Kollidiert das Recht auf Vergessenwerden mit der Blockchain-Technologie?

Ist das Recht auf Vergessenwerden gemäss EU-DSGVO mit Blick auf die Blockchain-Technologie eine archaische Forderung? Blockchains sollen ja gerade jede Transaktion transparent festhalten und verhindern, dass Daten gelöscht oder verändert werden können. Datenschutzrechlich wirft dies einige Fragen auf. Ein Essay.

1. Unveränderbarkeit als zentrales Element der Blockchain

Eine Blockchain ist eine kontinuierlich erweiterbare Liste von Transaktionen, die mittels kryptografischer Verfahren miteinander verkettet sind. Transaktionen können jede Art von Information sein, etwa Bestellungen oder Überweisungen. Jeder Block enthält dabei einen kryptografisch sicheren sogenannten Hash des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten. Aus vielen dieser Blocks besteht letztlich eine Blockchain. Die digitalen Transaktionen sind stets aktuell und lassen sich für die Teilnehmer nachvollziehbar dokumentieren, indem sie stets chronologisch und linear erweitert werden. Deswegen wird die Blockchain oft mit einem Buchhaltungssystem verglichen. Bei diesem Konzept, das auch als Distributed-Ledger-Technologie bezeichnet wird, ist entscheidend, dass spätere Transaktionen auf früheren Transaktionen aufbauen und deren Richtigkeit bestätigen, indem sie die Kenntnis der früheren Transaktionen beweisen. Eine Blockchain ist damit im Grunde eine Datenbank, jedoch in einem dezentralen Netzwerk aus vielen einzelnen Blockchains organisiert, die dieselbe Datenkette mit denselben komplexen Informationen enthält. Die Datenketten befinden sich auf unzähligen privaten und öffentlichen Rechnern. Sobald eine Blockchain ohne eine entsprechende Berechtigung verändert wird, ist diese nicht mehr im Einklang mit der Liste aller Transaktionen. Andere Teilnehmer der dezentralen Buchführung, die Kenntnis der späteren Transaktionen haben, erkennen eine manipulierte Kopie der Blockchain daran, dass plötzlich Inkonsistenzen in den Berechnungen bestehen. Damit wird es unmöglich gemacht, Existenz oder Inhalt der früheren Transaktionen zu manipulieren oder zu löschen, ohne gleichzeitig alle späteren Transaktionen zu zerstören. Würde eine Datenkette verändert, bestünden nach wie vor eine Vielzahl von Kopien mit dem ursprünglichen, richtigen Inhalt.

Um Daten in einem abgeschlossenen Block auf einer öffentlichen Blockchain tatsächlich nachträglich löschen oder verändern zu können, müsste die Mehrheit einer Chain, sprich über die Hälfte der Miner, zustimmen. Die Miner müssten also einen neuen, veränderten Block kreieren und künftig mit diesem arbeiten. Verfügt also eine Institution über 51 Prozent bei der Consensus-Bildung, könnte diese Macht dazu genutzt werden, eine Kette zu verändern. Transaktionen könnten nicht nur beliebig hinzugefügt und abgelehnt werden, sondern auch Teile der bestehenden Blockchain könnten entfernt und durch neue Abschnitte ersetzt werden. Das ist theoretisch möglich, in der Praxis aber zumindest zum aktuellen Zeitpunkt kaum denkbar. Die Unveränderbarkeit des Transaktionsregisters gilt als zentrales Element der Blockchain-Technologie und macht sie damit sicher. Gerade diese Eigenschaft wirft jedoch mit Blick auf die DSGVO, die hinsichtlich der Datenspeicherung auf technisch klassischen Paradigmen beruht, die Frage auf, ob eine öffentliche Blockchain überhaupt mit dem «Recht auf Vergessenwerden» vereinbar ist.

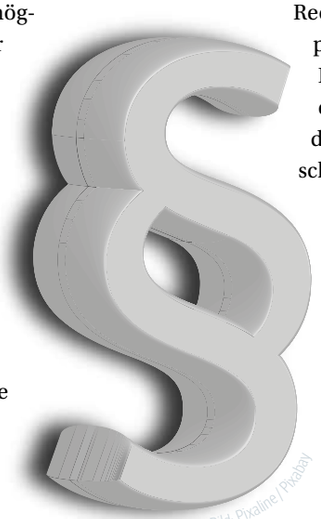

Bild: Pixaline / Pixabay

2. Recht auf Vergessenwerden gemäss Art. 17 DSGVO

a) Überblick

In Art. 17 DSGVO ist das sogenannte Recht auf Löschung («Recht auf Vergessenwerden») geregelt. Dieses hält in Abs. 1 fest, dass eine betroffene Person das Recht hat, vom Verantwortlichen zu verlangen, dass personenbezogene Daten, die sie betreffen, unverzüglich gelöscht werden. Hierbei werden in lit. a bis lit. f sechs Löschungsgründe genannt: der Wegfall der Notwendigkeit zur Zweckerfüllung, der Widerruf der Einwilligung, der Widerspruch gegen die Verarbeitung, die Unrechtmässigkeit der Verarbeitung, die anderweitige Rechtspflicht zur Löschung und die Erhebung personenbezogener Daten eines Kindes in Bezug auf angebotene Internetdienste. Ist einer dieser Löschgrunde gegeben, dann hat die betroffene Person grundsätzlich einen Löschungsanspruch. Unabhängig davon wird auch die Löschungspflicht erwähnt. Abs. 3 regelt fünf Ausnahmen vom Löschungsanspruch beziehungsweise von der Löschungspflicht, etwa die Ausübung des Rechts auf freie Meinungsäusserung und Information.

Lesen Sie weiter auf Seite 40

DIE AUTORIN

Dr. iur. Anne-Sophie Morand ist Legal Associate bei der Advokatur Fanger in Luzern – Anwaltsboutique für ICT-, Daten-, Medien- und Arbeitsrecht

www.advokatur-fanger.ch

Im Entwurf des schweizerischen DSG ist das Recht auf Vergessenwerden nicht explizit in einem eigenen Artikel geregelt.

Mit Art. 17 sollte in der DSGVO unter anderem die Problematik aufgenommen werden, dass das Internet nichts vergisst. Weit zurückreichende, im Internet vorzufindende Informationen über einen Menschen – mögen sie noch so der Wahrheit entsprechen – können die Persönlichkeitsentwicklung und die Privatsphäre beeinflussen. Datenverarbeitungssysteme müssen sich dies bei der Verarbeitung von personenbezogenen Daten bewusst sein und die normativen Anforderungen entsprechend technisch implementieren. Klassische Netzwerke setzen bekanntlich auf eine zentrale Datenbank beziehungsweise einen Server, auf den mehrere Nutzer, entsprechend ihren Berechtigungen, zugreifen. Hier kann aus technischer Sicht einfacher etwas gelöscht werden. Nichtsdestotrotz ist auch eine Löschung von Daten ausserhalb einer Blockchain nicht immer ganz einfach. Gerade die intensive Nutzung des Internets sowie das Kopieren und Verknüpfen von Daten führen dazu, dass das Umsetzen des Rechts auf Vergessenwerden in zentralen Systemen ebenfalls Schwierigkeiten unterworfen ist.

Im Entwurf des schweizerischen DSG ist das Recht auf Vergessenwerden nicht explizit in einem eigenen Artikel geregelt, sondern nach der Datenverarbeitung durch Private sowie Bundesbehörden unterteilt und in den entsprechenden Bestimmungen indirekt erwähnt. Nichtdestotrotz kann trotz der unterschiedlichen Regelungssystematik im Vergleich zur DSGVO – diese regelt die Voraussetzungen und Einschränkungsmöglichkeiten präzise – von einem ähnlichen Schutzniveau ausgegangen werden.

b) Inhalt der Löschungspflicht

In der DSGVO ist keine explizite Definition des Begriffs «Löschen» zu finden. Der Begriff wird jedoch dahingehend verstanden, dass das Löschen selbst auf unterschiedliche Art und Weise erfolgen kann, jedoch das Ergebnis der Löschungshandlung massgeblich ist, das heisst die Unmöglichkeit, die zuvor in den zu löschenden Daten verkörperte Information wahrzunehmen. Nach einem Löschvorgang sollte es niemandem mehr ohne unverhältnismässigen Aufwand möglich sein, die entsprechenden Informationen wahrzunehmen.

Werden Daten auf einem wiederbeschreibbaren Datenträger gelöscht, dann tritt der Erfolg der Löschungshandlung nicht schon dann ein, wenn die betreffenden Speicherplätze in der Indextabelle zum neuen Beschreiben freigegeben sind, sondern erst beim tatsächlichen Überschreiben mit neuen Daten. Aus diesem Grund reichen die in den Betriebssystemen zur Verfügung stehenden einfachen Löschbefehle in der Regel nicht, sodass in solchen Fällen der Einsatz spezieller Löschsoftware beziehungsweise der Einsatz von Programmen, welche die mit ihnen verarbeiteten Daten auch sicher löschen können, unumgänglich ist. Als keine ausreichende Löschungshandlungen gelten rein organisatorische Massnahmen, welche die Wahrnehmung der Information verhindern sollen. Auch explizite Hinweise, die bekannt geben beziehungsweise kennzeichnen, dass bestimmte Daten nicht mehr Geltung haben, ist nicht mit einem Löschen im Sinne der DSGVO gleichzusetzen. Ebenso wenig stellt das simple Entsorgen des Datenträgers ein Löschen dar, denn eine Kenntnisnahme der Informationen durch andere Personen ist theoretisch immer noch möglich. Die Löschungspflicht umfasst auch mögliche Kopien der Daten, die durch Dritte angefertigt wurden, denen die Daten offengelegt worden sind. Dritte unterliegen unter Umständen direkt eigenständigen Löschungspflichten. Das Verwenden der Begriffe «Kopie» und «Replikationen» in Art. 17 Abs. 2 DSGVO verdeutlicht zudem, dass nicht nur exakte Kopien der betreffenden Daten zu löschen sind, sondern auch Abbilder, die zwar nicht exakt mit dem Original übereinstimmen, aus denen aber die in den betreffenden Daten enthaltene Information entnommen werden kann.

Bezüglich der zeitlichen Dimension der Löschungspflicht ist in Art. 17 DSGVO vom «unverzüglichen» Löschen die Rede. Die betroffene Person hat hiermit einerseits das Recht, die unverzügliche Löschung zu verlangen und andererseits ist der Verantwortliche genauso verpflichtet, die Datenlöschung unverzüglich vorzunehmen. Wenn die betroffene Person einen Löschungsantrag stellt, werden die Anforderungen an den zeitlichen Ablauf durch Art. 12 Abs. 3 DSGVO konkretisiert, das heisst der Verantwortliche hat spätestens innerhalb eines Monats nach Eingang des Antrags die betroffene Person über die ergriffenen

Massnahmen beziehungsweise über die Gründe für deren Ablehnung zu informieren.

c) Urteil des EuGH vom 13. Mai 2014 («Google Spain») sowie vom 24. September 2019

In einem Urteil des Europäischen Gerichtshofs aus dem Jahr 2014 wurde Google in die Pflicht genommen, Suchergebnisse zu löschen, weil diese die Persönlichkeit der klagenden Person verletzten. Der Kläger hatte 2010 bei der spanischen Datenschutzbehörde gegen die Herausgeberin einer Tageszeitung sowie gegen Google Spain und Google Inc. eine Beschwerde eingereicht, mit der er verlangte, dass Google die ihn betreffenden personenbezogenen Daten zu löschen habe, sodass diese künftig weder in den Suchergebnissen noch in Links zur besagten Zeitung erscheinen. Das EuGH hatte mit dem vorliegenden Entscheid nicht nur grundsätzlich entschieden, dass Google den Vorschriften der EU-Datenschutzrichtlinie untersteht, sondern auch festgelegt, dass Suchmaschinenbetreiber zur Löschung von Suchergebnissen verpflichtet werden dürfen, die bei der Suche mit dem Namen einer Person angezeigt werden. Dies gilt selbst dann, wenn die Veröffentlichung des Namens auf den Websites als solche rechtmässig ist.

Der EuGH hatte es 2019 sodann bei einem Fall aus Frankreich erneut mit der Löschungsthematik hinsichtlich Google-Suchergebnissen zu tun. Dadurch befasste sich das Gericht mit der zwischenzeitlich in Kraft getretenen DSGVO und damit mit der Reichweite des Rechts auf Vergessenwerden in Art. 17 DSGVO. Es kam zum Schluss, dass Google nicht verpflichtet sei, eine weltweite Löschung personenbezogener Suchergebnisse vorzunehmen, das heisst in sämtlichen Versionen der Suchmaschine. Nach EU-Recht müssen die Informationen jedoch aus den Ergebnislisten in allen EU-mitgliedstaatlichen Versionen der Suchmaschine entfernt werden, denn das Ziel der DSGVO besteht letztlich darin, ein hohes Schutzniveau für personenbezogene Daten in der gesamten Europäischen Union sicherzustellen. Sodann hat das EuGH weiter festgehalten, dass die DSGVO den EU-Mitgliedstaaten nicht verbietet, den Suchmaschinenbetreibern trotzdem «weltweite» Löschungspflichten aufzuerlegen. Suchmaschinenbetreiber könnten zur Ergreifung von Massnahmen verpflichtet sein, welche die Internetnutzer zumindest zuverlässig davon abhalten, von einem Mitgliedstaat aus auf die im Anschluss an eine Suche angezeigten Ergebnislinks in Nicht-EU-Versionen der Suchmaschine zuzugreifen.

Sind somit zusammengefasst die Voraussetzungen von Art. 17 DSGVO erfüllt, ist eine Suchmaschine wie Google verpflichtet, dass die beanstandeten Suchergebnisse bei der Suche mit dem Namen zumindest in den nationalen Versionen der EU-Länder nicht mehr erscheinen. Im Einzelfall, wenn ein besonders starker Eingriff in die Grundrechte des Betroffenen gegeben ist, kann dem EuGH zufolge das Recht auf Vergessenwerden aber auch weltweit Geltung haben. Dies, weil eine Aufsichts- oder Justizbehörde eines Mitgliedstaates befugt bleibe, ausgehend von den nationalen Schutzstandards für Grundrechte gegebenenfalls dem Suchmaschinenbetreiber die Löschung der Suchergebnisse in allen Versionen seiner Suchmaschine aufzugeben. Für die Thematik der Blockchain ändert sich mit Blick auf den letzten Punkt nicht viel, da eine öffentliche Blockchain grundsätzlich weltweit und überall «in Erscheinung treten kann», und sobald ein involvierter, sich einer Blockchain anschliessender Dienst im EU-Raum ansässig ist oder sobald ein EU-Bürger mit seinen Daten involviert ist, ist die DSGVO mit Blick auf den räumlichen Anwendungsbereich relevant.

> Es stellt sich die Frage, wie den Betroffenenrechten entsprochen werden kann, wenn eine Löschung in einer Blockchain grundsätzlich nicht möglich ist.

d) Zwischenfazit mit Blick auf die Blockchain-Technologie

Die DSGVO hält unmissverständlich das «Recht auf Vergessenwerden» fest. Mit Blick auf die Veränderungsresistenz der Blockchain-Technologie als solche wirft der

Lesen Sie weiter auf Seite 42

Bild: Evgenia / Adobestock

Bild: Siarhei / Adobestock

Person zuordnen zu können. Sind die Hashwerte beispielsweise für den Verantwortlichen der Blockchain bekannt, beziehungsweise handelt es sich um eine zulassungsbeschränkten Blockchain, ist derjenige, der die Nutzerkennung vergibt, in der Lage, auf die Person rückzuschliessen, die sich hinter einem öffentlichen Schlüssel verbirgt. Seine Stellung kann mit einem Internet-Service-Provider verglichen werden. Dieser kann jederzeit den Nutzer einer IP-Adresse, dem er diese zugeteilt hat, zweifelsfrei identifizieren. Sodann sind auch Personen in einer öffentlich einsehbaren Blockchain in der Lage, mit verhältnismässigen Mitteln einen Personen-

In der Praxis werden verschiedene technische Ansätze diskutiert, um eine Revision von Daten in der Blockchain zu ermöglichen.

Löschungsanspruch beziehungsweise die Löschungspflicht in Art. 17 DSGVO automatisch die Frage auf, ob wir es vorliegend mit einem unlösbaren Widerspruch zu tun haben.

Eine Berichtigung der Daten kann grundsätzlich nur durch eine neue Transaktion realisiert werden, die eine neue Version der Daten bietet. Damit können Daten theoretisch nur aktualisiert, aber nicht überschrieben werden und die ursprüngliche Version bleibt in der Blockchain. Um Transaktionsdaten zu ersetzen und damit zu löschen, müssten bereits in der Blockchain verankerte Transaktionsdaten im Nachhinein verändert werden, was durch die Verkettung der Blöcke unmöglich sein sollte. Eine rechtliche Lösung scheint keine gegeben zu sein, ausser der Gesetzgeber würde Art. 17 DSGVO aushöhlen beziehungsweise künftig weniger restriktiv auslegen. Auf den zweiten Blick könnte dem vorliegenden Dilemma wohl aber die Stirn geboten werden, indem durch technische Ausführungen bestimmte Voraussetzungen geschaffen werden, welche die vorliegende Problematik umgehen.

3. Personenbezogene Daten in einer Blockchain

Damit Art. 17 DSGVO überhaupt zur Anwendung gelangt, muss es sich bei den verarbeiteten Informationen um personenbezogene Daten im Sinne von Art. 4 DSGVO handeln. Eine Blockchain speichert nach aktuellem Stand nicht unmittelbar elektronische Personendaten. Sie hinterlegt jedoch sogenannte Hashes der entsprechenden Daten und verwendet öffentliche Schlüssel als Nutzerkennungen. Obwohl die Hashwerte nur aus kryptischen Zahlen- und Buchstabenkombinationen bestehen, lassen sich diese konkreten Datensätzen zuordnen, womit die Hashwerte zu pseudonymen Daten werden. Eine Information ist letztlich für denjenigen personenbezogen, der über das notwendige Zusatzwissen verfügt, um sie mithilfe von verhältnismässigen Mitteln einer bestimmten bezug herzustellen. Nutzt beispielsweise ein Teilnehmer Dienste wie Bitcoin-Marktplätze, geht mit seiner Anmeldung hervor, dass er hinter bestimmten öffentlichen Schlüsseln steckt. Zudem ermöglichen heutzutage auch Big-Data-Analysen Teilnehmer einer Blockchain zu identifizieren. So ist es etwa möglich, die (personenbezogene) IP-Adresse des Rechners zu ermitteln, die ein Teilnehmer nutzt. Somit ist es in einer öffentlichen Blockchain möglich, mit den abgelegten Hashes und öffentlichen Schlüsseln mit verhältnismässigen Mitteln eine natürliche Person zu identifizieren, die hinter diesen Daten steht. Bei den mit dem Betrieb eines Blockchain-Netzwerks verbundenen Daten handelt es sich zusammengefasst somit um personenbezogene Daten, weshalb die Bestimmungen der DSGVO für die Verarbeitung dieser personenbezogenen Daten zur Anwendung gelangen.

Weniger eindeutig als der Personenbezug ist im Übrigen die datenschutzrechtliche Verantwortlichkeit im Blockchain-System. Diese Voraussetzung ist bei einer Blockchain mit ihrem dezentralen System verständlicherweise problematisch, da sich die Blockchain durch die Verteilung und Dezentralisierung der Speicherung und Verarbeitung von Daten auszeichnet. Dementsprechend kommen verschiedenste Akteure als Verantwortliche infrage. Die tatsächliche Verantwortlichkeit hängt dabei vom konkreten System ab und muss im Einzelfall analysiert werden.

4. Ein Dilemma! Eine Lösung?

Es stellt sich nun die Frage, wie den Betroffenenrechten entsprochen werden kann, wenn eine Löschung in einer Blockchain grundsätzlich nicht möglich ist. Unter anderem mit dieser Frage hatte sich Ende 2018 bereits die französische Behörde für Datenschutzaufsicht befasst und dazu einen Leitfaden herausgegeben. Darin wird festgehalten, dass es im Rahmen der Blockchain-Technologie technisch

unmöglich sei, dem Recht des Betroffenen auf Löschung seiner Daten im erforderlichen Mass gerecht zu werden. Möglich sei es zwar, sich diesem Recht zu nähern, indem etwa private Schlüssel gelöscht würden und im Falle eines Berichtigungsverlangens falsche Informationen auf dieselbe Weise entfernt würden, jedoch stelle keine der aktuell technisch möglichen Alternativen eine wirkliche Löschung von personenbezogenen Daten dar. Somit sei ganz klar fraglich, ob sich das Recht auf Vergessenwerden innerhalb einer Blockchain verwirklichen kann. Vielmehr kommt die Behörde letztlich zum Schluss, dass es einem Verantwortlichen technisch nicht möglich sei, einem Löschgesuch im Sinne von Art. 17 DSGVO in vollem Umfang zu entsprechen.

Etwas differenzierter sieht es der deutsche Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) in seinem Faktenblatt zum vorliegenden Thema. Er folgt zwar dem Fazit im technischen Sinne, ist aber der Ansicht, dass das Recht auf Löschung gar nicht unbeschränkt gelte, da es mit Rechten Dritter kollidiere – insbesondere der Meinungs- und Informationsfreiheit sowie dem Recht auf unternehmerische Freiheit gemäss der Charta der Grundrechte der Europäischen Union. Weiter wird ausgeführt, dass eine Interessenabwägung stattfinden müsse, wenn eine geforderte Löschung die Existenz einer gesamten Blockchain gefährde. Dabei müsse in der Interessenabwägung gefragt und berücksichtigt werden, ob sich ein Betroffener der Unveränderbarkeit der Blockchain vor der Nutzung bewusst war und ob er wusste beziehungsweise wissen musste, dass seine personenbezogenen Daten nicht ohne Weiteres gelöscht werden könnten, wenn dadurch die Existenz der Blockchain gefährdet wäre. Hierfür sind besonders transparente und ausdrückliche Datenschutzhinweise erforderlich, damit der Betroffene auf verständliche Art und Weise Kenntnis von der Löschproblematik in der Blockchain erlangen kann. Ob ein Verzicht auf das Recht auf Vergessenwerden im Endeffekt überhaupt zulässig ist, bleibt fragwürdig.

Nach dem Gesagten ist darauf hinzuweisen, dass in der Praxis verschiedene technische Ansätze diskutiert werden, um eine Revision von Daten in der Blockchain zu ermöglichen. Die Rede ist etwa von einer sogenannten Off-Chain-Datenspeicherung, also einer externen Speicherung von Daten, die in der Blockchain nur referenziert werden. Hierbei werden keine personenbezogenen Daten direkt auf der Blockchain gespeichert, sondern mit den einzelnen Bausteinen an eine Off-Chain-Datenbank geknüpft. Der Hash ist nach einer Änderung nicht mehr gültig, der entsprechende Transaktionsblock kann aber weiterhin verifiziert werden und die gesamte Blockchain bleibt ungefährdet. Durch die im Folgenden beschriebene Konstruktion lässt sich die Korrektheit der Daten beweisen, ohne dass Dritte unerwünscht Zugang erhalten. Sodann wird die kryptografische Möglichkeit von sogenannten Chameleon-Hashes diskutiert. Dabei handelt es sich um Hashfunktionen, bei denen über eine Hintertür (sog. Trapdoor) die Konstruktion von Kollisionen, also von unterschiedlichen Daten mit demselben Hashwert ermöglicht wird. Damit können Daten auf der Blockchain ausgetauscht werden, ohne jedoch den Integritätsschutz der Blockchain abzuschaffen. Die besagte Hintertür muss dabei von einer vertrauenswürdigen Instanz verwaltet werden oder die Schlüssel müssen in einem sogenannten Secret-Sharing-Verfahren auf verschiedene Parteien aufgeteilt werden. Weitere technische Lösungswege wie Mutable Blockchains, Rollbacks oder Forks werden in der Praxis ebenso in Erwägung gezogen.

Allen Ansätzen, welche die vorliegende Problematik technisch lösen sollen, ist gemein, dass sie ein Stück weit den Grundgedanken der Blockchain-Technologie übergehen. Das kann heikel sein, denn die genannten Mechanismen bieten auch Raum für Missbrauch und es wird am Vertrauensmodell gerüttelt. Letztlich kann festgehalten werden, dass sich das Recht auf Vergessenwerden nicht ohne neue Lösungswege mit dem Charakteristikum der Blockchain-Technologie verträgt. Damit sind Datenschutzbehörden und Gesetzgeber angehalten, neue und gezielte Innovationen zu fördern, damit rechtssichere, aber auch praktische Lösungen geschaffen werden.

Den Beitrag finden Sie auch online
www.netzwoche.ch

Technische Lösungswege wie Mutable Blockchains, Rollbacks oder Forks werden in der Praxis ebenso in Erwägung gezogen.

Bild: geralt / Pixabay