Joachim Dorschel / Stephan Manz

Contract Management in der Blockchain

Verträge sind rechtlich bindende Vereinbarungen zwischen zwei oder mehr Personen, den Vertragsparteien. Ein Vertrag ist gekennzeichnet durch die Identität der Parteien, den Vertragsinhalt und die Rechtsfolgen, die die jeweils anwendbare Rechtsordnung ihnen beimisst. Der Vertragsinhalt wird durch gemeinsame oder wechselseitige Vertragserklärungen festgelegt. Dies sind typischerweise geschriebene Texte oder Abbildungen, mündliche Aussagen, Gesten oder in Software implementierte Algorithmen.

Keine Formvorschriften für Vertragserklärungen

Das deutsche Recht stellt es den Vertragsparteien grundsätzlich frei, welche Form sie für ihre Vertragserklärungen wählen. Nur in besonders geregelten Ausnahmefällen, etwa bei Verfügungen über Grundstücke oder GmbH-Geschäftsanteile, schreibt das Gesetz eine bestimmte Form vor. Die gängigsten gesetzlichen Formerfordernisse sind die Schriftform und die notarielle Beurkundung.

Kommt es zum Streit über den Inhalt oder die richtige Anwendung eines Vertrages, ist es entscheidend, Klarheit darüber zu schaffen, welcher Vertragsinhalt zwischen welchen Parteien tatsächlich vereinbart wurde. Mitunter stellt sich auch die Frage, ob die handelnden Personen berechtigt waren, für die beteiligten Parteien im Rechtsverkehr aufzutreten, juristisch gesprochen, ob sie Vertretungsmacht besaßen. Ist ein Vertrag notariell beurkundet, ist die Situation einfach. Der Notar verfügt über eine durch seine Urkundenrolle eindeutig identifizierte Fassung des Vertrages. Da er die Vertretungsmacht der vor ihm handelnden Personen bei der Beurkundung überprüfen muss, ist die Frage einer ausreichenden Bevollmächtigung ebenfalls nachweisbar beantwortet.

Bei einem Vertrag, bei dem das Gesetz Schriftform vorschreibt, existiert mindestens ein von allen Vertragsparteien unterzeichnetes Originaldokument, welches, wenn es vorliegt, den Vertragsinhalt eindeutig dokumentiert. Die Frage einer ausreichenden Bevollmächtigung ist dagegen im Vertrag selbst nicht dokumentiert. Will man eine beweissichere Situation für die Zukunft schaffen, muss man die Originalvollmachten zusammen mit dem Vertrag aufbewahren. Bei Vollmachten, die sich aus Unterschriftenregelungen in Konzernen ergeben, ist dies in aller Regel nicht praktikabel und auch nicht üblich. In allen anderen Fällen gibt es keine gesetzlichen Mechanismen, Inhalt und Parteien eines Vertrages sicher festzustellen.

Aufgrund handels- und steuerrechtlicher Bestimmungen sind Unternehmen verpflichtet, Handelsbriefe in einer geordneten Ablage aufzubewahren. Hierzu zählen auch Vertragserklärungen. In der Praxis haben sich zu diesem Zweck Dokumentenmanagement- und Archivsysteme etabliert, die eine revisionssichere Ablage solcher Dokumente sicherstellen. Eine digitale Ablage ist in der Unternehmenspraxis etabliert und rechtlich unproblematisch zulässig, wenn bestimmte Regeln der ordnungsgemäßen Datenverarbeitung beachtet werden.

Verträge in der Blockchain

Die Abbildung von Verträgen in der Blockchain ist ein nahe liegendes und in zahlreichen Projekten untersuchtes Anwendungsszenario. Die Blockchain-Technologie ermöglicht eine dauerhafte und unveränderliche Dokumentation von Ereignissen. Bei solchen Ereignissen kann es sich, wie im Fall von Bitcoin, um Transaktionen handeln, genauso aber um andere kommunikative Inhalte, etwa Vertragserklärungen oder die Stimmabgabe zur Herbeiführung eines Gesellschafterbeschlusses. Die Blockchain bietet sich überall dort als Basistechnologie an, wo Zweifel über das Ob und Wann rechtserheblicher Erklärungen oder deren Inhalt entstehen können und die Umstände eine sichere Aufklärung und Beseitigung solcher Zweifel verlangen.

Bei der Konzeption entsprechender Lösungen ist zu unterscheiden zwischen der Do-

Joachim Dorschel und Stephan Manz, beide Managing Partner, DPS & Manz Innovations GmbH, Leinfelden-Echterdingen

Welche Auswirkungen wird der Einsatz der Blockchain-Technologie in der gesamten Wirtschaft und damit auch in der Finanzindustrie haben? Wo und wie schnell wird sie sich durchsetzen? Welche Prozesse und Strukturen werden sich ändern? All diese Fragen verbreiten derzeit nicht nur in der Finanzbranche eine große Unsicherheit. Die Autoren nähern sich den Antworten mit Blick auf die Möglichkeiten und Grenzen rund um das Vertragswesen. Ihr Fazit: Die Blockchain ist heute noch keine geeignete Technologie für das klassische Vertragsmanagement. Einen Mehrwert bietet die Technologie aber bei der Schaffung einer sicheren Beweislage. Das wesentliche Defizit beim heutigen Stand der Technik sehen sie in dem Fehlen einer sicheren, allgemein gültigen und praktisch leicht nutzbaren digitalen Identität. Hinsichtlich der Vielfalt der derzeit laufenden Initiativen und Vorhaben halten sie es für entscheidend, verschiedene Ansätze der Identifikation so zu integrieren, dass ein Einsatz über Insellösungen hinweg möglich ist. (Red.)

kumentation von Erklärungsinhalten, Sender und Empfänger der Erklärung und den möglicherweise erforderlichen Vollmachten oder sonstigen Berechtigungen.

Erklärungsinhalte: Die Blockchain ist für die Ablage kleinerer Datenmengen gemacht. Die Gebühren, die man für die Aufnahme einer Transaktion an einen Miner zu entrichten hat, werden je Kilobyte berechnet. Auch wenn die Preise bei den heute etablierten Blockchains wie Bitcoin und Ethereum noch stark variieren und erheblichen Schwankungen ausgesetzt sind, darf man davon ausgehen, dass die Ablage ganzer Dokumente mit einer Größe von mehreren Megabyte in der Regel unwirtschaftlich ist.

Jederzeitige Überprüfbarkeit

Aufgrund der hohen Kosten für Datenvolumina ist es in der Blockchain die Regel, nicht die Originaldateien, sondern deren Hash-Werte abzulegen. Der Hash-Wert einer Datei ist eindeutig. Die Speicherung des Hash-Wertes einer mit einem Timestamp versehenen Datei in der Blockchain erlaubt eine sichere Aussage darüber, dass genau diese Datei mit ihrem jeweiligen Inhalt zu einem bestimmten Zeitpunkt abgelegt wurde. Es ist allerdings nicht möglich, aus dem Hash-Wert den Inhalt der Originaldatei zu bestimmen. Der Hash-Wert eines Vertragsdokuments in der Blockchain hat also nur so lange Aussagekraft, wie die Originaldatei vorhanden ist.

Der praktische Nutzen der Blockchain-Technologie ergibt sich also aus der Möglichkeit, die Hash-Werte von Vertragsinhalten und Vertragserklärungen dauerhaft und unverfälscht abzulegen, sodass, das Vorhandensein der Originaldateien vorausgesetzt, jederzeit überprüft und nachgewiesen werden kann, dass Erklärungen eines bestimmten Inhalts zu einem bestimmten Zeitpunkt abgegeben wurden. Um den Beteiligten eine sinnvolle Überprüfung zu ermöglichen, sollte ein Hashing-Algorithmus gewählt werden, bei dem ein identischer Dateiinhalt stets denselben Hash-Wert ergibt, unabhängig von dem Betriebssystem, dem Dateinamen und anderen umgebungsabhängigen Faktoren, also jede unveränderte Kopie der Datei denselben Hash-Wert ergibt.

Smart Contracts: Smart Contracts werden als idealer Anwendungsfall der Blockchain gehandelt. Es gibt nicht wenige Prophezeiungen, wonach Blockchain-implementierte Smart Contracts Notare und Gerichte langfristig überflüssig machen werden. Bedenkt man die Breite und Vielfalt der in der Finanzindustrie verwendeten Vertragstypen ergibt sich freilich ein differenzierteres Bild.

Dabei ist zunächst festzuhalten, dass ein Smart Contract nicht zwingend in einer Blockchain implementiert sein muss. Smart Contracts sind Computerprogramme, in denen Vertragsinhalte implementiert sind, die sonst in menschlicher Sprache formuliert wären. Als Beispiel mag man sich ein Programm vorstellen, das eine Kaufpreiszahlung automatisch auslöst, wenn diese fällig, also die Kaufsache übergeben und übereignet ist. Die Blockchain sorgt in einem solchen Szenario für eine Unverfälschbarkeit der implementierten Vertragsinhalte und Erfüllungshandlungen und erlaubt damit eine sichere Abwicklung von Verträgen zwischen Parteien, die einander im Zweifel nicht kennen und somit auch nicht vertrauen. Dies gilt freilich unter der Voraussetzung, dass die Implementierung frei von Programmfehlern erfolgte.

Kein Bedarf an menschlicher Intervention

Smart Contracts eignen sich nur für solche Vertragsregeln, die einer Umsetzung durch Computeralgorithmen zugänglich sind, also keiner menschlichen Intervention bedürfen. Dies sind typischerweise solche Regeln, die mit Mitteln der Mathematik (zum Beispiel Zinsberechnungen) oder logischen Verknüpfungen (zum Beispiel das Vorliegen oder Nichtvorliegen von Zustimmungserklärungen) beschrieben werden können. Wo die Bestimmung einer Rechtsfolge juristischer Wertungen bedarf, ist eine Umsetzung der jeweiligen Vertragsbestimmung in einem Smart Contract kaum möglich.

Bei den in Smart Contracts abbildbaren Vertragsregeln ist zu unterscheiden zwischen solchen, bei denen sich Regelwerk, Tatbestand und Rechtsfolgen ausschließlich in der Blockchain realisieren und solchen, bei denen eine Anbindung an externe Systeme, sogenannte Orakel, erforderlich ist. Ein Beispiel für die erstgenannte Ausprägung ist eine Darlehensabrede, bei der die Zeitpunkte für Zins- und Tilgungszahlungen von vornherein feststehen und die Zahlungen in einer Kryptowährung aus der Blockchain selbst heraus erfolgen. Bei der zweitgenannten Ausprägung kann es sich beispielsweise um ein derivatives Finanzinstrument handeln, bei denen die Rechte und Pflichten von Marktdaten abhängen, die ein externes System zuliefert.

Identifizierung durch einen Private Key

Identifizierung der Vertragsparteien: In der analogen Welt dokumentieren die Parteien eines Vertrages ihre Erklärungen durch ihre Unterschrift oder digital verfasste Willenserklärungen. Häufig sind auch Kombinationen, etwa der Austausch unterzeichneter und gescannter Dokumente per E-Mail. Es hängt von der gewählten Form ab, wie sichergestellt werden kann, dass eine Erklärung tatsächlich von der angegebenen Vertragspartei stammt. Der klassische Weg ist die eigenhändige Unterzeichnung, bei der im Streitfall über ein Schriftgutachten geklärt werden kann, ob eine Unterschrift tatsächlich von dem angegebenen Urheber stammt.

In der Blockchain identifizieren sich die Parteien typischerweise durch einen Private Key. Hierdurch ist eindeutig und nahezu fälschungssicher dokumentiert, dass die in der Blockchain abgelegte Erklärung vom Inhaber des Private Key stammt.

Problematisch ist die Zuordnung des Private Key zu der Person des Erklärenden. In etablierten Blockchain-Netzwerken wie Bitcoin endet die sichere Zuordnung beim Private Key. Wer Inhaber des Private Key ist, kann über die in der Blockchain gespeicherten Bitcoins verfügen. Angriffe auf das System richten sich daher typischerweise auch nicht auf die Blockchain selbst, sondern auf die Wallets, in denen die Private Keys abgelegt sind. Bei Verlust des Private Key sind die hiermit verbundenen Bitcoins für den Inhaber für immer verloren.

Um die Blockchain sinnvoll im Vertragsmanagement einzusetzen, muss eine hinreichend sichere Verbindung zwischen dem Private Key und der Vertragspartei geschaffen werden. Ein sicherer Weg ist hier die elektronische Signatur nach dem Signaturgesetz. Der Zertifizierungsdiensteanbieter (ZDA), der die elektronische Signatur bereitstellt, ist nach dem Signaturgesetz verpflichtet, den Signaturinhaber zu iden-

tifizieren. Das vom ZDA ausgestellte Zertifikat, also der öffentliche Schlüssel, impliziert die Aussage, dass es sich bei dem Verwender der Signatur um die identifizierte Person handelt. In der Praxis hat sich die qualifizierte elektronische Signatur jedoch kaum durchgesetzt, da Erwerb und Nutzung als unpraktisch und aufwendig gelten.

Eine weitere Möglichkeit der sicheren digitalen Identifikation bietet der in den Personalausweisen integrierte Chip (eID). Dort sind die für eine rechtssichere Identifikation des Ausweisinhabers notwendigen Informationen verschlüsselt gespeichert. Durch eine entsprechende Integration in den für den Vertragsabschluss genutzten Dienst ist die Identifizierung des Teilnehmers so lange sicher möglich, wie dieser im Besitz des Personalausweises und der Zugangsdaten zu dem Chip ist.

Praktikabilität als Schlüsselkriterium

Auch hier ist der entscheidende Nachteil die Praktikabilität. Für die Nutzung der eID ist ein Kartenleser erforderlich. Die Zugangsdaten werden vom Bürgeramt per Post verschickt. Obwohl seit einigen Jahren alle neuen Personalausweise über einen Chip verfügen, wird dieser in der Praxis kaum genutzt. Für Contract Management Services ist weiterhin die Beschränkung auf Deutschland hinderlich. Solche Services werden insbesondere dort benötigt, wo Vertragsparteien einander nicht kennen und die Identität nicht einfach überprüft werden kann. Dies ist typischerweise bei internationalen Sachverhalten der Fall. Mehrere prominente Initiativen haben das Bedürfnis nach einer einfachen und gleichwohl sicheren und ubiquitär nutzbaren elektronischen Identität erkannt.

Einige deutsche Großunternehmen, unter anderem die Deutsche Bank, Allianz, Daimler und Axel Springer, haben sich zusammengeschlossen, einen gemeinsamen „Web-Schlüssel" oder „Master Log-in Zugang" für die rechtssichere Identifikation gegenüber digitalen Diensten zu entwickeln. Das Projekt wurde unter dem Namen DIPP im Mai 2017 vorgestellt.

Diverse Forschungsinitiativen untersuchen die Entwicklung einer digitalen Identität auf Basis der Blockchain-Technologie (Self-Sovereign Identity). Einige Publikationen weisen insbesondere auf die Möglichkeiten von Kreditinstituten hin, regulatorisch gebotene Know-Your-Customer (KYC)-Lösungen mittels Blockchain über das Institut hinaus verfügbar zu machen.

Nutzung von konventionellen Verfahren der Authentifizierung

Selbstverständlich besteht die Möglichkeit, auch konventionelle Verfahren der Authentifizierung einer Person im Internet zu nutzen, etwa die im E-Commerce weit verbreitete Anmeldung mit einer per Double-Opt-in verifizierten E-Mail-Adresse. Technisch bieten solche Verfahren längst nicht die gleiche Sicherheit wie die auf Kryptografie basierende elektronische Signatur oder die eID.

Es gibt nach aktueller Rechtsprechung auch keinen generellen Anscheinsbeweis, dass die bestimmungsgemäße Nutzung von Zugangsdaten zu einem User Account stets durch den Inhaber erfolgt ist, mit der Folge, dass eine missbräuchliche Nutzung von der anderen Vertragspartei zu beweisen wäre. Diese Rechtsauslegung wird von Juristen mit der Tatsache begründet, dass die typischen Zugangssicherungen zu User Accounts mittels User-ID oder E-Mail-Adresse und Passwort von technisch versierten Dritten leicht ausgespäht werden könnten und in der Praxis auch regelmäßig werden.

Tragfähige Konzepte für ein Contract Management auf Blockchain-Basis stehen und fallen daher mit der technischen Absicherung der Identität der Parteien.

Vollmachten

Für den Nachweis einer Vollmacht gilt nichts anderes als für die Vertragserklärung selbst. Die Berechtigung für einen Dritten, sei es eine natürliche oder eine juristische Person, ergibt sich entweder von Gesetzes wegen oder durch eine entsprechende Bevollmächtigung. Vollmachten können in gleicher Weise über die Blockchain gesichert werden wie Vertragserklärungen.

Einen deutlichen Mehrwert könnte die Blockchain dort bieten, wo Vollmachten von unterschiedlichen Vertragspartnern immer wieder überprüft werden müssen. Dies ist etwa bei Unterschriftsberechtigungen in Konzernen der Fall. Es ist heute nur schwer möglich, nach einigen Jahren zu überprüfen, ob eine bestimmte Person bei Abschluss eines Vertrages über die notwendige Vertretungsmacht verfügte. Kommt es, zum Beispiel im Rahmen einer Due Diligence, hierauf an, ist häufig eine aufwendige Aktenrecherche notwendig. Ein Ansatz, der die Vertretungsrechte einschließlich deren Veränderungen im Zeitablauf eindeutig und irreversibel dokumentiert, könnte dieses Problem leicht lösen. Voraussetzung wäre allerdings, dass sich die Nutzer eines solchen Systems auf ein gemeinsames Protokoll zur elektronischen Abbildung von Vertretungsregelungen verständigen. Dies ist freilich keine technische oder rechtliche Frage, sondern eine des politischen Willens.

Keine geeignete Technologie für das klassische Vertragsmanagement

Die Blockchain ist heute keine geeignete Technologie für das klassische Vertragsmanagement. Die Dokumentenablage muss je nach Anwendung bei einer Partei, einer gemeinsam genutzten Cloud-Ressource oder in einer verteilten Datenbank erfolgen.

Einen Mehrwert bietet die Blockchain bei der Schaffung einer sicheren Beweislage. Erklärungen, die einmal in der Blockchain verschlüsselt wurden, sind dort unveränderlich abgelegt. Solange zumindest eine Kopie der Originaldatei existiert, kann stets sicher bewiesen werden, dass eben diese Erklärung zum fraglichen Zeitpunkt abgegeben wurde.

Das wesentliche Defizit beim heutigen Stand der Technik ist das Fehlen einer sicheren, allgemein gültigen und praktisch leicht nutzbaren digitalen Identität.

Lösungen, die sich in der Finanzindustrie dauerhaft etablieren wollen, werden hierauf eine Antwort geben müssen. Dabei wird es mit Blick auf die Vielfalt der Initiativen und Vorhaben entscheidend darauf ankommen, verschiedene Ansätze der Identifikation so zu integrieren, dass ein Einsatz über Insellösungen hinweg möglich ist. Dabei kann es je nach Kritikalität des konkreten Falls durchaus unterschiedliche Sicherheitslevel geben, sodass Praktikabilität und Rechtssicherheit unter Risikogesichtspunkten in einem ausgewogenen Verhältnis stehen.