



Blockchain und das Notariat – Interview mit Jörn Erbguth

Jörn Erbguth, was ist eine Blockchain aus technischer Sicht?

Erbguth: Es gibt viele Spielarten von Blockchains. Den verschiedenen Spielarten der Blockchain ist gemeinsam, dass wir es mit einer Datenablage in Blöcken zu tun haben. Diese Blöcke werden nicht verändert und kryptografische Verfahren sowie ein Konsensmechanismus sorgen dafür, dass keine Blöcke entfernt werden können. Blockchains haben keine zentrale Koordination. Der Konsensmechanismus sorgt dafür, dass trotzdem eine Abstimmung unter den Beteiligten stattfindet, welche Transaktionen in den nächsten Block einer Blockchain aufgenommen werden.

Und was ist eine Blockchain aus juristischer Sicht?

Erbguth: Auch wenn es keine juristische Definition gibt, so beziehen zunehmend Gesetze gezielt die Blockchain-Technologie mit ein. So hat Frankreich im Jahr 2016 im Code monétaire et financier im Artikel L223-12 diese als „un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations“ beschrieben. In Liechtenstein wird im aktuellen Gesetzentwurf von „auf vertrauenswürdigen Technologien beruhende Transaktionssystemen“ gesprochen. Mit solchen, möglichst technologieneutralen Formulierungen, sollen auch künftige technische Entwicklungen umfasst werden.

Aus juristischer Sicht ist die zentrale Eigenschaft von Blockchains die technische Absicherung von Transaktionen über das Peer-to-Peer-Prinzip ohne zentrale Kontrolle. Daraus ergibt sich in rechtlicher Hinsicht eine Verteilung der Kontrolle auf viele Beteiligte und es ist häufig eine offene Frage, wer in einem solchen System die rechtliche Verantwortung trägt.

Weshalb werden Blockchains immer wieder in Verbindung mit den Aufgaben der Notar/innen gebracht?

Erbguth: Die Arbeit der Notarinnen und Notare wird mit Vertrauen assoziiert. Ein Dokument, das bei einem Notar liegt, so die Idee, wird nicht verändert und kommt auch nicht abhanden. Die Tatsache, dass Blockchains auch eine Form von

Vertrauen herstellen können, scheint diese Assoziation mit Notaren zu befördern. Ich teile aber die Meinung nicht, dass Blockchains die Tätigkeiten von Notarinnen und Notaren eins zu eins abbilden könnten.

Weshalb nicht?

Erbguth: Mit Blockchains kann die Einhaltung von Transaktionsregeln sichergestellt werden. Dabei kann jedoch nur schematisch geprüft werden. Blockchains sind dann am Limit, wenn im Einzelfall ein bestimmtes Schema nicht anwendbar ist. Ich sehe durchaus, dass mit Blockchains einfache Dienstleistungen automatisiert werden können. Aber wenn der über Blockchains realisierte Automatismus nicht passt, dann ist "manuelles Vertrauen" gefragt. Deshalb können sich die Arbeit von Notarinnen und Notaren und die der Blockchain-Technologie gut ergänzen.

Wie könnte diese Ergänzung in der Praxis aussehen?

Erbguth: Die Sicherheitsmechanismen von Blockchains sehen ja vor, dass man sich als Beteiligter einer Blockchain mit einem oder mehreren privaten Schlüsseln authentisiert. Verliere ich meine privaten Schlüssel, dann habe ich keinen Zugriff mehr auf meine Assets in der Blockchain. Wer hingegen den oder die Schlüssel erspäht hat, kann mir meine Assets wegnehmen. Angriffe auf private Schlüssel sind das häufigste Angriffsszenario auf Krypto-Assets. Die Frage ist daher: Was geschieht, wenn etwas Unvorhergesehenes passiert? Wie finden Nachkommen im unvorhergesehenen Todesfall des Erblassers dessen Assets auf der Blockchain und den oder die dazugehörigen privaten Schlüssel? Wenn es um die Vorsorge für digitale Assets geht, dann ist das Vertrauen von Notaren gefragt. Das gilt auch für viele andere Ausnahmesituationen, die man nicht programmieren kann.

Wenn sich ein Notar oder eine Rechtsanwältin intensiver mit Blockchains auseinandersetzen möchte: Welche Fragen gäbe es zu bearbeiten?

Erbguth: Die Blockchain-Technologie hat neue Geschäftsfelder entstehen lassen, zu denen die bestehenden Regulierungen häufig nicht passen. Das betrifft neben der Finanzmarktregulierung auch viele weitere Bereiche und ist ein weites Betätigungsfeld für Juristen. Weitere Möglichkeiten ergeben sich aus der Unveränderlichkeit der auf Blockchains abgelegten Informationen. Ergeben sich nach Ablage eines Vertrags oder einer Transaktion auf einer Blockchain unvorhergesehene Änderungen, so wird der Eintrag auf der Blockchain die neue Situation nicht immer adäquat regeln. Jurist/innen kümmern sich ja auch jenseits von Blockchains um diese Art von Konflikten und versuchen zu ergründen, wie man solche Situation geregelt hätte, wenn man an sie gedacht hätte. Solche Situationen wird es im Umfeld der Blockchain-Technologie noch viel häufiger geben. Notare und Rechtsanwälte sind also immer dann gefragt, wenn bei automatisierten Dienstleistungen Fälle auftreten, an die man nicht gedacht hat – wenn also der Formalismus einer Blockchain nicht zum richtigen Ergebnis führt.

Es heisst, Register, wie etwa das Grundbuch, könnten künftig auf der Blockchain geführt werden? Wie funktioniert das?

Erbguth: Es gibt grob gesagt zwei Ansätze, Blockchains für öffentliche Register zu verwenden. Zum einen könnte das Registeramt durch eine Blockchain ersetzt werden. Über ein „Smart Contract“ genanntes Programm auf einer Blockchain werden die Berechtigungen und die Transaktionen automatisiert geprüft und direkt ausgeführt. Bei Grundbüchern ist dies jedoch eine so komplexe Angelegenheit, dass das noch in weiter Ferne liegt.

Der andere, etwas oberflächlichere Ansatz des Einsatzes von Blockchains für Register besteht darin, sie als ergänzende, vertrauensbildende Technologie einzusetzen. In diesen Fällen wird beispielsweise ein Grundbuch nach wie vor zentral geführt. Transaktionen, Auszüge – oder auch nur deren Hashwerte – werden aber auf einer Blockchain hinterlegt, gewissermassen als Sicherung gegen unautorisierte Änderungen. Das ist beispielsweise beim Handelsregister in Genf oder dem Grundbuch in Georgien der Fall. In Regionen, in denen Korruption herrscht, erhofft man sich von einer solchen Überprüfbarkeit durch eine Blockchain die Korruption eindämmen zu können. Das funktioniert insofern, als unberechtigte Änderungen effektiv nicht spurlos ausgeführt werden können. Es schützt aber natürlich nicht gegen das Durchführen eigentlich nicht zulässiger Transaktionen durch Berechtigte. Die Blockchain verbessert hier also die Beweislage – den Rest muss auch weiterhin ein funktionierender Rechtsstaat gewährleisten.

Sie bearbeiten auch Fragen zu Datenschutz und Blockchain. Freuen sich Datenschützer über die Blockchain-Technologie?

Erbguth: Datenschützer sind in Bezug auf Blockchains ambivalent. Einerseits besteht in Blockchains datenschutztechnisch ein grosses Potential. Die Datenskandale der letzten Jahre bestanden ja zu einem grossen Teil darin, dass Unternehmen grosse zentrale Datensammlungen missbräuchlich verwendet haben oder dass diese Datensammlungen gehackt wurden. Die Datenschutzgrundverordnung versucht daher, die Unternehmen scharf zu regulieren, die die Kontrolle über große Datenbestände haben. Dieses Vorgehen ist mit mittelmässigem Erfolg gesegnet. Potential haben Blockchains in diesem Bereich deshalb, weil sie es ermöglichen, Datensammlungen zu dezentralisieren und damit grosse Sammlungen personenbezogener Daten zu vermeiden. Damit wird in vielen Fällen der mögliche Schaden reduziert. Das Konzept der self-sovereign Identity sieht beispielsweise vor, dass die Informationen zu einer Person dezentral abgelegt werden und eine Blockchain dazu eingesetzt wird, diese Informationen zu authentifizieren. Damit haben die Nutzerinnen und Nutzer die Möglichkeit selbst zu entscheiden, wer auf welche Inhalte zugreifen kann.

Die Unveränderbarkeit der Blockchain-Technologie ist nicht gerade kompatibel mit Datenschutzprinzipien.

Erbguth: Datenschützer legen Wert darauf, dass Daten nur so lange gespeichert werden, wie sie benötigt werden. Daher spielen Berichtigungs- und Löschbegehren im Datenschutz eine wichtige Rolle – bis hin zum Recht auf Vergessenwerden. Insofern besteht ein Zielkonflikt zwischen Blockchain-

Technologie und Datenschutz. Es gibt hierzu eine Reihe von technischen und juristischen Lösungsansätzen.

Sehen Sie Bereiche, in denen der Datenschutz „zu weit“ geht?

Erbguth: Zu weit geht möchte ich nicht sagen. Aber der Datenschutz und insbesondere die DSGVO sind nicht ausreichend technologieneutral. Der heutige Ansatz im Datenschutz geht davon aus, dass eine Datenverarbeitung von einem oder vielleicht auch zwei oder drei Unternehmen kontrolliert wird. Man müsse daher nur diese Unternehmen ausreichend mit Auflagen und Strafdrohungen versehen, um ein gutes Datenschutzniveau zu erreichen. Bei Peer-to-Peer-Technologie, wie zum Beispiel Blockchain, liegt die Kontrolle jedoch in den Händen vieler. Das verringert den Einfluss der Einzelnen und schützt die Daten vor Manipulation und Missbrauch. Doch was bedeutet dies für die Regulierung? Weder scheint es angemessen, alle Beteiligten für alle Datenverarbeitungen in Peer-to-Peer-Systemen verantwortlich zu machen, gerade weil sie diese praktisch nicht beeinflussen können. Doch auch ein Ergebnis, welches davon ausgeht, dass in bestimmten Fällen niemand verantwortlich sei, erscheint problematisch.

Wie lässt sich abschätzen, ob eine Idee für den Einsatz von Blockchains tauglich ist?

Erbguth: Bei Blockchains werden alle Daten auf allen Knoten gespeichert. Im Allgemeinen ist das sehr ineffizient. Daher lohnt sich der Einsatz von Blockchains nur dort, wo eine hohe Manipulationssicherheit und Autonomie des Systems gefordert ist. Wenn Sie ein Projekt statt mit einer Blockchain genauso gut mit einer konventionellen Datenbank umsetzen können, sollten Sie auf den Einsatz von Blockchains verzichten. Der Blockchain-Hype ist vorüber und damit auch die Zeit der Projekte, die Blockchain nur aus Gründen des Marketings verwendet haben. Seriöse Projekte beschäftigen sich zudem von Anfang an mit Fragen des Datenschutzes (privacy by design). Sie legen auch fest, wie mit Fehler- und Ausnahmefällen umgegangen wird. Die Regelung dieser Governance ist ein wichtiger Punkt, damit Blockchain-Anwendungen dauerhaft funktionieren und nicht an den früher oder später immer auftretenden Ausnahmefällen scheitern. Dabei können Notarinnen und Notare eine wichtige Rolle spielen.

Die Fragen stellte RA Claudia Schreiber (Advokatur Schreiber, Support elektronische Kanzlei SEK, Bern).

Jörn Erbguth (<https://erbguth.ch>) wohnt und arbeitet in Genf. Er ist Diplom Jurist und Diplom Informatiker und arbeitet derzeit neben seiner Beratertätigkeit zu Blockchain, Smart Contracts und Datenschutz an einer Dissertation zum Thema Blockchain Governance an der Universität Genf. Erbguth ist auch Vorstandsmitglied des Vereins [entscheidsuche.ch](https://www.entscheidsuche.ch)



Blockchain et notariat – Interview de Jörn Erbguth

Jörn Erbguth, qu'est-ce qu'une blockchain d'un point de vue technique?

Erbguth: Il existe de nombreuses variantes de blockchains. Tous les types de blockchain ont en commun qu'il s'agit de stockage de données en blocs. Ces blocs ne sont pas modifiables et des procédures cryptographiques ainsi qu'un mécanisme de consensus garantissent qu'aucun bloc ne peut être supprimé. Les blockchains fonctionnent sans organe central de contrôle. Le mécanisme de consensus permet de garantir qu'il existe pourtant une coordination entre les participants sur les transactions à intégrer dans le bloc suivant d'une blockchain.

Et qu'est-ce qu'une blockchain d'un point de vue juridique?

Erbguth: Même s'il n'existe pas de définition juridique, les lois intègrent de plus en plus la technologie de la blockchain. Ainsi, en 2016, le Code monétaire et financier français décrit à l'article L223-12 la technologie blockchain comme étant: „un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations“. Au Lichtenstein, le projet de loi actuel parle de „auf vertrauenswürdigen Technologien beruhende Transaktionssystemen“. De telles formulations, les plus neutres possible technologiquement parlant, permettent d'englober également d'éventuels développements techniques futurs.

D'un point de vue juridique, la caractéristique centrale de la blockchain est la sécurisation technique des transactions via le principe du peer-to-peer sans contrôle central. Ainsi, au niveau juridique, le contrôle est réparti entre de nombreux participants, et la question de savoir qui porte la responsabilité juridique dans un tel système se pose fréquemment et reste ouverte.

Pourquoi les blockchains sont-elles régulièrement associées aux tâches des notaires?

Erbguth: Le travail du/de la notaire est associé à la confiance. Un document conservé par un notaire ne peut, c'est l'idée, être modifié ni se perdre. Le fait que les blockchains peuvent créer également une forme de confiance semble favoriser cette association avec les notaires. Je ne partage toutefois pas l'opinion selon laquelle les blockchains pourraient reproduire précisément les activités des notaires.

Pourquoi pas?

Erbguth: Les blockchains peuvent assurer le respect des règles de transaction. Cependant le contrôle n'est possible que de façon schématique. Les blockchains atteignent leur limite si un certain schéma n'est pas applicable dans un cas particulier. Je considère que des prestations simples peuvent être automatisées au moyen de blockchains. Mais si la fonction automatique exécutée par la blockchain ne convient pas, alors une action manuelle est nécessaire («confiance manuelle»). Ainsi le travail des notaires et celui de la technologie de la blockchain peuvent bien se compléter.

A quoi cette complémentarité pourrait-elle ressembler dans la pratique?

Erbguth: Les mécanismes de sécurité des blockchains prévoient une authentification du participant à une blockchain au moyen d'une ou de plusieurs clés privées. Si je perds ma clé privée, je n'ai plus accès à mes actifs dans la blockchain. Celui qui, en revanche, a repéré la ou les clés, peut me prendre mes actifs. Les attaques sur les clés privées constituent le scénario d'attaque le plus courant sur les actifs cryptographiques. La question est donc: que se passe-t-il lorsqu'un événement imprévu survient? En cas de décès imprévu, comment les descendants trouvent-ils les actifs du défunt sur la blockchain et la ou les clés privées correspondantes? Pour ce qui touche à la prévoyance des risques concernant des actifs numériques, la «confiance manuelle» est utile. C'est le cas également dans beaucoup d'autres situations exceptionnelles qui ne peuvent être programmées.

Quelles seraient les questions à traiter pour un notaire ou une avocate qui souhaiterait aborder les blockchains de manière plus approfondie?

Erbguth: La technologie de la blockchain a conduit à l'émergence de nouveaux domaines d'activité pour lesquels les réglementations en vigueur ne sont souvent pas adaptées. Outre la réglementation des marchés financiers, beaucoup d'autres domaines sont concernés, et cela constitue un vaste champ d'activité pour les juristes. L'immutabilité des informations contenues dans la blockchain ouvre d'autres possibilités. Si des modifications imprévues se produisent après l'enregistrement d'un contrat ou d'une transaction dans une blockchain, l'entrée dans la blockchain ne réglera pas toujours la nouvelle situation de manière adéquate. En effet, les juristes s'occupent aussi de ce genre de conflits en-dehors des blockchains et essaient de comprendre comment une telle situation aurait été gérée si on y avait pensé. De telles situations se présenteront beaucoup plus souvent dans le domaine de la technologie de la blockchain. Les notaires et les avocats sont donc toujours sollicités lorsqu'une occurrence à

laquelle on n'avait pas pensé survient dans le cadre de services automatisés – c'est-à-dire lorsque le formalisme d'une blockchain n'aboutit pas au bon résultat.

On dit que des registres, comme par exemple le registre foncier, pourraient à l'avenir être tenus sur la blockchain? Comment cela fonctionnerait-il?

Erbguth: Il existe grosso modo deux approches concernant l'utilisation de la blockchain pour les registres publics. Selon la première, le bureau du registre pourrait être remplacé par une blockchain. Les autorisations et les transactions seraient contrôlées de façon automatisée et directement exécutées sur la blockchain au moyen d'un logiciel intitulé «Smart Contract». Cependant, dans le cas des registres fonciers, la question est si complexe qu'une mise en pratique est loin d'être réglée.

Selon l'autre approche, qui est un peu plus superficielle, la technologie de la blockchain serait utilisée comme une technologie complémentaire renforçant la confiance. Dans ce cas, par exemple, un registre foncier continue à être tenu de manière centralisée, mais les transactions, les extraits – ou uniquement leur code de hachage – sont déposés sur une blockchain, en guise, en quelque sorte, de protection, contre les modifications non autorisées. C'est le cas par exemple au registre du commerce à Genève ou au registre foncier en Géorgie. Les régions où la corruption est importante espèrent être en mesure d'endiguer celle-ci grâce à cette possibilité de contrôle au travers d'une blockchain. Cela fonctionne dans la mesure où les modifications non autorisées ne peuvent pas être effectuées sans laisser une trace effective. Bien entendu, cela ne protège pas contre l'exécution par des ayants-droit de transactions non autorisées à proprement parler. La blockchain améliore donc ici l'administration de la preuve – le reste doit continuer à être garanti par un Etat de droit efficace.

Vous traitez également des questions relatives à la protection des données en relation avec la blockchain. Les responsables de la protection des données se réjouissent-ils de la technologie de la blockchain?

Erbguth: Les responsables de la protection des données sont ambivalents en ce qui concerne la blockchain. D'une part, la technologie de la blockchain présente un potentiel important du point de vue technique pour la protection des données. Les scandales de ces dernières années relatifs aux données étaient surtout liés à des entreprises ayant utilisé des collectes centralisées importantes de données à mauvais escient, ou à des cas de piratages de ces données. La réglementation de base en matière de protection des données tente donc de réglementer de manière stricte les entreprises qui contrôlent de grands volumes de données. Cette approche n'a pas toujours rencontré le succès escompté. Les blockchains ont du potentiel dans ce domaine parce qu'elles permettent de décentraliser les collectes de données et d'éviter ainsi des banques de données à caractère personnel volumineuses. Cela réduit les dommages potentiels dans de nombreux cas. Le concept de la «self-sovereign identity» prévoit, par exemple, que les informations relatives à une personne sont stockées de manière décentralisée et qu'une blockchain est utilisée pour authentifier ces informations. Les utilisatrices et les utilisateurs ont ainsi la possibilité de décider eux-mêmes qui peut accéder à quel contenu.

L'immutabilité de la technologie de la blockchain n'est pas exactement compatible avec les principes de protection des données.

Erbguth: Pour les responsables de la protection des données il est important que les données ne soient conservées qu'aussi longtemps qu'elles sont nécessaires. Par conséquent, les demandes de rectification et d'effacement jouent un rôle important dans la protection des données – jusqu'au droit à l'oubli. Dans ce contexte, il existe un conflit d'objectifs entre la technologie de la blockchain et la protection des données. Il existe un certain nombre de solutions techniques et juridiques à ce problème.

Voyez-vous des domaines où la protection des données «va trop loin»?

Erbguth: Je n'irais pas jusqu'à dire que la protection des données «va trop loin» dans certains domaines. Toutefois, la protection des données, et en particulier le RGPD, ne sont pas suffisamment neutres sur le plan technologique. L'approche actuelle en matière de protection des données suppose que le traitement des données est contrôlé par une, voire deux ou trois entreprises. Et qu'il suffirait que ces entreprises se voient imposer des obligations et des sanctions pour garantir un bon niveau de protection des données. Avec une technologie peer-to-peer, comme celle de la blockchain par exemple, le contrôle est cependant entre les mains de nombreuses personnes. Cela réduit l'influence de l'individu et protège les données contre les manipulations et les abus. Mais qu'est-ce que cela signifie au niveau de la réglementation? Il ne semble pas approprié de rendre tous les participants responsables pour l'ensemble des traitements de données dans les systèmes peer-to-peer, précisément parce qu'ils ne peuvent pas les influencer dans la pratique. Cependant, une solution qui suppose que, dans certains cas, personne n'est responsable, apparaît problématique.

Comment déterminer si une idée est compatible avec l'utilisation de la blockchain?

Erbguth: Avec les blockchains, toutes les données sont stockées sur tous les nœuds, ce qui, en général, est très peu efficace. Raison pour laquelle l'utilisation de blockchains n'est profitable que lorsqu'un degré élevé de sécurité dans la manipulation et d'autonomie du système est nécessaire. Si vous pouvez tout aussi bien implémenter un projet avec une banque de données conventionnelle qu'une blockchain, vous devriez éviter d'utiliser une blockchain. Le battage médiatique autour de la blockchain est retombé, et le temps des projets qui n'utilisaient la blockchain que pour de pures raisons de marketing est révolu. Les projets sérieux traitent en outre dès le départ des questions de protection des données (privacy by design). Ils définissent également la manière dont les erreurs et les cas exceptionnels doivent être traités. Il est important de régler cette «Governance» pour que les applications blockchains fonctionnent sur la durée et ne capotent pas dès l'apparition des premiers cas exceptionnels, qui surviennent tôt ou tard. Les notaires peuvent jouer un rôle important à cet égard.

Les questions ont été posées par Me Claudia Schreiber (Advokatur Schreiber, Service d'assistance électronique SAE, Berne).