Stephan Noller, Christian Pfeiffer

Blockchain aus Sicht eines Datenschutzbeauftragten

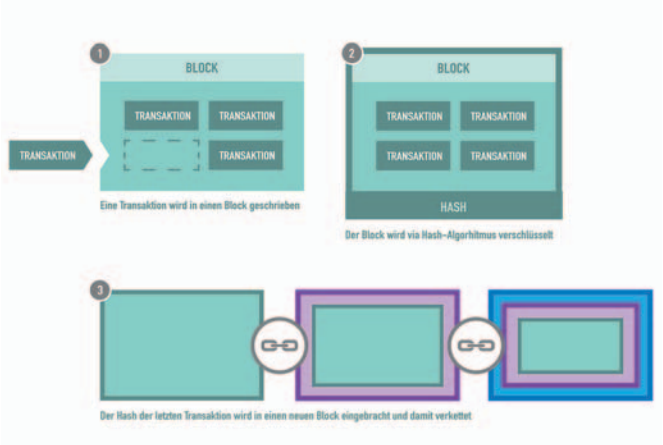
Die Blockchain ist ein kryptographisches Protokoll, das sich derzeit großer Beliebtheit bei neuen Internet-Geschäftsmodellen erfreut. Sie ermöglicht ein permanentes Speichern von Daten, Werten und Transaktionen im Netz und implementiert dabei überraschend viele Aspekte von Privacy by Design. Banken, Versicherungen, Startups und auch Regierungen prüfen derzeit die Anwendung der Blockchain für unterschiedlichste Anwendungsfälle – häufig auch in sehr kritischen Bereichen mit sensitiven Daten oder Risiken für die Pseudonymisierung der Daten. Für den Datenschutz ergeben sich durch diese Technologie interessante Möglichkeiten, aber auch große neue Herausforderungen.

Eine neue Internet-Technologie – meist keine gute Nachricht für den Datenschutz ...

Üblicherweise führen technische Neuerungen aus der Sicht des Datenschutzes selten zu Verbesserungen der Lage: Datenbanken werden stärker vernetzt und im Internet zugänglich gemacht, es entstehen immer neue Datenquellen (häufig mit klarem Personenbezug).

Algorithmen werden immer besser darin, selbst kleinste Auffälligkeiten in Datenmustern zu erkennen und eindeutig einer Person zuzuordnen. Umso bemerkenswerter ist es, dass zur Zeit in der IT-Industrie weltweit ein Phänomen heiß diskutiert und vielfach als ein Mega-Trend angesehen wird, das unter Umständen zur Verbesserung des Datenschutzes beitragen könnte – qua Design und trotz Vernetzung. Die Rede ist von der Blockchain, einer im Internet verteilten und mit kryptographischen Mitteln abgesicherten Datenbank.

Abb. 1: Grundlegende Funktionsweise der Blockchain



Bisher ist die Blockchain vor allem durch die virtuelle Währung Bitcoin bekannt. Tatsächlich fungiert sie als technisches Backend, um Transaktionen mit Bitcoins als Zahlungsmittel abzuwickeln – häufig übrigens unter Wahrung vollständiger Anonymität der agierenden Personen. Die Blockchain ersetzt in diesem Fall durch ein völlig neuartiges Verfahren die bei Zahlvorgängen sonst immer benötigte Instanz des Vertrauens (also beispielsweise eine Bank), die sicherstellt, dass ein Wert tatsächlich von A nach B übertragen wird und A nicht weiter behaupten kann, den Wert zu besitzen. In der Blockchain wird diese „Trust-Quelle" durch ein technisches Protokoll ersetzt, das sicherstellt, dass jedermann die Transaktion „sehen" kann und darüber auch in einer Art Abstimmungsprozess unter allen Beteiligten Zeugnis ablegt. Jeder Teil der Blockchain speichert alle jemals mit dieser durchgeführten Transaktionen vollständig und kryptographisch abgesichert ab. So finden sich Einträge teilweise auf tausenden von Rechnern über die ganze Welt verstreut wieder – und keine zentrale Instanz kontrolliert diese Rechner oder das Protokoll. Daraus ergeben sich aus der Sicht des Datenschutzes spannende Probleme, aber auch Features.

Kryptographische Verkettung mit Hashes

Die kryptographische Absicherung erfolgt so, dass über jeden Eintrag in die Blockchain ein sogenannter „Hash" berechnet wird – eine Zeichenkette, die den jeweiligen Inhalt eindeutig repräsentiert, ohne dass dieser jedoch aus ihr zurückberechnet werden könnte. Jede kleinste Veränderung am Inhalt führt sofort zu deutlichen Änderungen in der Hash-Berechnung. Zusätzlich wird bei dieser Hash-Bildung jede neue Transaktion mit der vorherigen verknüpft, d.h. der Hash wird eigentlich über den Verbund zweier Transaktionen gebildet. Auf diese Weise sind alle Transaktionen in einer so gebauten Blockchain miteinander verbunden. Somit führen selbst kleinste Änderungen irgendwo in der Historie der Blockchain dazu, dass alle Folge-Hashes ungültig werden.

Da diese Berechnungen zudem verteilt über tausende Rechner auf der ganzen Welt und mit sehr hohem Rechenaufwand erfolgen, gilt es derzeit als praktisch unmöglich, Einträge in der Blockchain nachträglich zu ändern. Das hat erhebliche Folgen für Anwendungs-Szenarien auf einer Blockchain – aber natürlich genauso für viele zentrale Fragen des Datenschutzes.

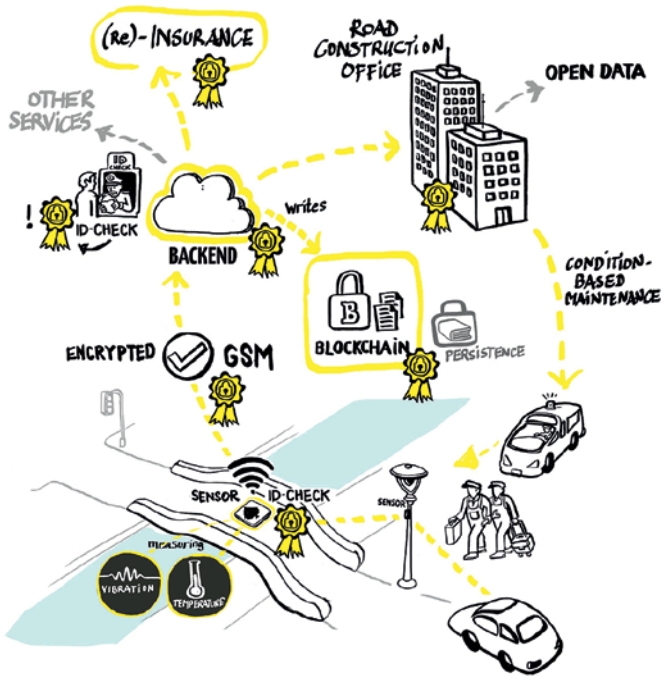
Anwendungs-Szenarien in der Blockchain

Was die Anwendungs-Szenarien anbelangt, starten derzeit an sehr vielen Stellen Pilotprojekte, um auszuloten, welche Geschäftsmodelle sich schon heute auf der Blockchain realisieren lassen. Denkbar ist, dass es automatisch agierende Versicherungen geben wird, beispielsweise gegen Wetterschäden im Weinbau.

Ein speziell abgesicherter Sensor würde dann Temperatur-Daten in die Blockchain loggen, und ein in der Blockchain abgelegter Algorithmus (ein sogenannter „Smart Contract“) würde ständig überprüfen, ob bestimmte kritische Werte erreicht werden (zum Beispiel Frost). Ist dies der Fall, könnte im Extremfall eine Überweisung vollautomatisch ablaufen – der Weinbauer könnte mit dem Geld der Versicherung schon am nächsten Morgen neue Reben kaufen und den Schaden beheben. Die Versicherung benötigt weniger Personal und reduziert sowohl das Betrugsrisiko als auch die Verfahrenskosten.

Es gibt zahllose weitere Beispiele aus den unterschiedlichsten Branchen und Lebensbereichen. Auch vor hoheitlichen Vorgängen wird die neue Technik nicht Halt machen. So ist es in Estland bereits heute möglich, bestimmte Verwaltungsvorgänge (beispielsweise in Bezug auf Grundbesitz oder bei Gründung einer Firma) auf diesem Wege zu erledigen; auch der Transfer von Gesundheitsdaten in die Blockchain ist dort aktuell in Vorbereitung.

Abb. 2: Anwendungsfall: Intelligente Brücke

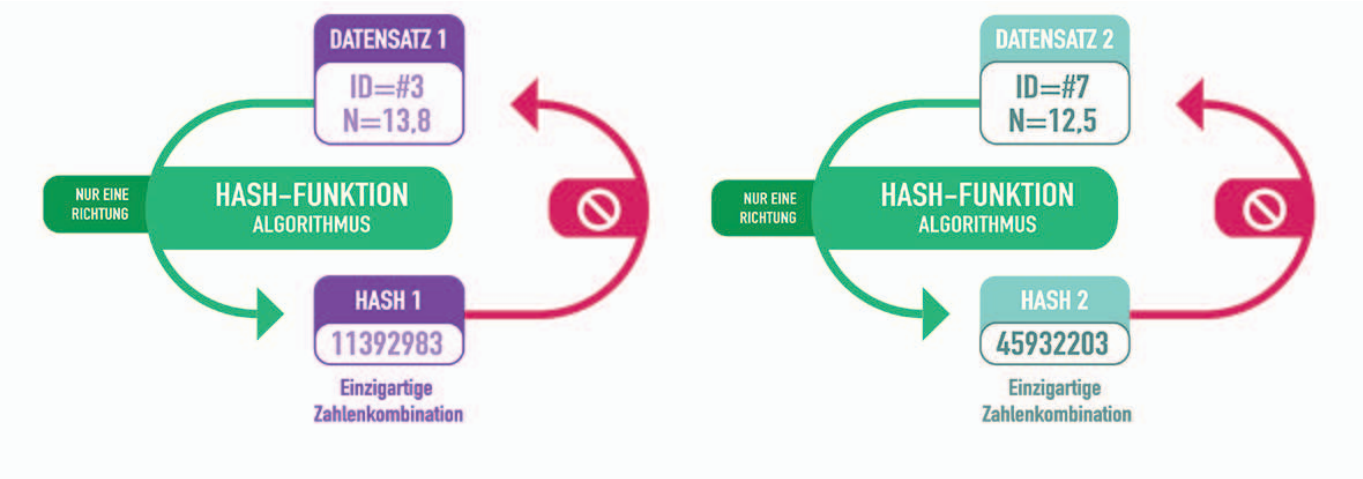


Blockchain = Privacy by Design?

Und – man glaubt es kaum – das alles ermöglicht eine Technologie, die im Kern auf Privacy by Design setzt. Dabei ist die Blockchain nicht aus einem Forschungsprojekt der EU-Kommission hervorgegangen, sondern es gibt eine überraschende Schnittmenge der Interessen von Datenschützern, Aufsichtsbehörden und den Verantwortlichen hinter der Datenschutz-Grundverordnung auf der einen Seite und Hackern, IT-Futuristen und Netzaktivisten auf der anderen Seite. Die Blockchain ist zum einen ein in sich kryptographisches Protokoll, d.h. es wird vor allem mit Schlüsseln, Hashes und kryptographischen Platzhaltern gearbeitet. Dabei wird größter Wert auf Nichtverfolgbarkeit dieser Konstrukte gelegt. Pseudonymisierung und Anonymisierung sind hier also nicht nachträglich eingezogene Schutzprinzipien, die ständig überprüft und eingefordert werden müssen, sondern es sind die Konstruktionsprinzipien des Service an sich. Natürlich gilt auch hier, dass Pseudonymisierung dennoch schwach und angreifbar umgesetzt werden kann – dies wird aber im Einzelfall bei einer auf der Blockchain basierenden Lösung üblicherweise eher an einer mangelhaften „Drumherum-Implementierung“ liegen und nicht an der Kerntechnik selbst. Wenn also beispielsweise tatsächlich Gesundheitsdaten in die Blockchain kämen, ist natürlich trotzdem die Frage, wie die Pseudonymisierung genau abläuft, und ob und wo Träger des Pseudonyms und Platzhalter zusammengeführt werden könn(t)en. Die Blockchain ist allerdings (vor allem im Fall der sogenannten Public Blockchains) ein öffentliches Protokoll und auch sehr auf Datensparsamkeit angewiesen – allein aus technischen Gründen, denn es werden alle Transaktionen miteinander verkettet und in jedem Knoten der Blockchain gespeichert. Wenn also ein Service entstünde, der Patientendaten im Klartext und mit vielen Zusatzinformationen ablegen würde, gäbe es einen Aufschrei der Techniker und Betreiber – nicht nur der Datenschützer!

Die kryptographische Architektur hat aber noch weitere Vorteile. So ist es beispielsweise ebenfalls Design-Prinzip, für einen Vorgang immer nur absolut benötigte Daten herauszugeben– der Goldstandard ist die nicht nachvollziehbare Anonymität bei einer Transaktion. So wäre es in einer Blockchain-Anwendung zum Beispiel problemlos möglich, in einem Validierungs-Szenario nur bestimmte Flags zu übermitteln (wie zum Beispiel „ist volljährig“ oder „Guthaben reicht aus“). Durch die sichere kryptographische Verkettung kann der Empfänger der Information trotzdem relativ sicher sein, dass die Information tatsächlich vom handelnden Subjekt abgeleitet wurde. Zudem sind ja alle Transaktionen generell persistiert und für alle einsehbar. Das handelnde Subjekt selbst wiederum kann ziemlich sicher sein, dass der Pseudonymisierungs-Schutz hält, denn hochspezialisierte Kryptographen haben die Algorithmen

Abb. 3: Hash-Funktion

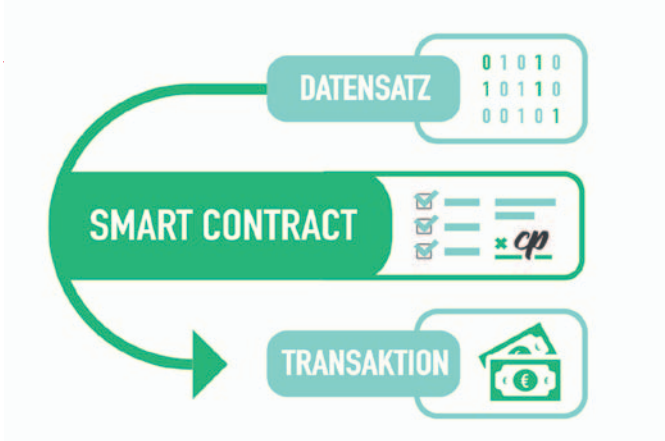


entwickelt und überwachen deren Funktion permanent, da es sich um sogenannte Open Source-Implementierungen handelt, bei denen jeder Entwickler jederzeit den Quellcode einsehen kann.

Smart Contracts – vollautomatisch laufende Prozesse mit pseudonymen Daten

Das Maximal-Szenario eines Dienstes auf der Blockchain ist der sogenannte Smart-Contract. Dabei handelt es sich um einen Teil einer Software, die selbst auf der Blockchain verteilt und validiert wurde und auch dort abläuft. Der Code selbst ist damit jederzeit nachvollziehbar und ausgesprochen schwer zu fälschen – selbst in kleinsten Details. Die verwendeten Daten stammen idealerweise ebenfalls aus der Blockchain, und etwaige Bezahlvorgänge im Rahmen des Smart-Contracts werden auch über diese abgewickelt. Das könnte beispielsweise eine Versicherung gegen Wasserschäden in einem Haus sein – oder auch eine automatisierte Erstattung in einem Freizeitpark, wenn das Emotions-Armband nicht die zugesicherten Begeisterungswerte aufzeigt.

Abb. 4: Smart Contracts



Blühende Landschaften für den Datenschutz?

Ist also alles gut und es kommen blühende Landschaften für den Datenschutz? Ganz so einfach ist es natürlich nicht. Daten in der Blockchain lassen sich praktisch nicht löschen – schon dies wirft zahlreiche regulatorische Fragen auf. Blockchain-Architekturen und Smart-Contracts werden außerdem dazu führen, dass immer mehr Daten aufgezeichnet, dauerhaft gespeichert und wirtschaftlich verwertet werden. Dabei kann auch die Blockchain nicht verhindern, dass ein immer komplexer werdendes Netzwerk an Daten trotz starker Bemühungen um Pseudo- und Anonymisierung mit immer stärker werdenden Algorithmen den Pseudonymisierungsschutz durchlöchern wird.

Schon heute können mit starken maschinenlernenden Verfahren aus Daten einfachster Vibrationssensoren Stimm-Muster konkreter Personen zugeordnet werden. Diese Entwicklung wird sich nicht einfach aufhalten lassen. Aber mit der Blockchain steht erstmals eine Technologie im Zentrum, die wesentliche Ideen des Datenschutzes in ihrer DNA mitführt. Einen besseren Ausgangspunkt, um das Datenzeitalter mit einem gesunden Level von Datenschutz zu gestalten, wird es wohl auf lange Sicht nicht mehr geben.

Internet:	www.siehe.eu/da816, www.siehe.eu/da817
Stichwort:	Blockchain, Smart Contract
Autoren:	Stephan Noller, Diplom-Psychologe und Internet-Unternehmer aus Köln. Mitglied des Beirats junge digitale Wirtschaft im BMWi. Derzeit Mit-Gründer von mehreren Start-ups, die Anwendungen des Internet der Dinge umsetzen.
	Christian Pfeiffer, Datenschutz-Beauftragter einer Berliner Firma für Targeting-Technologie, die mehrfach mit Datenschutz-Gütesiegeln ausgezeichnet wurde. **Kontakt: redaktion@gliss-kramer.de**