BLOCKCHAIN-KOMMUNIKATION FÜR ON-CHAIN-CONTRACTING IM ZAHLUNGSVERKEHR

Marc A. Ostoja-Starzewski

RA Marc A. Ostoja-Starzewski, Diplom-Jurist, Universität des Saarlandes, Institut für Rechtsinformatik
Campus Gebäude A 5.4, 66123 Saarbrücken, DE
marc.ostoja-starzewski@uni-saarland.de

Schlagworte: ***SEPA-Instant-Payments, Blockchain/Distributed Ledger Technology, Smart Contracts, Vertragsrecht***

Abstract: *Der Zahlungsverkehr wird bereits heute unter Einsatz elektronischer Datenverarbeitungssoftware weitestgehend automatisiert durchgeführt. Zunehmend werden Whitepaper veröffentlicht, Proof-of-Conzept erarbeitet und Pilotierungen vorgenommen, die eine Automatisierung unter Einsatz von dezentralen Netzwerken, wie beispielsweise Blockchain, zum Gegenstand haben. Rechtlich gesehen werden an verschiedenen Stellen bei Anbahnung, Erteilung eines Zahlungsauftrags und Durchführung des Zahlungsauftrags Willenserklärungen und rechtsgeschäftsähnliche Handlungen vorgenommen und Erklärungen abgegeben. Auch das Onboarding des Bankkunden, sowie die Erfüllung von Anti-Geldwäsche- und Anti-Korruptions-Verpflichtungen und die Einhaltung von Sanktionslisten erfordert Informationsaustausch und an verschiedenen Stellen Erklärungen des Bankkunden. Sofern die Zahlung nicht als Echtzeitüberweisung im Rechtsrahmen des SEPA-Instant-Payment ausgeführt wird, sondern als herkömmliche Überweisung oder im Lastschriftverfahren, kommen aufgrund der zeitlich versetzten Ausführung und Finalität weitere zwischenzeitig Rechtsgeschäfte, z.B. ein Widerruf, in Betracht. Die Automatisierung der Transaktionsausführung in Distributed Ledger Technologies bietet Möglichkeiten der dezentralen, abgesicherten und schnellen Interaktion, die u.a. im Rechtsverkehr mit Wertpapieren bereits testweise implementiert werden. Zugleich stellen sich bei Einsatz der unterschiedlich ausgeformten DLTs grundlegende Fragen der Rechtsgeschäftslehre.*

1. Rechtliche Analyse anhand ausgewählter Technologien

Im privatrechtlichen Vertragsrecht bietet es sich für eine Detailanalyse an, den Tatbestand von Willenserklärungen, deren Abgabe und deren Zugang zu untersuchen. Die Subsumtion der technischen Abläufe in DLT-Netzwerken auf Basis der Dogmatik der Rechtsgeschäftslehre erfolgt anhand typischer Informationsflüsse und Verarbeitungsschritte in den Blockchain Frameworks Bitcoin, Ethereum und Tendermint.

1.1. Elektronische Erklärungen in DLT-Netzwerken

Die Willenserklärung des Erklärenden eines Angebots zum Vertragsschluss muss inhaltlich so bestimmt oder zumindest bestimmbar und vollständig sein, dass der Erklärungsempfänger das Angebot durch ein schlichtes „Ja“ annehmen kann.[1] Die Auslegung der Willenserklärung richtet sich im Zweifel nach den §§ 133, 157 BGB.[2] Das Angebot muss alle wesentlichen Vertragsbestandteile (essentialia negotii) beinhalten. Darunter fallen wenigstens die Vertragsparteien und die jeweils zu erbringenden Leistungen.[3]

[1] Staudinger/Bork, BGB, 2015, § 145, Rn. 17.
[2] Staudinger/Bork, BGB, 2015, § 145, Rn. 17.
[3] Erman/Armbrüster, BGB Kommentar, 15. Aufl. 2017, § 145, Rn. 2.

Das Kommunikationsdesgin Representational State Transfer (REST)[4] für webbasierte Applikationen beschreibt, wie zwei Computer, zum Beispiel ein Server und ein Client, in einem verteilten Netzwerk miteinander kommunizieren können. Dazu werden anhand von Application Programming Interfaces (API)[5] Schnittstellen definiert, die ein vordefiniertes Eingabeformat akzeptieren. Anhand von Rahmenverträgen kann der Gestaltungsraum für die entsprechenden APIs so vorgegeben werden, dass sie nur Eingaben akzeptieren, welche den rechtlichen Anforderungen an ein Angebot entsprechen.

Hierbei ist zu beachten, dass nur syntaktische Vorgaben gemacht werden können. Ein Beispiel wäre, dass eine gesendete Nachricht Felder zu den Angebotsinhalten haben muss und diese nicht leer sein dürfen. Ob auf der semantischen Ebene auch essentialia negotii enthalten, kann nicht ohne Implementierung weiterer Algorithmen sichergestellt werden, sofern es sich um Freitexteingaben handelt. Mittels generativer AI- Chatbots lassen sich bereits heute Large Language Models implementieren, die eine semantische Prüfung durchführen können. Sofern der Einsatz von künstlicher Intelligenz nicht vorgesehen werden soll, kommen Festtextfelder mit Auswahlmöglichkeiten in Betracht. Diese haben dann allerdings stets definierte Werte, mit denen Parametersprünge verbunden wären. Kautelarjuristisch sollten die Teilnehmer eines solchen Netzwerks in den Rahmenverträgen[6] verpflichtet werden, ihre Nachrichten mit entsprechenden Inhalten zu versehen, die die Anforderungen im Hinblick auf die spezifischen essentialia negotii erfüllen.

1.1.1. Objektiver Tatbestand der Willenserklärung

Bei objektiver Betrachtung muss dem bekundeten Willen des Antragenden entsprechen, dass mit der Annahme seines Angebots ein gültiger, ihn bindender Vertrag zustande kommt. Entscheidend ist der nach außen erklärte Wille, nicht der tatsächliche Wille. Fehlt es an Letzterem, kann dieser Irrtum zur Anfechtung berechtigen.[7]

Der objektive Tatbestand einer Willenserklärung kann in Blockchain-Netzwerken dadurch manifestiert werden, dass eine entsprechende Information ins Netzwerk gesendet wird. Hierfür müssen Rahmenvertragsbedingungen festlegen, welche Rechtswirkungen das Handeln von Teilnehmern und deren Entitäten hat. Rahmenvertragsbedingungen können definieren, dass und unter welchen Voraussetzungen Erklärungen, die in das Netzwerk eingebracht werden, den objektiven Tatbestand einer Willenserklärung erfüllen und zu diesem Zweck eindeutig ihrem Sender und dessen Rechtsträger zuzuordnen sind. Das technische Mittel, um eine Erklärung einem Absender eindeutig zuordnen zu können, könnten Client-Authentifizierung, Zertifikate und fortgeschrittene oder qualifizierte elektronische Signaturen[8] sein. Das Verfahren zur Verwendung der Zertifikate und Signaturen durch die Entitäten der Netzwerk-Teilnehmer muss entsprechend als notwendige Bedingungen für die rechtlich wirksame Abgabe von Erklärungen definiert sein. Hierbei wäre es gleichermaßen ausreichend, dass eine natürliche Person als Entität die Willenserklärung in das Netzwerk einspeist, oder dies durch eine automatisiert ausführende bzw. autonom agierende Softwarekomponente[9] geschieht, welche für eine natürliche Person aus der Sphäre des zuständigen Rechtsträgers betrieben wird. In Blockchain-Netzwerken werden Informationen Transaktionen genannt, da sie ursprünglich nur Informationen zu einer digitalen Finanztransaktion beinhalteten[10]. Spätere Blockchain Frameworks, insbesondere die programmierbaren, fas-

4 Fielding, Roy Thomas, DISSERTATION – Architectural Styles and the Design of Network-based Software Architectures, 2000, S. 75.
5 Fielding, Roy Thomas, Architectural Styles and the Design of Network-based Software Architectures, 2000, S. 138.
6 Wülfing, Thomas, Praxishandbuch Multimediarecht, 2002, S. 244 ff.
7 jurisPK-BGB, Band 1, 9. Aufl. 2020, Rn. 11.
8 Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, Artikel 26.
9 Zur Abgrenzung von autonomen und nicht autonomen Algorithmen vgl. Borges, NJW 2018, 977, 978.
10 Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, https://bitcoin.org/de/bitcoin-paper (aufgerufen am 14. Januar 2024).

sen unter dem Begriff jegliche Informationen[11] zusammen, welche dem Netzwerk hinzugefügt werden und somit das Blockchain-Netzwerk in einen aktualisierten Zustand versetzen.

Hier kann die Umsetzung sogar über die Konfiguration der jeweiligen Blockchain und ihrer technischen Policies programmatisch umgesetzt werden. Im Genesisblock[12], welcher als aller erster Block in einer Blockchain bereits alle Regeln für die Arbeitsweise dieser beinhaltet, kann beispielsweise konfiguriert werden, dass Transaktionen mit fortgeschrittenen oder qualifizierten Signaturen versehen werden müssen. Die meisten Blockchain Frameworks benutzten bereits Signaturen oder andere technische Mittel zur Identifikation, um den Absender zu verifizieren.

1.1.2. Subjektiver Tatbestand der Willenserklärung

Ferner muss bei subjektiver Betrachtung dem bekundeten Willen des Antragenden entsprechen, dass mit der Annahme seines Angebots ein gültiger, ihn bindender Vertrag zustande kommt. Entscheidend ist der nach außen erklärte Wille, nicht der tatsächliche Wille. Fehlt es an letzterem, kann dieser Irrtum zur Anfechtung berechtigen.[13]

Der subjektive Tatbestand einer Willenserklärung lässt sich technisch nicht unmittelbar abbilden. Vielmehr ist er zu schließen aus dem Ingangsetzen und Ausführen des jeweiligen – signierten – Vorgangs. Hieraus sind Wertung herzuleiten, die aus Sicht eines objektiven Dritten anstelle der Teilnehmer des Blockchain-Netzwerks für einen subjektiven Handlungswillen, Rechtsbindungswillen und Geschäftswillen sprechen. Flankierende Interaktionsregelungen aus den Rahmenvertragsbedingungen sichern das Zusammenwirken der Teilnehmer im Blockchain-Netzwerk. Sofern dennoch ein Mangel des Geschäftsbindungswillen nachweisbar ist, verbleibt die Möglichkeit einer Anfechtung der zunächst wirksamen rechtsgeschäftlichen Erklärung, die dann allerdings zum Ersatz des Vertrauensschadens begrenzt auf das negative Interesse verpflichtet.

1.2. Abgabe und Zugang der Erklärungen in DLT-Netzwerken

Sofern der Tatbestand der Willenserklärung objektiv und subjektiv erfüllt ist, bedarf es zur Wirksamkeit die Abgabe und den Zugang der Erklärung.

In den traditionellen Kommunikationsmedien wie Briefverkehr, Telefon und E-Mail sind die Abläufe der Abgabe und des Zugangs hinreichend dogmatisch untersucht und stützen sich auf eine umfangreiche ausdifferenzierte Rechtsprechung. Einige Abläufe in der Blockchain-Technologie lassen sich analog zu diesen Medien erklären, andere Abläufe aber müssen neu betrachtet werden. Eine hinreichend vergleichbare Technologie ist der E-Mail-Verkehr. Auch hier wird eine Nachricht verfasst, diese in ein Netzwerk von Mail-Providern geschickt und am Ende des Prozesses vom Adressaten empfangen. Analog dazu wird auch in einem Blockchain-Netzwerk eine Nachricht bzw. Transaktion erzeugt, in das Blockchain-Netzwerk gestreut und kann dann vom Empfänger ausgelesen werden. Die wesentlichen Unterschiede werden in den folgenden Abschnitten beleuchtet.

1.2.1. Abgabe im Blockchain-Netzwerk

Das Angebot des Erklärenden muss mit seinem Willen in den Verkehr gelangen. Erforderlich ist, dass der Erklärende die Erklärung willentlich in Richtung des Empfängers in Bewegung setzt und dass er mit der Empfangnahme durch den Adressaten, bei Zugrundelegung normaler Verhältnisse, rechnen darf.[14]

---

[11] Transactions, https://docs.cosmos.network/main/learn/advanced/transactions#type-definition (aufgerufen am 14. Januar 2024).

[12] Creating the genesis Block, go-ethereum Documentation, 2023, https://geth.ethereum.org/docs/fundamentals/private-network (aufgerufen am 08.01.2024).

[13] jurisPK-BGB, Band 1, 9. Aufl. 2020, Rn. 11.

[14] BGH 65, 13, 14 f.; WM 1983, 712; München NJW-RR 2005, 1470 f.

Wie der Wille des Erklärenden nachgehalten werden kann, ist bereits im Tatbestand der elektronischen Erklärung aufgezeigt. Dass unter „normalen Verhältnissen" ein Zugang an den Adressaten zu erwarten ist, ergibt sich aus der Stabilität des jeweiligen Blockchain-Netzwerks. Soweit Informationen zwischen den Betreibercomputern nicht korrumpiert synchronisiert werden, funktioniert das Netzwerk. Das Tendermint-Framework ist auf Grund seines Konsensmechanismus leistungsfähig, sofern weniger als 1/3 der Betreibercomputer böswillig agieren[15]. Beim Bitcoin Framework ist davon auszugehen, dass es mit seinem Proof-of-Work-Konsensmechanismus ordnungsgemäß funktioniert, sofern nicht 51% der Gesamtrechenleistung versucht, das Netzwerk zu manipulieren[16]. Auch Blockchains wie das Ethereum Framework, die nach ihrem Wechsel einen Konsensmechanismus auf der Basis eines Proof-of-Stake[17] haben, sind theoretisch angreifbar. Dies ist zum Beispiel durch eine Sybill-Attacke möglich, in dem eine böswillige Entität vorgibt, dass viele unterschiedliche Betreiber handelten und dadurch das Netzwerk über eine – tatsächlich nicht gegebene – Mehrheit täuscht[18]. Zunächst ist davon auszugehen, dass der Adressat an dem Blockchain-Netzwerk teilnimmt und grundsätzlich in der Lage ist, das Angebot zu erhalten und zu verarbeiten.

Sofern eine Erklärung ohne Wissen und Wollen des Erklärenden in den Verkehr gelangt, kann von einer Abgabe nicht ausgegangen werden. Ausnahmsweise gilt diese Erklärung doch als Abgabe, wenn sie aufgrund fahrlässigen Verhaltens des Erklärenden in den Verkehr gelangt.[19] Dann sind die Grundsätze, die für Erklärungen ohne Erklärungsbewusstsein gelten, entsprechend anzuwenden und eine wirksame Erklärung, die vom Erklärenden analog § 119 Abs. 1 BGB innerhalb der Frist des § 121 BGB angefochten werden kann, ist anzunehmen[20].

Eine technische Verifikation, ob die Erklärung mit oder ohne Wissen und Wollen in den Verkehr gebracht wurde, kann an dieser Stelle nicht stattfinden. Die rechtliche Brücke wird durch die Zustimmung der Teilnehmer des Netzwerks im Rahmenvertrag geschlagen. Die Zustimmung beinhaltet, dass der Wille, eine auf einen Vertragsschluss gerichtete Erklärung oder eine rechtsgeschäftsähnliche Handlung automatisch und zurechenbar durch eine Software oder auch digital durch eine natürliche Person abgeben bzw. vornehmen zu lassen, mittels entsprechender technischer Verfahren manifestiert wird.

Zugleich sollte in einem Rahmenvertrag berücksichtigt werden, dass eine Willenserklärung trotzdem ohne tatsächlichen Willen oder unter inhaltlicher Abweichung in den Verkehr gelangt sein kann. Dies könnte zum Beispiel durch ein versehentliches Absenden passiert sein, vergleichbar mit dem versehentlichen Absenden einer E-Mail. Syntaktisch wird weder ein Mailprovider noch ein Blockchain-Netzwerk in der Lage sein, dies zu erkennen. Hierfür müsste es technische Mechanismen geben, welche in der Lage sind, den Willen des Versenders zweifelsfrei zu überprüfen. Zugleich müsste der Willen aus der versendeten Erklärung semantisch zu analysieren und mit dem Willen des Versenders abgleichbar sein. Da dies nicht dem Stand der Technik entspricht – Stand Oktober 2023[21] –, ist die Möglichkeit der Anfechtung einer in den Verkehr gelangten digitalen Willenserklärung bei Konzeptionierung und Implementierung des Netzwerks und bei der Ausgestaltung der Policies und rechtlichen Rahmenverträge zu beachten und ggf. manuell oder teilautomatisiert vorzunehmen.

---

15 Lamport, Leslie/Shostak, Robert/Pease, Marshall, The Byzantine Generals Problem, 1983, S. 1.

16 Aponte-Novoa/Orozco/Villanueva-Polanco/Wightman, The 51% Attack on Blockchains: A Mining Behavior Study. In IEEE Access, vol. 9, S. 140549–140564, 2021, doi: 10.1109/ACCESS.2021.3119291, 2021, S. 140550.

17 Proof-of-stake, https://ethereum.org/de/developers/docs/consensus-mechanisms/pos (aufgerufen am 15.1.2024).

18 Deirmentzoglou, Evangelos/Papakyriakopoulos, Georgios/Patsakis, Constantinos, A Survey on Long-Range Attacks for Proof of Stake Protocols. In: IEEE Access 7, 2019, S. 28712–28725. DOI: 10.1109/ACCESS.2019.2901858.

19 BGH 65, 13, 14.

20 Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 4.

21 Rathkopf, Charles/Heinrichs, Jan Hendrik/Heinrichs, Bert, Can we read minds by imaging brains?. In: Philosophical Psychology, Volume 36, Issue 2, 2023, S. 221–246, DOI: 10.1080/09515089.2022.2041590.

1.2.2. Zugang im Blockchain-Netzwerk

Die Abgabe einer Erklärung in einem Blockchain-Netzwerk ist somit mit dem Versand einer E-Mail vergleichbar. Der nächste Prozessschritt – Zugang – bedarf allerdings einer detaillierten Betrachtung und auch Differenzierung bei unterschiedlichen Technologien. Es stellt sich die Frage, ob und ggf. wann bei einer Kommunikation über eine Blockchain ein Zugang nach den Grundsätzen von Erklärungen unter Abwesenden oder Anwesenden vorliegt.

1.2.2.1. Zugang unter Abwesenden

Das Angebot des Erklärenden wird gemäß § 130 Abs. 1 S. 1 BGB erst mit Zugang beim Empfänger wirksam. Dabei muss die Willenserklärung derart in den Machtbereich des Empfängers gelangen, dass der Erklärende unter normalen Umständen mit einer Kenntnisnahme rechnen kann. Auf die tatsächliche Kenntnisnahme des Empfängers kommt es dagegen nicht an.[22] Der Verlust (die Veränderung, Verfälschung, Zerstörung) der Erklärung auf dem Wege zum Empfänger und Zugangshindernisse außerhalb des Einwirkungsbereichs des Empfängers gehen zulasten des Erklärenden.[23]

Grundsätzlich sind auch davon abweichende Regelungen des Zugangs zulässig. Für Regelungen in AGB sind insbesondere die Grenzen der §§ 308 Nr. 6 und 309 Nr. 13 BGB zu beachten.[24]

Zudem ist als Vorfrage zu klären, ob es sich um verkörperte und nicht verkörperte Erklärungen handelt.

1.2.2.1.1. Verkörperte Erklärungen

Bei einer verkörperten Erklärung ist der Zugang beim Empfänger entscheidend. Die Erklärung muss auch hier so in den Machtbereich des Empfängers gelangt sein, dass unter normalen Umständen mit einer Kenntnisnahme gerechnet werden kann.[25]

1.2.2.1.2. Nicht verkörperte Erklärungen

Eine nicht verkörperte Erklärung wird hingegen mit der Abgabe durch den Erklärenden wirksam. Die Erklärung muss vom Empfänger wahrgenommen worden sein. Außerdem darf der Erklärende vernünftigerweise keinen Zweifel daran gehabt haben, dass der Empfänger die Erklärung auch verstanden hat.[26]

1.2.2.2. Zugang unter Anwesenden

Da es für den Zugang unter Anwesenden keine gesetzliche Regelung gibt, ist auch hier der Grundgedanke des § 130 BGB zu berücksichtigen und zu entscheiden, ob es sich um eine verkörperte oder nicht verkörperte Erklärung handelt.[27]

Verkörperte Erklärungen, also physikalisch auf einem Medium gespeicherte Erklärungen[28] (zum Beispiel: Brief, elektronischer oder optischer Datenträger) gehen unter Anwesenden mit ihrer Aushändigung dem unmittelbaren Adressaten oder diesem mittelbar über seinen Vertreter zu. Die Aushändigung nur an einen Empfangsboten stellt hingegen die Abgabe einer Erklärung unter Abwesenden dar. Eine Übergabe von Hand zu Hand ist nicht erforderlich, es genügt, wenn die verkörperte Erklärung in den Einwirkungsbereich des Empfängers gelangt, bei räumlicher unmittelbarer Anwesenheit etwa dadurch, dass sie ihm auf den Tisch

[22] Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 5.
[23] Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 5.
[24] Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 5.
[25] Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 22.
[26] Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 23.
[27] Erman/Arnold, BGB Kommentar, 15. Aufl. 2017, § 130, Rn. 21.
[28] Noack/Uhlig JA 2012, 740 (742).

gelegt wird.[29] Allerdings muss der Empfänger zumindest Gelegenheit haben, die Übergabe zu bemerken; ein unbemerktes Zustecken einer verkörperten Willenserklärung bewirkt keinen Zugang. Ist die verkörperte Willenserklärung in einer Fremdsprache verfasst, die der Empfänger nicht beherrscht, gilt sie erst nach Ablauf einer angemessenen Übersetzungsfrist als zugegangen; entsprechendes muss für Erklärungen gelten, die nur unter Zuhilfenahme von erkennbar nicht sofort verfügbaren technischen Hilfsmitteln zur Kenntnis genommen werden können, zum Beispiel weil sie auf einem nur maschinell lesbaren Datenträger gespeichert sind.[30]

1.2.2.3. Analyse des Zugangs im Blockchain-Netzwerk

Unter den genannten Gesichtspunkten ist zunächst zu ermitteln, welche Tatbestandsvoraussetzungen für den Zugang einer Willenserklärung in einem Blockchain-Netzwerk zu erfüllen sind. Hierbei spielt die Verortung des Erklärenden und des Adressaten genauso eine Rolle wie die etwaige Verkörperung der Erklärung. Im Folgenden werden bereits am Markt technologisch implementierte Verfahren außerhalb von Blockchain Anwendungen beispielhaft dargestellt, um sie im Anschluss anhand einer Auswahl von Blockchain Frameworks mit den dort anzutreffenden Verfahren vergleichen zu können.

Nicht verkörperte Erklärung unter Anwesenden

Eine nicht verkörperte Erklärung unter Anwesenden kann trivial mit mindestens zwei Personen im gleichen Raum dargestellt werden, die ihre Erklärungen mündlich abgeben. Allein die räumliche Nähe oder die Nutzung von technischen Hilfsmitteln, wie zum Beispiel dem Telefon oder der Videotelefonie ändert nichts daran, dass die Erklärung unter Anwesenden abgegeben wird. Der gemeinsame Faktor ist hier die Echtzeit-Kommunikation, bei der beide Personen im direkten Austausch sind[31]. Dies ist sowohl der Fall, wenn die Personen im gleichen Raum sind, als auch wenn sie per Telefon, Videotelefonie oder Chat miteinander kommunizieren. Die Kommunikationspartner können ihren Willen direkt an dem Gegenüber erklären und zugleich ist eine direkte Rückmeldung möglich. Daher ist die Abgabe der Willenserklärung hier eine hinreichende Tatbestandsvoraussetzung. Dass die Willenserklärung bei einer direkten Kommunikation auch verstanden wird, wird vorausgesetzt. Andernfalls besteht die Möglichkeit, direkt eine Rückfrage zu stellen oder Hilfsmittel, wie zum Beispiel Übersetzer oder Berater zu involvieren. Eine Kommunikation über eine Blockchain erfüllt nicht die Anforderungen an eine Willenserklärung unter Anwesenden. Echtzeitnahe Kommunikation, also das Programmaufgaben und Abläufe innerhalb strikten zeitlichen Grenzen ablaufen[32], ist hier technisch nicht möglich und somit gibt es auch keine Möglichkeit einer direkten bidirektionalen Kommunikation.

Verkörperte Erklärung unter Anwesenden

Eine verkörperte Willenserklärung unter Anwesenden ist analog zu einer nicht verkörperten zu behandeln, bis auf die Verkörperung der Willenserklärung. Dies bedeutet, es existiert eine schriftliche oder andere, in dauerhaften Zeichen dargelegte, Form des Willens[33]. Ein Szenario zur Verdeutlichung wäre eines mit mindestens zwei Parteien, die einen schriftlichen Vertrag vor sich haben. Sofern der Vertrag übereinstimmt mit dem Willen der erklärenden Parteien, unterzeichnen sie diesen; dadurch liegt eine schriftliche Form der übereinstimmenden Willenserklärungen in dauerhaften Zeichen vor. Dieses Prinzip lässt sich technisch abbilden, zum Beispiel mit Unterschriftenpads (engl.: signature pads). Dies ist sowohl grundsätzlich juristisch möglich[34], als

29 BGH NJW-RR 1996, 641 (642).
30 BeckOK BGB/Wendtland, 61. Ed. 1.2.2022, BGB § 130 Rn. 27.
31 Weber und Trick, SIP und Telekommunikationsnetze, Next Generation Networks und Multimedia over IP, 2015, S. 21.
32 Tannenbaum, Andrew S./Bos, Herbert, Modern operating systems. 4. Ed., Prentice Hall, Boston, 2015, S. 37.
33 MüKoBGB/Einsele, 9. Aufl. 2021, BGB § 130 Rn. 2.
34 MüKoBGB/Einsele, 9. Aufl. 2021, BGB § 126 Rn. 2.

z.B. auch im medizinischen Sektor bereits technisch und juristisch anerkannt[35]. Da die echtzeitnahe Kommunikation und somit auch die bidirektionale Kommunikation fehlt, qualifiziert die Blockchain-Kommunikation nicht als Erklärung unter Anwesenden.

Nicht verkörperte Erklärung unter Abwesenden

Eine Kommunikation über eine Blockchain lässt sich am ehesten mit einer Abgabe von Erklärungen unter Abwesenden vergleichen. Analog zum Mailversand werden auch hier Nachrichten in einer Kommunikationsinfrastruktur vom Absender eingebracht. Von hier aus gelangen sie in den Machtbereich des Empfängers. Die Frage, ob bei dieser Art. der Kommunikation eine nicht verkörperte Willenserklärung unter Abwesenden abgegeben wird, ist nicht eindeutig zu beantworten. Die Betrachtung dieser Position bedarf zunächst eines Vergleichs mit analogen Abläufen, z.B. dem Briefversand. Hier wird die Willenserklärung in einem Schreiben in eine dauerhafte Schriftform gebracht und somit verkörpert. Anschließend wird sie willentlich in Richtung des Empfängers, gekennzeichnet durch die Empfängeradresse, in den Postverkehr gebracht. Unter der Voraussetzung normaler Umstände kann davon ausgegangen werden, dass diese verkörperte Nachricht in den Machtbereich des Empfängers gelangt, in dem sie in seinen Briefkasten eingeworfen und somit empfangen wird.

Einen ähnlichen, aber digitalen Ablauf nimmt der Versand einer Mail[36]. Hier findet die Verkörperung aber in der Regel später statt. Während ein Brief direkt in eine dauerhafte Schriftform gebracht wird, stellt das Eingeben von semantisch dargestellten Zeichen im Sinne eines Schreibens einer Mail in der Regel noch keine Verkörperung dar. Eine dauerhafte Speicherung auf einem Medium findet hier meist noch nicht statt. Dies wird deutlich, wenn die Arbeitsweise von aktuellen Computern betrachtet wird.

Was die Elemente der Speicherhierarchie gemeinsam haben, ist dass alle Elemente volatile sind und somit flüchtige Speicher darstellen[37]. Das bedeutet, die beinhaltenden Informationen stehen nur so lange zur Verfügung, solange auch eine Spannung anliegt.[38] Sobald keine Spannung mehr anliegt, sind die Daten und die durch sie repräsentierten Informationen verloren. Somit stellen die bloße Verarbeitung und Darstellung von Informationen noch keine dauerhafte Speicherung auf einem Medium dar.

Was landläufig als „gespeichert" bezeichnet wird, findet erst in der nächsten Hierarchieebene statt, wenn Daten aus dem Arbeitsspeicher auf Laufwerke übertragen werden. Die Differenzierung eines Briefversands und eines Mailversands erfordert eine Betrachtung des Zeitpunkts der Speicherung der Mail. Häufig findet die Speicherung nicht beim Tippen der Mail statt, auch wenn viele Mailanbieter oder auch Mailprogramme an dieser Stelle schon eine Entwurfsfassung sichern. Eine Mail in diesem „Entwurfsstadium" ist noch nicht willentlich in Umlauf gebracht und stellt noch keine Willenserklärung da, vergleichbar mit dem Entwurf einer Idee oder eines Willens, die bzw. der noch nicht geäußert wurde. Eine Mail hingegen, die bereits versendet ist, wird im Normalfall auf dem Server des Providers gespeichert, genannt „persistiert", und ist somit sowohl auf einem dauerhaften Medium hinterlegt, als auch in Richtung des Empfängers in Umlauf gebracht. Spätestens auf dem Server des Mailproviders des Empfängers findet eine Speicherung statt. Denn dieser muss zunächst die Mail nach Erhalt vorhalten. Wenn der Empfänger sein Postfach nach neuen Inhalten abfragt, übermittelt der Mailprovider diese an ihn. Es kann also angenommen werden, dass der Empfänger unter normalen Umständen diese Willenserklärung in seinem Machtbereich vorfinden wird, wenn sie auf dem Mailserver des Mailproviders des Empfängers ankommt.

Der Vergleich des Mailversands mit der Kommunikation in einer Blockchain führt zu einem komplexen Bild. Es fließen zwar auch in einer Blockchain Informationen, aber da hier eine verteilte Infrastruktur vorliegt ist

[35] Deutscher Bundestag Drucksache 504/18, S. 147, Entwurf eines Gesetzes für schnellere Termine und bessere Versorgung (Terminservice- und Versorgungsgesetz – TSVG), 12.20.2018.

[36] Postel, Jonathan B., RFC 821, https://www.rfc-editor.org/info/rfc821, 1982, (aufgerufen am 09.01.2024).

[37] Bryant, Randal E./O'Hallaron, David R., Computer systems. A programmer's perspective. Third edition. 2016, S. 614.

[38] Bryant, Randal E./O'Hallaron, David R., Computer systems. A programmer's perspective. Third edition. 2016, S. 610.

es anders als beim Mailversand weniger klar, wann diese Informationen nicht nur verarbeitet, sondern auch persistiert ist.

Verkörperte Erklärung unter Abwesenden

Nach dem Ausschlussprinzip müsste eine Kommunikation über eine Blockchain eine verkörperte Willenserklärung darstellen. Diese Schlussfolgerung ist am Ende der Kommunikation zwar zutreffend, aber nicht von Anfang an. Für ein besseres Verständnis wird zunächst betrachtet, was am Ende einer Kommunikation innerhalb einer Blockchain liegt und was auf dem Weg bis dahin passiert. Weiter erschwert wird diese Betrachtung dadurch, dass unterschiedliche Blockchain Frameworks das Persistieren, also das Hinzufügen eines neuen Blocks, auf Grund ihrer unterschiedlichen Implementierung jeweils anders ausführen. Um nachzuvollziehen, warum diese Schlussfolgerungen nicht trivial sind, werden die Blockchain-Infrastrukturen und die Abläufe detaillierter betrachtet.

Wie beim Postversand und auch beim Mailversand gibt es auch in Blockchain-Infrastrukturen unterschiedliche Arten von Beteiligten[39]. Zum einen gibt es Entitäten, die eine Blockchain nutzen. Dafür brauchen sie in der Regel einen Mechanismus und eine Autorisierung. Ein Wallet[40] oder ein LightClient[41] sind Begriffe, die in diesem Zusammenhang häufig fallen. Stark vereinfacht erlauben es diese technischen Hilfsmittel bzw. Programme Informationen in das Blockchain-Netzwerk zu senden und auch aus diesem auszulesen. Eine Analogie ist hier ein Onlinebanking-Zugang und ein TAN-Generator. Wie der Banking-Zugang und der TAN-Generator es ermöglichen, auf die individuellen Bankinformationen zuzugreifen und gegebenenfalls auch Transaktionen auszulösen, so sind auch ein Blockchain-Zugang und eine Wallet dazu in der Lage. Hierbei ist es unerheblich, ob die verarbeitete Information eine tatsächliche Transaktionsanweisung von Kryptowährungen ist oder eine Sensorinformation[42]. Im Blockchain-Umfeld hat sich für diese unterschiedlichen Informationen der Begriff Transaktion durchgesetzt.

Die Instanzen, welche die Datenhaltung und Verarbeitung gewährleisten und damit die Blockchain-Infrastruktur bereitstellen und betreiben heißen Nodes[43]. Sie stellen, wie Knoten (engl. Nodes) in einem Netz die Verbindungspunkte im Netzwerk dar. Verglichen mit der analogen Welt wären diese die Postsortier- und Postverteilstationen oder im Mailverkehr die Mailserver. Um nun nachzuvollziehen, wann eine Transaktion, welche eine Willenserklärung oder rechtsgeschäftsähnliche Handlung beinhaltet, nun verkörpert wird, muss ihr Weg nachverfolgt werden. Dieser beginnt mit der Verarbeitung an einem Senderclient bzw. Senderwallet. Von dort wird sie in das Blockchain-Netzwerk gesendet, durchläuft einen Konsensmechanismus, bei dem sie auch persistiert und schließlich von einer Empfangswallet wieder ausgelesen oder empfangen werden kann.

Bitcoin

Die Bitcoin-Blockchain ist eine Permissionless-Blockchain[44], das bedeutet, jeder ist in der Lage und auch berechtigt dazu an dem Netzwerk teilzunehmen, indem eine Wallet eingerichtet wird. Darüber hinaus ist es möglich einen Node zu betrieben und selbst ein Teil der Blockchain-Infrastruktur zu sein. Auf Grund dieser offenen Architektur ist es nicht vorhersehbar, wie sich Informationen über das gesamte Netzwerk verteilen und

[39] Gürpinar, Tan/Korkmaz, Timucin/Henke, Michael, Rollen und Aufgaben Interdisziplinärer Projektteams zur Blockchain-Integration im Unternehmensumfeld, 2022, S. 2–4.

[40] Wallets, https://developer.bitcoin.org/devguide/wallets.html (aufgerufen am 06. Januar 2024).

[41] Sparer, Dominik/Günther, Max David/Heyer, Christofer, A Multi-Light-Node Blockchain Architecture, DOI:10.24406/IML-N-614399, 2020, S. 6.

[42] Schlatt, Vincent/Schweizer, André/Urbach, Nils/Fridgen, Gilbert, Blockchain: Grundlagen Anwendungen und Potenziale. Online verfügbar unter https://publica.fraunhofer.de/handle/publica/298479, 2016.

[43] Strehl, Luisa Marie/Kopka, Jan-Philip/Bohlen, Marius Alfred/Preut, Anna/Schumacher, Christina, Umsetzung eines digitalen Produktpasses mit Hilfe der Blockchain-Technologie, DOI: 10.24406/publica-1314, 2023.

[44] Henke, M., Schulte, A.T., Jakob, S., Blockchain-basiertes Supply Chain Management. In: ten Hompel, M., Bauernhansl, T., Vogel-Heuser, B. (eds) Handbuch Industrie 4.0. Springer Vieweg, Berlin, Heidelberg. DOI:10.1007/978-3-662-58530-6_116, 2020, S. 600–601.

wann neue Informationen bei einem bestimmten Teilnehmer verfügbar sind. Da in der Bitcoin-Blockchain nur Transaktionen gehandhabt werden, wird im Folgenden anstelle von allgemeinen Informationen der Einfachheit halber von Transaktionen gesprochen. Eine neue Transaktion findet in der Regel ihren Weg über eine Wallet in das Bitcoin-Netzwerk. Hier wird diese Transaktion an viele weitere Nodes des Netzwerks weitergeleitet und landet in den jeweiligen Mempools[45]. Diese Mempools bilden bei jedem Node ein individuelles Auffangbecken für Transaktionen, die zu Blöcken zusammengefasst werden sollen. Zu diesem Zeitpunkt gibt es die neue Transaktion bereits mehrmals abgebildet im Netzwerk, aber da die Mempools im Arbeitsspeicher der Nodes gehandhabt werden und diese einen flüchtigen Speicher darstellen, ist die Transaktion noch nicht persistiert. Sie ist also noch nicht in dauerhaften Zeichen dargelegt und erfüllt noch nicht die Bedingungen einer verkörperten Willenserklärung. Die einzelnen Nodes versuchen immerwährend neue Blöcke zu bilden und diese der Bitcoin-Blockchain anzufügen. Dazu bilden sie aus den Transaktionen in ihrem jeweiligen Mempool einen Block, in dem sie den Hash[46] des aktuell letzten Blocks nehmen, dann eine Reihe an Transaktionen anfügen und dann einen Hash über diesen neun Block bilden[47]. Dabei ist ein Hash ein Abbild der zugrundeliegenden Daten auf eine kürzer definierte Datenmenge. Vereinfacht ein digitaler Fingerabdruck, der leicht zu überprüfen, aber sehr schwer bis gar nicht herzuleiten ist. Damit aber das gleichzeitige Hinzufügen von Millionen von Blöcken an unterschiedlichen Nodes nicht zu einer völligen Verästelung in der Bitcoin Blockchain führen, gibt es noch eine Bedingung. Diese muss erfüllt werden, bevor ein Node einen neuen Block anfügen und diesem im Netz als neuen Block propagieren darf. Es muss noch ein zusätzlicher und zufälliger Wert hinzugefügt werden, die Nonce[48]. Erst wenn der neue Block zusammen mit der Nonce einen Hash ergibt, der einem bestimmten Muster folgt, liegt ein korrekter Block vor. Ein Hash ist aber eine Einwegfunktion, das heißt, sie ist leicht auszurechnen, aber fast nicht zurückzurechnen. Es kann also nur immer wieder ein neuer Zufallswert „erraten" werden, dann wird der mögliche Block verhasht und falls der Hash dem Muster nicht entspricht, wird erneut probiert. Dies ist das sogenannte Mining des Proof-of-Work (PoW) Verfahrens. Der Hash mit dem richtigen Muster ist dann der Nachweis für die geleistete Arbeit, die erbracht wurde, um diesen Block zu erstellen. Das alles passiert noch im flüchtigen Speicher, dem Arbeitsspeicher, im Englischen Random-Access Memory (RAM). Erst der fertige Block wird in einem Laufwerk zur dauerhaften Speicherung abgelegt, und würde auch nach einem Neustart oder Stromausfall zur Verfügung stehen. An dieser Stelle ist die Transaktion zwar abgespeichert und damit verkörpert, aber sie ist nichts zwangsläufig im Machtbereich des Empfängers. Das ist sie erst, wenn der neue Block in der Bitcoin Blockchain verteilt und auch akzeptiert ist. Der neue Block wird zwar im Netzwerk verteilt und von anderen Nodes empfangen, geprüft und falls sie diesen als korrekt anerkennen auch an ihre Kette an Blöcken angehängt, aber es kann sein, dass gleichzeitig auch ein anderer Block generiert wurde. In dem Fall gäbe es mindestens zwei Stränge, also eine Gabelung im Verlauf der Blockchain, ein sogenannter Fork. Je nachdem, an welchem der Äste schneller Blöcke angehängt werden, kann es passieren, dass der Ast mit der Transaktion des sendenden Wallets nicht mehr beachtet wird. Denn der Konsens in der Bitcoin-Blockchain ist der, dass der Ast, der am schnellsten wächst und in den die meiste „Arbeit" eingeflossen ist, als die „Wahrheit" angesehen wird. Falls also ein anderer Ast schneller wächst, müsste die Transaktion erneut in einen Block aufgenommen werden und erneut versucht werden, diesen an den längsten Ast anzufügen. Daher wird empfohlen, ca. sechs Bestätigungen[49] des

[45] Transactions, Ethereum – Developers. Online verfügbar unter https://ethereum.org/en/developers/docs/transactions/, 2023 (aufgerufen am 16.12.2023).

[46] Rogaway, P./Shrimpton, T., Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, S. 371–388. Springer, Heidelberg (2004)

[47] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/de/bitcoin-paper, (aufgerufen am 17.12.2023), 2008.

[48] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/de/bitcoin-paper, (aufgerufen am 17.12.2023), 2008.

[49] Payment Processing. bitcoin Developers Guide. https://developer.bitcoin.org/devguide/payment_processing.html.

Astes abzuwarten bevor davon ausgegangen werden kann, dass der Block in der Blockchain auch aufgenommen und nicht ignoriert wird. Sechs Bestätigungen bedeutet hier, dass nach dem Block mit den gewünschten Informationen noch sechs weitere Blöcke angehängt worden sind, und der Ast damit den schnellsten wachsenden Ast darstellt. Im Durchschnitt müsste eine Stunde gewartet werden bevor davon ausgegangen werden kann, dass ein Block gespeichert und auch finalisiert worden ist. In einem Bitcoin-Netzwerk kann also erst nach einer Stunde davon ausgegangen werden, dass eine Erklärung verkörpert und auch mit der Möglichkeit der Kenntnisnahme in den Machtbereich des Empfängers gelangt ist. Vorher ist keine sichere Aussage über den Zugang zu treffen.

Ethereum

Die Ethereum-Blockchain ist ebenfalls eine permissionless Blockchain und gehört schon zur 2. Generation[50] der Blockchains. Sie kann nicht nur ihre Kryptowährung, den Ether, handhaben, sondern auch andere Arten von Informationen, und ist in der Lage Smart Contracts zu verarbeiten. Dies führt zugleich dazu, dass die Ethereum-Blockchain weitere Funktionalitäten bietet und selbst komplexer wird. Zudem wurde bei Ethereum 2022 beim großen „Merge“[51] der Konsensmechanismus vom PoW zum Proof-of-Stake (PoS) geändert. Proof-of-Stake setzt voraus, dass eine Entität mit einer großen Menge Ether eine intrinsische Motivation hat, dass die Kryptowährung stabil bleibt und das Kryptowährungssystem nicht manipulieren möchte. Der Einsatz der Entität wird verwahrt und berechtigt die Entität an einer Verlosung teilzunehmen. Der Gewinner der Verlosung darf den nächsten Block bilden und anfügen. Wenn der neue Block von den anderen Teilnehmern validiert und für korrekt befunden wird, so bekommt der jeweilige Node seinen Einsatz und eine kleine Gebühr zurück. Falls er allerdings versucht manipulativ einzugreifen, in dem er zum Beispiel mehrere oder falsche Blöcke propagiert, so kann es passieren, dass er seinen Einsatz verliert oder sogar aus dem Verfahren für gewisse Zeit ausgeschlossen wird. Hierbei steigt die Wahrscheinlichkeit den Zuschlag zu erhalten mit der Höhe des Einsatzes. Vergleichbar ist das mit dem Kauf von Lotterielosen: je mehr Geld eingesetzt wird, also mehr Lose gekauft werden, umso größer ist die Chance zu gewinnen. Der Fairnesshalber gibt es aber eine Kappung beim Einsatz von 32ETH (Ether). Ein niedrigerer Einsatz verringert die Wahrscheinlichkeit, ein noch höherer Einsatz als 32ETH erhöht aber nicht die Wahrscheinlichkeit weiter.[52] Die Nodes, die nicht ausgewählt werden, erhalten ihren Einsatz ebenfalls zurück, da diese nicht im Zugzwang sind, einen korrekten Block abzuliefern. Um den Weg einer Transaktion in Ethereum so nachvollziehen zu können wie bei der Bitcoin-Blockchain, muss der Inhalt einer Transaktion näher betrachtet werden. Denn neben Informationen wie Sender, Empfänger, Signatur, Value und anderen Werten gibt es auch die, die sich auf etwas beziehen, das sich „gas“ nennt[53]. In gas[54] wird der Rechenaufwand für die Ethereum Blockchain bemessen, um eine Transaktion durchzuführen. Die Ethereum Blockchain kann im Vergleich zur Bitcoin-Blockchain auch Smart Contracts verarbeiten. Dies bedeutet, dass jede Transaktion einen gewissen Rechenaufwand verursacht, ob es nun eine einfache Transaktion mit Informationen ist oder eine Transaktion, die eine komplexe Smart Contract Berechnung anstößt. Dieser Aufwand wird in gas bemessen und muss kompensiert bzw. bezahlt werden. Daher enthält eine Ethereum Transaktion auch Informationen darüber wie viel der Versender bereit ist als Gebühr zu bezahlen (gasLimit) und wie viel er als „Trinkgeld“ (maxPriorityFeePerGas) dem Validator geben möchte. Ein Validator ist in diesem Zusammenhang ein Node, der dazu berechtigt ist Blöcke zu überprüfen und ggfs. auch selbst Blöcke vorzuschlagen. Die Gebühr wird bei einer Transaktion immer entrichtet und verbraucht, da ja der Berechnungsaufwand für den Validator auch dann entsteht, wenn die Transaktion nachher nicht

[50] Buterin, Vitalik, A next-generation smart contract and decentralized application platform, 2014.

[51] Die Zusammenführung, https://ethereum.org/de/roadmap/merge/, (aufgerufen am 09.01.2024).

[52] Block proposal, https://ethereum.org/de/developers/docs/consensus-mechanisms/pos/block-proposal/#who-produces-blocks, (aufgerufen am 09.01.2024).

[53] Transactions, https://ethereum.org/en/developers/docs/blocks#block-timeers/docs/transactions, (aufgerufen am 18.12.2023).

[54] Gas, https://ethereum.org/de/developers/docs/gas (aufgerufen am 18.12.2023).

validiert wird. Das „Trinkgeld“ ist für den Validator vorgesehen, daher wird für diesen ein Anreiz geschaffen eine Transaktion einer anderen vorzuziehen, insbesondere in Zeiten großer Auslastung. Eine Transaktion ohne ausgewiesenes „Trinkgeld“ ist zwar formal korrekt, aber wird sehr wahrscheinlich nie verarbeitet, da sie einem Validator keinen Anreiz bietet diesen zu prüfen und in einen Block zu schreiben.

Die Bedeutung dieser Aspekte für die Verkörperung ist ähnlich wie bei der Bitcoin-Blockchain. Es gibt auch bei der Ethereum-Blockchain Beobachtungsmöglichkeiten (z.B. Etherscan[55]), die es erlauben eine Transaktion zu sehen, noch bevor sie in einen Block geschrieben wird. Hier ist aber der Schritt von der Transaktion zu einem Block noch unvorhersehbarer als bei der Bitcoin-Blockchain. Denn die Auswahl einer Transaktion, um diesen in einen Block zu persistieren, wird zusätzlich durch die Parameter für das „gas“ beeinflusst. Und auch hier gibt es keine mathematische Sicherheit, dass der Empfänger einer Transaktion diese sehen kann, bevor sie persistiert ist. Denn selbst wenn der Empfänger einen eigenen Node betreibt, ist es nicht garantiert, dass die entsprechende Transaktion diesen Node erreicht hat. Von einem Zugang kann nur dann ausgegangen werden, wenn die Transaktion in einem Block aufgenommen wurde, also eine Verkörperung stattgefunden hat. Bei der Ethereum-Blockchain ist der Konsensmechanismus so gestaltet, dass nach 12 Sekunden ein neuer Block geschrieben wird (die sogenannte „blocktime“[56]). Im normalen Betrieb wird es im Netzwerk einen Ast geben, an dem der neue Block angehängt wird. Falls es aber durch Latenzen o.ä. im Netzwerk unterschiedliche Informationen darüber gibt, welcher der letzte Block ist, also wenn ein Fork entstanden ist, so wird der Ast als der korrekte angesehen, welcher die meisten Bestätigungen in der letzten Epoche hatte. Eine Epoche ist hierbei ein Zeitintervall von 6,4 Minuten[57] bzw. 32 Slotes/Sequenzen[58]. In jeder Epoche sendet ein Validator seine Sicht der Blockchain und bestätigt damit eine Sequenz in der Epoche vom Startblock der Epoche bis zu dem letzten gerechtfertigten Block. Diese Attestierungen führen zu einem Konsens über den aktuellen Zustand der Blockchain.

Hieraus lässt sich folgern, dass eine Transaktion in der Ethereum Blockchain zwar eine nicht verkörperte Willenserklärung darstellen kann, aber in diesem Status nicht sichergestellt werden kann, dass sie zugegangen ist. Ein finalisierter persistierter Block wird im Vergleich zur Bitcoin-Blockchain schneller erreicht. Auch hier ist es theoretisch möglich, dass die Blockchain an einem Ast weiterwächst, der nicht einen korrekten Ablauf darstellen würde. Im Gegenteil zur Bitcoin-Blockchain, in dem eine Transaktion dann einfach in einem anderen Block erneut aufgenommen wird, wäre es hier allerdings nicht systembedingt. So ein Verhalten der Blockchain setzt einen manipulativen Eingriff voraus, bei dem der Angreifer gewillt ist, mindestens 1/3 seiner gestakten Einsätze zu verlieren[59].

Tendermint/CosmosSDK

Das Blockchain Framework Tendermint und seine Programmierschnittstelle CosmosSDK ist ein Beispiel der Permissioned-Blockchain[60]. Während Permissionless-Blockchains eine völlig offene Architektur haben, sind Permissioned-Blockchains dafür gedacht, von einem geschlossenen Anbieterkreis betrieben zu werden. Das Framework ist eine Open Source Software, dennoch kann sich nicht jeder einfach die Software herunterladen und sich einem bestimmten Tendermint Netzwerk anschließen. Genauer definiert gehört die Tendermint-Blockchain zur Untergruppe der Consortial-Blockchains[61]. In diesen haben alle Fullnodes, Nodes mit

55 Pending Transactions, https://etherscan.io/txsPending (aufgerufen am 18.12.2023).

56 Blocks, https://ethereum.org/en/developers/docs/blocks#block-time (aufgerufen am 18.12.2023).

57 Attestations, https://ethereum-org-fork.netlify.app/developers/docs/consensus-mechanisms/pos/attestations (aufgerufen am 18.12.2023).

58 Proof-of-Stake, https://ethereum-org-fork.netlify.app/developers/docs/consensus-mechanisms/pos (aufgerufen am 18.12.2023).

59 Proof-of-Stake, https://ethereum-org-fork.netlify.app/developers/docs/consensus-mechanisms/pos (aufgerufen am 18.12.2023).

60 Henke, M., Schulte, A.T., Jakob, S. (2020). Blockchain-basiertes Supply Chain Management. In: ten Hompel, M., Bauernhansl, T., Vogel-Heuser, B. (eds) Handbuch Industrie 4.0. Springer Vieweg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-58530-6_116, S. 601.

61 Henke, M., Schulte, A.T., Jakob, S. (2020). Blockchain-basiertes Supply Chain Management. In: ten Hompel, M., Bauernhansl, T., Vogel-Heuser, B. (eds) Handbuch Industrie 4.0. Springer Vieweg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-58530-

einer vollständigen Kopie der zugrundeliegenden Blockchain und in der Regel allen verfügbaren administrativen Berechtigungen, die Möglichkeit bei administrativen Aufgaben mitzuentscheiden. Dies schließt u.a. das Aufnehmen neuer Fullnodes, den Ausschluss von diesen und andere Aufgaben mit ein. Diese Eingruppierung gibt aber keine Sonderechte in Bezug auf den benutzten Konsensalgorithmus. Die korrekte Verarbeitung der vorliegenden Aufgabe liegt weiterhin bei jedem, an dem Konsens beteiligten Node und damit verteilt im gesamten Netzwerk. Dies ist auch bei der zweiten Unterkategorie, den Permissioned-Private-Blockchains, so, nur dass hier die Verwaltungsaufgaben nur einem ausgewählten Kreis oder sogar nur einem Node zugeteilt ist. Diese strukturellen Unterschiede haben direkten Einfluss auf den verwendeten Konsensmechanismus und damit auf die Art. und Weise wie ein Block persistiert wird, also auch wie eine Erklärung verkörpert wird.

Die Tatsache, dass die Fullnodes in einem Tendermint Netzwerk verwaltet und damit bekannt sind, lässt eine andere Art. an Konsensmechanismen zu. Zunächst findet auch hier eine nicht verkörperte Willenserklärung in Form einer Transaktion ihren Weg in das Netzwerk. Hier wird sie in den Mempool des ersten Nodes auf den sie trifft aufgenommen und an weitere Nodes verteilt. Die Tendermint-Blockchain ist ebenfalls in der Lage Smart Contracts zu verarbeiten, aber sie benötigt dafür keine gesonderte Kryptowährung oder zusätzlicher Bearbeitungsschritte. Die Transaktionen werden zu Blöcken zusammengefasst und dem Netzwerk vorgeschlagen. Dabei wird ungefähr ein Block pro Sekunde[62] persistiert, welcher direkt final ist.

In der Tendermint-Blockchain gelingt das durch den Byzantine Fault Tolerant Algorithmus, welcher eine Lösungsvariante zum Byzantines Generals Problem[63] darstellt. Die Problemstellung ist aus dem alten Byzanz, in dem die Generäle vor dem Problem standen, bei der Belagerung einer größeren Stadt untereinander sicher zu kommunizieren. Die Ausgangssituation setzt eine Positionierung in unterschiedlichen Lagern um die Stadt herum voraus. Aus dieser verteilten Stellung mussten sie kommunizieren, wobei die Gefahr bestand, dass die Boten abgefangen wurden oder selbst ihre Generäle hintergingen. Eine erfolgreiche Belagerung war aber nur in Aussicht, wenn sie entweder einheitlich die Stadt angriffen oder gemeinsam ausharten. Eine dezentral generierte Einigung musste sichergestellt werden. Diese Problemstellung lässt sich in die Blockchain Technologie übertragen. Unterschiedliche Fullnodes müssen sich auch hier darüber einig werden, welches der nächste Block in der Kette der Blockchain ist. Und auch hier müssen sie eine Einigung erzielen und das unabhängig voneinander. Bei der Lösung des Problems kommt das implizite Wissen über die Anzahl der Fullnodes zum Tragen. In jeder Runde, in der ein Block persistiert werden soll, wird zufällig einer der Nodes ausgewählt, der den neuen Block vorschlagen darf. Dies erfolgt, indem den Block ins Blockchain-Netzwerk sendet und dieser dort geprüft wird. Jeder andere Node, der den Vorschlag erhält, validiert den Block. Dies geschieht unter anderem dadurch, dass aufgerufene Smart Contracts nachgerechnet werden. Bei korrektem Ablauf sollte das Ergebnis übereinstimmen, so das auch die Transaktion, welche das Ergebnis darstellt in den Block aufgenommen werden kann und dem vorgeschlagenen Wert entspricht. Wenn das der Fall ist, sendet der Fullnode seine Bestätigung ins Netzwerk, andernfalls seine Ablehnung. Also erwartet jeder validierende Fullnode von jedem anderen eine Antwort. So kann am Ende einer Runde jeder Fullnode prüfen, ob er mindestens von 2/3 aller Fullnodes eine Bestätigung erhalten hat. Falls ja, kann er den neuen Block anhängen, wenn die Mehrheit ein anderes Ergebnis hat, dann muss er sich mit der Mehrheit synchronisieren. Dieses Konsensmechanismus gewährleistet, dass das Tendermint Netzwerk funktionsfähig bleibt, solange die fehlerhaften Fullnodes echt kleiner als 1/3 aller Fullnodes sind. Die Quote schließt sowohl böswillig handelnde Nodes ein, als auch Nodes, die einfach offline sind oder z.B. zu hohe Latenzen haben und nicht rechtzeitig antworten.

Für den Empfang der nicht verkörperten Erklärung ändert sich die Situation auch bei der Tendermint-Blockchain nicht. Auch hier kann kein Zeitpunkt oder ein Status definiert werden, der garantiert, dass eine Trans-

6_116, S. 601.

62 Configuration, https://docs.tendermint.com/v0.34/tendermint-core/configuration.html.

63 Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4, 3 (July 1982), S. 382–401. https://doi.org/10.1145/357172.357176.

aktion im Machtbereich des Empfängers ist. Aber für die verkörperte Erklärung, also die in einem Block persistierte Transaktion, gibt es hier qualitative Vorteile. Die Blockbildung ist zum einen deutlich schneller, als auch die Finalisierung eines Blockes ist zuverlässiger, da dieser mit dem Persistieren direkt final und unveränderlich ist.

2. Schlussfolgerungen und Ausblick

Eine pauschale Bewertung des Zeitpunkts des Zugangs ist ausgeschlossen. Selbst innerhalb desselben Blockchain-Frameworks kann die Kommunikation aufgrund abweichender Implementierungen und Policies von Netzwerk zu Netzwerk unterschiedlich ablaufen. Die konkreten Verarbeitungsvorgänge sind jeweils zu untersuchen. Ferner sind die rechtlichen Wertungen auf Basis bestehender Rahmenverträge zu berücksichtigen, um Rechtsfragen zum Wirksamwerden von rechtsgeschäftlichen Erklärungen und rechtsgeschäftsähnlichen Handlungen zu beantworten. Die eindeutige Zuweisung der elektronischen Erklärungen zu Rechtsträgern von am Blockchain-Netzwerk teilnehmenden Entitäten bedarf der rechtlich und technisch validen Konzeptionierung und Implementierung. Dabei sind die Erklärungen entsprechend aufgesetzter Rollen- und Berechtigungskonzepte unter Verwendung von gültigen Zertifikaten und elektronischer fortgeschrittener oder qualifizierter Signaturen von den digitalen Identitäten zu senden.

Die rapiden Entwicklungen der unterschiedlichen Blockchain Frameworks erfordert die Festlegung von Standards, um eine wirtschaftliche Rentabilität aufgrund kontrollierter Transaktionskosten und ein hohes Maß an Rechtssicherheit zu gewährleisten. Die Code-Qualität bedarf dezidierter Überprüfung im Wege von Code-Auditing. Dabei sind die Anbahnung und Durchführung von Rechtsgeschäften im Zahlungsverkehr als kritische Infrastrukturabläufe zu bewerten. Hier bietet sich an, dass die Marktteilnehmer Normen zur (Selbst-) Regulierung und (Selbst-)Kontrolle anstreben, ähnlich zur Regulierung von Hoch-Risiko-KI.