ZKP die Eigenschaft, dass der Rechenaufwand für das Verifizieren des Korrektheitsbeweises signifikant kleiner ist als das Durchführen der ursprünglichen Berechnung, und dass die Beweise nur sehr wenig Speicherplatz in Anspruch nehmen. Somit ist es möglich, die Korrektheit einer komplexen Berechnung, die mehrere Minuten oder Stunden dauert, innerhalb weniger Millisekunden zu verifizieren – die Irrtumswahrscheinlichkeit kann dabei so klein gemacht werden, dass sie für alle praktischen Zwecke irrelevant ist. Bei der oben beschriebenen Blockchain Z-Cash werden ZKP für Beweise der Form „A überweist x Einheiten der Kryptowährung an B, wobei x nicht-negativ ist, A mindestens x besitzt, A die Überweisung mit einer digitalen Signatur autorisiert hat, und A die Einheiten der Kryptowährung nicht zuvor bereits ausgegeben hat“ eingesetzt, wobei weder x noch A und B (nicht einmal in Form ihrer Pseudonyme) offengelegt werden müssen. Damit werden vollständig anonyme und vertrauliche Transaktionen ermöglicht (s. etwa https://z.cash/technology/, Abruf: 18.9.2020). Auch in zugangsbeschränkten Blockchains innerhalb eines Konsortiums von Unternehmen werden ZKP bereits in der Praxis eingesetzt, bspw. in MediLedger. Hier wird in der Supply Chain von Pharmaunternehmen dokumentiert, dass nie mehr Medikamente verkauft werden, als zuvor eingekauft wurden, ohne die vertraulichen Mengen selbst oder die an dem Handel beteiligten Unternehmen preisgeben zu müssen.

Mittlerweile ist jedoch noch eine weitere, komplexere Verwendung von ZKP populär geworden: Der größte Teil des Speicherplatzes und Rechenaufwands von Nodes wird aktuell für das Abspeichern digitaler Signaturen bzw. deren Überprüfung verwendet. Statt die Transaktionen auf allen Nodes einzeln nachzurechnen und damit zu prüfen, kann nun in sog. zk-Rollups ein Koordinator eine große Zahl von Transaktionen sammeln, deren Gültigkeit prüfen und die daraus resultierende aggregierte Veränderung des Kontenbuchs berechnen. Dann schickt er dieses Update zusammen mit einem ZKP für die Korrektheit der aggregierten Veränderung an die Blockchain (genauer: an einen Smart Contract), wodurch der Beweis von allen Nodes geprüft wird. Da das Überprüfen des Beweises signifikant weniger Aufwand für die Nodes bedeutet als das Nachrechnen aller darin enthaltenen Transaktionen und bei dem auf der Blockchain abgespeicherten aggregierten Update auf digitale Signaturen verzichtet werden kann, bedeutet dies eine erhebliche Ersparnis von Rechen- und Speicherkapazität (nur der Koordinator benötigt für die Beweiserstellung hoch performante Hardware). Mit Hilfe von bereits heute auf der nicht zugangsbeschränkten Ethereum-Blockchain verfügbaren zk-Rollups können anstatt der üblichen ca. zehn Transaktionen pro Sekunde bis zu mehrere tausend Transaktionen pro Sekunde durchgeführt werden (s. etwa https://loopring.org/#/protocol oder https://zksync.io/faq/intro.html#zksync-in-comparison, Abrufe: 18.9.2020). Natürlich stellt dieses Vorgehen in gewisser Weise eine Zentralisierung dar: Im Gegensatz zu zahlreichen anderen in der Vergangenheit erprobten Verfahren, um den Durchsatz von Blockchains zu erhöhen (zu nennen sind hier bspw. Payment-Hubs oder das Lightning-Netzwerk) hat der Koordinator jedoch wegen des erforderlichen Korrektheitsbeweises nicht die Möglichkeit, Transaktionen zu fälschen und so etwa Einheiten der Kryptowährung ungerechtfertigt an sich zu nehmen, da sonst der Beweis von den anderen Nodes als fehlerhaft erkannt und die von ihm vorgeschlagene aggregierte Veränderung abgelehnt werden würde. Die Sicherheitsgarantien von Transaktionen, die mittels eines zk-Rollup durchge-

führt werden, entsprechen daher denen „normaler" Transaktionen. Bei genauerer Betrachtung gibt es auch bei zk-Rollups unterschiedliche Nuancen, und durch ein leichtes Reduzieren der Sicherheit in Form eines Verzichts auf die Verfügbarkeit aller Daten auf einer Blockchain kann der Durchsatz sogar noch einmal deutlich gesteigert werden.

Ausblick

Mit den beschriebenen Technologien ist es somit bereits heute möglich, vertrauliche Transaktionen und hohe Performanz auf zugangsbeschränkten Blockchains zu ermöglichen. Hier stehen somit technologisch alle Möglichkeiten offen, ein Blockchain-basiertes, digitales Währungssystem mit der erforderlichen Performanz und Vertraulichkeit zu ermöglichen. Bei nicht zugangsbeschränkten Blockchains muss man sich im Moment noch zwischen hoher Performanz und hoher Vertraulichkeit entscheiden, mittelfristig wird aber wohl auch die Kombination aus beidem verfügbar sein: Aktuell wird an der Kombination von vertraulichen Transaktionen und zk-Rollups geforscht – man nennt dies auch zk^2-Rollup, da dann der Koordinator nicht „normale" Transaktionen prüfen und aggregieren muss, sondern wiederum Beweise der Korrektheit einzelner, vertraulicher Transaktionen in Form von ZKP (s. *Walton-Pocock*, Aztec: Fast Privacy with ZK^2 Rollup, abrufbar unter https://medium.com/aztec-protocol/aztec-fast-privacy-with-zk%C2%B2-rollup-7c742f45457, Abruf: 18.9.2020). Unterdessen entstehen erste Plattformen, auf denen nicht nur vollkommene Transparenz oder vollkommene Vertraulichkeit von Transaktionen möglich ist, sondern beliebige Punkte in diesem Spektrum (s. etwa https://findora.org/, Abruf: 18.9.2020). Bspw. ist es mit Hilfe von ZKP konzeptionell möglich, sicherzustellen, dass von einem Absender monatlich nur Transaktionen unter insgesamt 10000 Euro vollkommen anonym zugelassen werden, und für Transaktionen oberhalb dieser Grenze das Vorhandensein eines KYC-Check, eine Überprüfung der Transaktion durch eine Bank oder die Garantie, dass Sender und Empfänger der Transaktion im selben Land gemeldet sind (ohne das Land selbst offenlegen zu müssen) einzufordern. So könnten insbesondere alle charakteristischen Eigenschaften von Bargeld mit einer CBDC in Form eines „digitalen Euros" abgebildet werden. Auch die automatische Abführung von Steuern, ohne dass die anderen Netzwerkteilnehmer die exakte Berechnung oder den Betrag erfahren, sind denkbar. Natürlich bleiben bei der Nutzung solch neuer Technologien stets auch technische Risiken, aber bislang kann die Experimentierfreude von Kryptowährungen durchaus als Erfolgsgeschichte betrachtet werden, und das Vertrauen von Community und Investoren in die noch junge und sehr komplexe Technologie sprechen für sich. Natürlich sind Fehler im Code von Blockchains und Smart Contracts – wie bei normaler Software – stets möglich, und entsprechend Komplexitätsreduktionen zur Fehlervermeidung zwingend erforderlich. Zudem ist die Rückabwicklung von irrtümlich veranlassten oder etwa gesetzeswidrigen Transaktionen wegen der dezentralen Konsensfindung in zugangsbeschränkten Blockchains nur schwer und in nicht zugangsbeschränkten Blockchains praktisch nicht möglich, ohne die Dezentralisierung ein Stück weit aufzugeben und dadurch neue Herausforderungen für die Sicherheit in Kauf zu nehmen. Entsprechend stellt ein blockchainbasiertes digitales Währungssystem bspw. auch Versicherungen vor große Herausforderungen. Auf der anderen Seite könnten aber gerade Blockchains als redundant betriebene und dezentrale Systeme, die auch von Anfang an unter höchsten Sicherheitsanforderungen konzipiert werden, besonders resistent gegen Systemausfälle und Hacker-Angriffe sein.

Letztlich wird es wohl schon bald nicht mehr vorrangig eine technische Fragestellung sein, wie Währungen und digitale Eigentumsübertragungen in Zukunft abgewickelt werden sollen. Vielmehr muss die Gesellschaft Fragen beantworten wie: Wer soll das Geldsystem operativ betreiben? Wie dezentral soll das Netzwerk organisiert sein? Welcher Grad an Datenschutz und gegenüber welchen Parteien ist wünschenswert, um die Gesellschaft vor Kriminalität, aber auch die Privatsphäre des Einzelnen vor Überwachung zu sichern? Für eine feingranulare Regelung wird es nötig sein, automatisiert digitale Identitäts- und Berechtigungsnachweise führen zu können. Auf Basis von Blockchain-Technologie und Zero-Knowledge Proofs wird aktuell auch ein neues, passwortfreies und interoperables Identitätsmanagement, auch bekannt unter portablen oder selbstsouveränen Identitäten, erforscht, welches gerade in Kombination mit den oben beschriebenen Möglichkeiten für digitale Währungen viele Potenziale bieten könnte. Mit dem Wissen um diese bereits jetzt oder in naher Zukunft praktisch umsetzbaren Möglichkeiten sollten Potenziale und Risiken der Anwendung von Blockchain-Technologie für digitale Währungen nun im Detail aus gesellschaftlicher, ökonomischer, rechtlicher und technischer Perspektive interdisziplinär untersucht werden. Politik und Rechtswissenschaften müssen dabei rechtzeitig die geeigneten Rahmenbedingungen bereitstellen, damit Innovation möglich ist, aber dennoch unsere gesellschaftliche Grundordnung stabil bleibt.

AUTOR

Johannes Sedlmeir *ist Doktorand in Wirtschaftsinformatik an der Universität Bayreuth und Wissenschaftlicher Mitarbeiter am Kernkompetenzzentrum FIM in der Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT.*