DATENSCHUTZ AUF ÖFFENTLICHEN BLOCKCHAINS

Jörn Erbguth

PhD Candidate – Information Systems, Centre Universitaire d'Informatique, Université de Genève
Battelle bâtiment A, 7 route de Drize, 1227 Carouge, CH
Jorn.Erbguth@unige.ch; https://erbguth.ch/

Schlagworte: ***Blockchain, Datenschutz, Smart Contracts, Recht auf Vergessen, Recht auf Berichtigung***

Abstract: *Die Blockchain-Technologie verspricht die Unveränderlichkeit und Transparenz der auf einer öffentlichen Blockchain abgelegten Informationen. Im Datenschutz gibt es jedoch ein Recht auf Berichtigung und Löschen (Art. 16, 17 DS-GVO). Der Beitrag untersucht, inwieweit Chamäleon-Hashfunktionen, Beschränkung auf Hashwerte, Verschlüsselung und Zero Knowledge Proofs einen Ausweg aus diesem Dilemma darstellen.*

1. Einleitung

Ein wesentliches Merkmal der Blockchain-Technologie, auch Distributed-Ledger-Technologie genannt, ist die Unveränderlichkeit einmal generierter Blöcke und der darin enthaltenen Transaktionen. Diese technisch abgesicherte Unveränderlichkeit schafft Vertrauen in die Authentizität und Vollständigkeit der Daten. Die DS-GVO dagegen kennt ein *Recht auf Berichtigung* (Art. 16 DS-GVO) und ein *Recht auf Löschen* (Art. 17 DS-GVO). Daher stellt sich die Frage, ob und wie Daten trotzdem auf einer Blockchain datenschutzkonform abgelegt werden können. Im Folgenden werden verschiedene technische Ansätze diskutiert und juristisch bewertet.

2. Technische Lösungsansätze

2.1. Modifizierbare öffentliche Blockchain auf Basis von Chamäleon-Hashfunktionen

2.1.1. Idee

Eine öffentliche Blockchain könnte dadurch bereinigt werden, dass nicht mehr benötigte oder unrichtige Daten entfernt werden.[1] Dazu muss zum einen sichergestellt werden, dass sich die übrigen Daten unabhängig davon sicher validieren lassen und zum anderen, dass keine noch benötigten Informationen entfernt werden.

2.1.2. Technische Realisierung

2.1.2.1. Kryptografische Hashfunktionen

Blockchains sind über Hashfunktionen[2] verkettet. Hashfunktionen berechnen aus jedem digitalen Objekt einen Hashwert – das ist eine Art digitaler Fingerabdruck. Jede kleinste Veränderung des Objekts führt zu einem deutlich unterschiedlichen Hashwert. Blockchains nutzen *kryptografische* Hashfunktionen[3], die zusätzlich kollisionsresistent sind. Dies bedeutet, dass zu einem Hashwert eines Objektes, kein zweites Objekt gefunden werden kann. Aus dem Hashwert lässt sich auch das ursprüngliche Objekt nicht berechnen – es könnte höchstens durch Ausprobieren gefunden werden.[4]

---

1 Martini/Weinzierl, 2017, 1251, 1254 f.

2 Wikipedia, Hashfunktion, https://de.wikipedia.org/wiki/Hashfunktion (alle Hyperlinks am 7. Januar 2018 abgerufen).

3 Wikipedia, kryptografische Hashfunktion, https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion.

4 Um ein Erraten zu verhindern, kann eine Nounce hinzugefügt werden, Wikipedia Salt (Kryptologie), https://de.wikipedia.org/wiki/Salt_(Kryptologie).

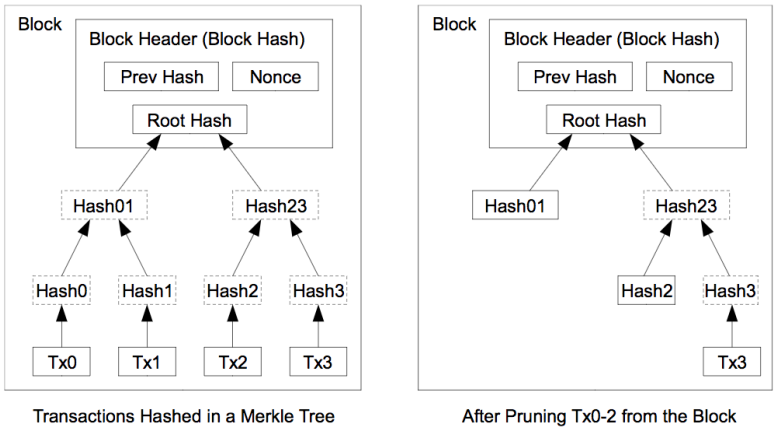

Abb. 1 Hash-Baum in einem Bitcoin-Block

2.1.2.2. Hash-Bäume innerhalb der Blöcke einer Blockchain

Nicht nur die Blöcke einer Blockchain sind durch kryptografische Hashwerte verknüpft, sondern es wird auch für jede einzelne Transaktion ein Hashwert gebildet. Für jeweils zwei Hashwerte wird wieder ein Hashwert berechnet, wodurch sich eine Baumstruktur ergibt. Solche Hash-Bäume[5] – auch als *Merkle-Tree* bezeichnet – erlauben, einen einzelnen Eintrag zu überprüfen, ohne dafür den gesamten Block lesen zu müssen. Die Bitcoin-Blöcke sind entsprechend strukturiert (Abb. 1, links). Bitcoin kennt *Lightweight Nodes*[6], die dadurch Speicherplatz sparen, indem alle bereits weiter transferierten Transaktionen entfernt werden (Abb. 1, rechts). Die Hashwerte der verbleibenden Transaktion können trotzdem noch validiert werden. Zwar ist erkennbar, wo Transaktionen fehlen, aber nicht, ob diese Transaktionen bereits weitertransferiert wurden und daher entfernt werden durften. Mit einem manipulierten Lightweight-Node wäre es deshalb möglich, eine Transaktion zu unterdrücken und die entsprechenden Bitcoins nochmals zu transferieren (Double-Spend). Daher sind stets ausreichend viele *Full-Nodes* erforderlich, um die Korrektheit des Entfernens von Transaktionen in einem Lightweight-Node überprüfen zu können. Für eine vollständige Entfernung von Transaktionen eignet sich dieses bereits von Satoshi Nakamoto[7] beschriebene Verfahren daher nicht.

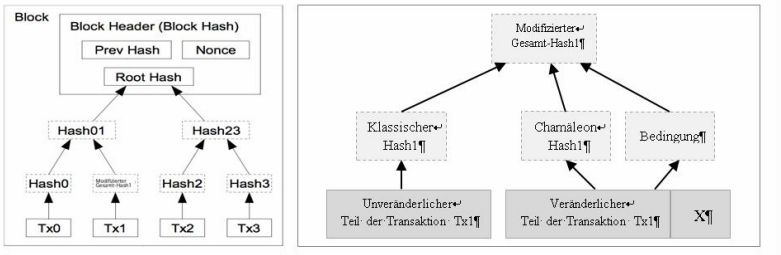

Abb. 2 Modifizierter Hash-Baum mit Chamäleon Hashes (links) sowie Tx1 im Detail (rechts)

5 Wikipedia, Hash-Bäume, https://de.wikipedia.org/wiki/Hash-Baum.
6 Bitcoin-Wiki, Full node, https://en.bitcoin.it/wiki/Full_node.
7 Nakamoto, 2008.

2.1.2.3. Chamäleon-Hashfunktionen

Um ein Löschen oder Verändern noch benötigter Einträge zu verhindern, müssten Modifikationen an Bedingungen geknüpft werden können. Hierbei können Chamäleon Hashfunktionen[8] helfen. Chamäleon Hashfunktionen sind kryptografische Hashfunktionen, die zusätzlich ein Schlüsselpaar besitzen. Dieses Schlüsselpaar – bestehend aus einem privaten und einem öffentlichen Schlüssel – hat folgende Eigenschaften:

- Mit dem öffentlichen Schlüssel kann die Hashfunktion vom Objekt zum Hashwert berechnet werden.
- Mit dem privaten Schlüssel lässt sich für einen Hashwert ein Objekt so konstruieren oder ergänzen, dass dieses zu einem Hashwert passt. Soll das Objekt beliebig gewählt werden können, so kann dazu ein Ausgleichswert – im folgenden *X* genannt – hinzugefügt werden.

Damit kann in einem Hash-Baum an den Stellen, an denen eine spätere Veränderung durch Berechtigte erwünscht ist, statt eines gewöhnlichen kryptografischen Hashwerts ein Chamäleon-Hashwert verwendet werden.

Dieses Schema kann dann um Bedingungen erweitert werden – wie etwa dem Abwarten einer bestimmten Frist oder dem Vornehmen einer Folgetransaktion.In Abb. 2 ist ein Hash-Baum dargestellt, bei dem für die Transaktion Tx1 der klassische kryptografische Hashwert mit einem Chamäleon-Hashwert erweitert wurde. Beim Erstellen der Transaktion Tx1 wird zunächst der unveränderliche und der veränderliche Transaktionsteil aufgenommen sowie X auf 0 gesetzt. Eine Änderungsbedingung wird hinzugefügt und die Hashwerte berechnet. Wenn Tx1 geändert wurde, kann nur mit dem privaten Schlüssel des Chamäleon-Hash1 ein Wert für X berechnet werden, der dazu führt, dass der Eintrag insgesamt weiterhin zum ursprünglichen Chamäleon-Hashwert passt. Wenn bei späterer Prüfung alle Hashwerte gültig sind und X=0 ist, ist damit nachgewiesen, dass sich der Eintrag im Ursprungszustand befindet. Daher wird bei der Prüfung die Änderungsbedingung ignoriert. Stimmen die Hashwerte, ist aber $X \neq 0$, wurde der veränderliche Wert durch einen Berechtigten verändert. Dies bedeutet, dass die Änderung auch der neben dem Hashwert abgelegten Bedingung genügen muss.

2.1.3. Anwendungsbereiche

Mit Chamäleon-Hashfunktionen können in eine Blockchain Einträge aufgenommen werden, die unter bestimmten Bedingungen geändert werden können. Vor dem Ändern oder Löschen sind diese jedoch öffentlich. Daher eignet sich diese Technologie nur für Daten, die zunächst öffentlich sein dürfen oder müssen, später aber gelöscht werden müssen. Art. 17 Abs. 2 DS-GVO regelt solche Fälle. Denkbar ist z.B. die Veröffentlichung von Privatinsolvenzen auf einer derartigen Blockchain. Gut geeignet ist dies auch für Smart Contracts, da diese nicht auf verschlüsselte Information zugreifen können, ohne diese damit öffentlich zu machen. Die Blockchain stellt dabei stets sicher, dass die Modifikation oder das Löschen der Bedingung entspricht und der richtige private Schlüssel vorlag. Im Bereich der nicht-öffentlichen «permissioned» Blockchains bewirbt Accenture ein ähnliches Konzept.[9]

2.2. Verschlüsselung der auf einer öffentlichen Blockchain abgelegten Daten

Werden Daten auf öffentlichen Blockchains verschlüsselt abgelegt, so kann der Zugriff auf diese Daten dadurch begrenzt werden, dass der Schlüssel nur ausgewählten Personen zur Verfügung steht. Die Blockchain garantiert dabei, dass die Daten unverändert bleiben, während die Verschlüsselung den Zugriff beschränkt. Soll der Zugriff auf die Daten nicht mehr möglich sein, genügt es, wenn alle Kopien des Schlüssels gelöscht

[8] Kraeczyk/Rabin, NDSS 2000.
[9] Bennett 2017.

werden. Dies ist ein gängiges Verfahren, genannt *Crypto-Shredding*, zur effektiven Löschung von Daten z.B. auf SSDs[10] oder in der Cloud[11].

Dieses Verfahren ist auch für Blockchains anwendbar. Damit ergeben sich zwei Einschränkungen:

- Nur Personen, die den Schlüssel besitzen, können auf die Daten zugreifen. Beim Löschen des Schlüssels muss sichergestellt sein, dass diese Personen den Schlüssel tatsächlich löschen.
- Kein Zugriff auf verschlüsselte Daten durch Smart Contracts: Smart Contracts werden auf allen Knoten der Blockchain ausgeführt. Die Knoten können dabei nicht nur auf alle Eingaben, Ausgaben und Zwischenwerte der Verarbeitung zugreifen, sondern dies auch jederzeit wiederholen. Hat ein Smart Contract Zugriff, wären die Daten dadurch öffentlich und nicht mehr löschbar.

Verschlüsselung auf Blockchains lässt sich daher dort gut anwenden, wo eine begrenzte Anzahl von Akteuren auf speziell gegen Veränderbarkeit gesicherte Daten zugreifen können soll. Ein mögliches Beispiel ist daher die beweissichere Dokumentation von Daten für Aufsichtsbehörden.

2.3. Beschränkung der Einträge auf der Blockchain auf kryptografische Hashwerte

Speicherplatz auf öffentlichen Blockchains ist teuer. Daher werden viele Daten außerhalb der Blockchain abgelegt und nur kryptografische Hashwerte der Daten auf die Blockchain geschrieben. Dieses Verfahren eignet sich besonders zur Validierung vertraulicher Dokumente. Ohne die externen Dokumente sind die Hashwerte bedeutungslos. Vom zu validierenden Dokument wird ein Hashwert gebildet und dieser dann mit dem Hashwert auf der Blockchain verglichen. Bereits der auf der Blockchain abgelegte Hashwert bestätigt dann, dass zum Zeitpunkt des Schreibens des Blocks das Dokument existiert hat. Diese Art von kryptografischem Zeitstempel ist dauerhaft und benötigt zur Beweiserhaltung keine ständige Erneuerung oder Aufbewahrung in einem zahlungspflichtigen kryptografischen Tresor[12]. Sollte allerdings die Sicherheit der verwendeten Blockchain eines Tages beeinträchtigt sein oder die Blockchain nicht mehr fortgeführt werden, so geht auch die Beweiskraft dieses Zeitstempels verloren. Die Berechnung des Hash-Wertes aus dem vertraulichen Dokument sollte außerhalb der Blockchain und daher auch nicht durch einen Smart Contract erfolgen, da sonst das vertrauliche Dokument bei der Validierung unveränderlich auf die Blockchain geschrieben wird.

2.4. Verwendung von Zero Knowledge Proofs (ZK-Proofs)

Zero Knowledge Proofs (ZK-Proofs)[13] ermöglichen es, Transaktionen abzulegen, bei denen später nur die rechnerische Korrektheit überprüft, aber nicht der tatsächliche Inhalt ausgelesen werden kann. Prominentestes Beispiel ist die Blockchain z-cash[14], die nicht nachverfolgbare Kryptogeld-Transaktionen ermöglicht. Auf Ethereum ist eine entsprechende Funktionalität ebenfalls seit Kurzem (rudimentär) verfügbar.[15] Um sich ZK-Proofs bildhaft vorzustellen, gibt es ein schönes Beispiel[16]: Ein Farbensehender hat einen roten und einen grünen Ball. Ein Farbenblinder kann die beiden Bälle nicht unterscheiden. Jetzt soll dem Farbenblinden bewiesen werden, dass die Bälle tatsächlich unterschiedliche Farben haben, ohne dass der Farbenblinde nachher weiß, welcher Ball welche Farbe hat. Für den Beweis gibt der Farbensehende dem Farbenblinden die beiden Bälle. Er soll sie hinter seinem Rücken verstecken und danach den Farbensehenden fragen, ob die Bälle vertauscht wurden. Wenn die Bälle die gleiche Farbe hätten, könnte der Farbensehende dies nur raten. Wenn

10 Klosowski, 2017.
11 Tanvashi/Shravani, 2015.
12 BSI, Technische Richtlinie 03125.
13 Goldwasser/Micali/Rackoff, 2018, S. 186–208.
14 Wikipedia z-cash, https://en.wikipedia.org/wiki/Zcash; What are zk-SNARKs, z-cash Reference, https://z.cash/technology/zksnarks.html.
15 Ethereum Blog, Byzantium Hard Fork Announcement, 12. Oktober 2017, https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/.
16 Huqing/Zhixin, 2013.

der Farbensehende dagegen die Frage sehr oft hintereinander richtig beantworten kann, hat er damit praktisch bewiesen, dass er die Bälle auseinanderhalten kann. Diese Art des Beweises übermittelt keine weitere Information an den Farbenblinden – er bleibt farbenblind. Gleichzeitig beweist aber der Farbensehende, dass er die Bälle auseinanderhalten kann.

2.4.1. Technische Beschreibung[17]

Im obigen Beispiel setzt der ZK-Proof eine Interaktion voraus – eine Interaktion zwischen demjenigen, der etwas beweisen möchte und demjenigen, der dies überprüft. Bei einem non-interaktiven ZK-Proof[18] wird die Interaktion durch einen beiden Seiten bekannten Zufallswert ersetzt. Darüber hinaus kann die Seite des Validierers durch eine digitale Signatur ersetzt werden.[19] Diese zudem Speicherplatz sparenden Beweise werden Zero Knowledge Succinct Non-interactive ARgument of Knowledge (ZK-SNARK) genannt. Für die digitale Signatur wird eine vorab generierte geheime Zufallszahl vorausgesetzt, die nach der Generierung und Verwendung vernichtet werden muss.[20] Die Variante *ZK-STARK*[21] soll ohne diese geheime Zufallszahl auskommen, ist aber noch nicht realisiert.

2.4.2. Einsatzbereich

Mit ZK-Proofs können keine Informationen von einer Blockchain gelöscht werden. Sie ermöglichen aber, Eigenschaften über Informationen zu beweisen, ohne jemals die Information selbst preiszugeben. Sie minimieren die offengelegten Daten viel stärker als klassische Datenverarbeitungsverfahren, die lediglich mit abgestuften Zugriffsrechten arbeiten. Denkbar ist der Einsatz etwa bei elektronischen Wahlen sowie beim Reporting von Transaktionsvolumina, bei denen die Summe öffentlich, aber die einzelnen Transaktionen geheim bleiben sollen. Gegenüber einfacher Verschlüsselung haben ZK-Proofs zudem den Vorteil, dass diese auch von Smart Contracts verwendet werden können.

2.5. Kombination der verschiedenen Techniken

Für Blockchain-basierte Anwendungen lassen sich Chamäleon-Hashfunktionen, Verschlüsselung, Hashwerte externer Dokumente und ZK-Proofs gut kombinieren. Für jedes Datum wird dabei die am besten geeignete Art der Ablage gewählt. Dies ermöglicht die Kombination von Datenminimierung mit hoher Beweiskraft. Wichtig ist allerdings, dass vorab bekannt ist, wer, in welcher Form und wie lange Zugang zu den Daten haben soll. Eine nachträgliche Änderung des Ablageverfahrens ist meistens nicht mehr möglich.

3. Datenschutzrechtliche Betrachtung

Die datenschutzrechtliche Betrachtung beschränkt sich auf die Rechte auf Berichtigung (Art. 16 DS-GVO) und Löschung (Art. 17 DS-GVO) sowie einige Vorfragen.

3.1. Personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO

Die DS-GVO findet nur Anwendung, wenn personenbezogene Daten verarbeitet werden (Art. 2 Abs. 1 DS-GVO). Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen. Erwägungsgrund 26 DS-GVO stellt bei der Identifizierbarkeit darauf ab, «ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden», dabei «sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand herangezogen werden». Bei der Frage, ob der Personenbezug tatsächlich entfernt (Anonymisierung) oder nur erschwert (Pseudonymisierung) wird, stellt die Art. 29 Datenschutzgruppe daher darauf ab, ob es mit

---

17 Hier wird nur die Grundidee beschrieben. Die genaue Beschreibung würde den Rahmen dieser Darstellung sprengen.

18 Blum/Feldman/Micali, 1988, S. 103–112.

19 Fiat/Shamir, 1986, S. 186–194, 190 ff.

20 Bowe/Gabizon/Green, 2017; siehe auch https://z.cash/technology/paramgen.html.

21 Buterin, 2017.

«Mittel(n) […], die vernünftigerweise [...] eingesetzt werden könnten» möglich ist, den Personenbezug wiederherzustellen.[22] Werden nur Teile der Daten mittels Verschlüsselung oder Hashing anonymisiert, ist nämlich das Risiko groß, dass eine Repersonalisierung möglich ist. Entgegen Finck[23] ist dadurch eine Anonymisierung von Daten auf einer Blockchain nicht generell ausgeschlossen. Vielmehr kommt es bei der konkreten Implementierung darauf an, ob nach dem oben genannten Kriterium ein Personenbezug herstellbar ist.

Da die Blockchain öffentlich ist, ist jeder potentiell Verarbeiter. Allerdings ist gemäß der relativen Theorie der Personenbezug immer in Bezug auf den jeweiligen Verarbeiter zu beurteilen.[24] Kann daher etwa nur der Betroffene selbst den Bezug zu sich herstellen, so gelten die Daten auch nur bei ihm als personenbezogen. Die DS-GVO ist jedoch auf die Selbstverarbeitung der eigenen personenbezogenen Daten nicht anwendbar.

3.1.1. Verschlüsselte Daten

Verschlüsselte personenbezogene Daten gelten nur für diejenigen als personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO, die den Schlüssel haben oder mit überschaubarem Aufwand erhalten können – etwa, weil sie einen Rechtsanspruch zur Herausgabe haben.[25] Dies kann auch der Fall sein, wenn nur der Betroffene über den Schlüssel verfügt, Dritte aber einen Herausgabeanspruch gegenüber dem Betroffenen haben. Ist der Schlüssel dagegen vernichtet, so dass er nicht mehr herausgegeben werden kann, entfällt der Personenbezug. Der Personenbezug kann aber wiederaufleben, wenn der Schlüssel wiedergefunden wurde oder wenn z.B. zukünftig ein Quantencomputer die Rekonstruktion des Schlüssels ermöglichen würde.

3.1.2. Kryptografische Hashwerte

Werden kryptografische Hashwerte auf einer öffentlichen Blockchain abgelegt, so beweist der Hashwert selbst zunächst nur, dass das digitale Objekt zum Zeitpunkt des Erstellens des Blocks existierte. Sind auf der Blockchain keine weiteren Merkmale oder Transaktionen neben dem Hashwert aufgeführt, so validiert der Hashwert damit lediglich außerhalb der Blockchain befindliche Daten. Werden diese außerhalb der Blockchain abgelegten Daten gelöscht, ist damit auch der Hashwert auf der Blockchain ohne jede Aussagekraft.

Anders sieht es aus, wenn der Hashwert als eine Art pseudonyme ID mit weiteren Daten, wie z.B. Transaktionen, verknüpft wird. Dann allerdings ergibt sich der Personenbezug nicht aus dem Hashwert selbst, sondern aus dem Netz der darüber verknüpften weiteren Informationen.

3.1.3. ZK-Proofs

Bei ZK-Proofs ist die lesbare Information begrenzt, aber weder lösch- noch korrigierbar. Sollte auf Grund eines Designfehlers doch ein Personenbezug herstellbar sein, lässt sich dieser nachträglich nicht entfernen.

3.1.4. Öffentliche Schlüssel

Viele Blockchains verwenden öffentliche Schlüssel, um Konten mit den dazugehörigen Transaktionen zu verknüpfen. Darüber lässt sich häufig ein Personenbezug herstellen.[26] Entgegen Finck ist es jedoch durchaus möglich, eine Blockchain so zu bauen, dass der Personenbezug vermieden wird. Dazu müssen z.B. immer wieder neue öffentliche Schlüssel verwendet werden und durch verschlüsselte Transaktionen muss verhindert werden, dass Transaktionen und öffentliche Schlüssel zu einem Netz verknüpft werden können.

3.2. Verantwortlicher im Sinne der DS-GVO

Verantwortlich i.S.v. Art. 4 Nr. 7 DS-GVO ist, wer alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Dies bedeutet umgekehrt, dass Verantwortlicher nicht sein kann, wer

22 Artikel 29 Datenschutzgruppe, Stellungnahme 5/2014, S. 9.
23 Finck, 2017, S. 10.
24 Hofmann/Johannes, 2017, 221, anders aber ohne Auswirkung auf das Ergebnis Artikel 29 Datenschutzgruppe (Fn. 22).
25 EuGH, 19. Oktober 2016, C-582/14; BGH, 16. Mai 2017, VI ZR 135/13.
26 Finck, 2017, S. 12 ff.

nicht effektiv entscheiden kann. Wer beispielsweise lediglich einen Server bereitstellt, den er nur an- und abschalten kann, ist nicht Verantwortlicher.[27] Analog dazu ist das System der öffentlichen Blockchain technisch so abgesichert, dass ein einzelner Knotenbetreiber oder Mineur den Inhalt der Blockchain nicht beeinflussen kann. Jede eigenmächtige Änderung würde den Knoten automatisch von der Blockchain ausschließen, was einem «Ausschalten» gleichkommt. Verantwortlicher i.S.d. DS-GVO ist daher nur, wer die Gewalt über die entsprechenden privaten Schlüssel hat und damit letztendlich entscheidet, ob damit eine Information auf eine Blockchain gestellt wird.[28] Wer eine Transaktion direkt – ohne Einschaltung von Dienstleistern wie Wallet-Services oder Exchanges – an eine Blockchain sendet, ist daher selbst Verantwortlicher.

3.3. Recht auf Berichtigung und Löschung (Art. 16 und 17 DS-GVO)

Betroffene haben nach Art. 16 DS-GVO ein Recht auf Berichtigung und nach Art. 17 DS-GVO ein Recht auf Löschung ihrer Daten. Im Erwägungsgrund 65 DS-GVO wird konkretisiert, dass dieses Recht nur gilt, wenn die Speicherung ihrer Daten gegen die DS-GVO oder anderes in einem Mitgliedsstaat geltendes Recht verstößt. Ist etwa die Speicherung von fehlerhaften Daten gesetzlich vorgeschrieben, so besteht daher kein Anspruch nach Art. 16 DS-GVO. So werden z.B. bei Buchhaltungssystemen fehlerhafte Einträge nicht gelöscht, sondern durch eine Stornobuchung ergänzt.[29] Eine Korrektur oder Löschung, die den ursprünglichen Eintrag nicht mehr erkennen ließe, ist nach § 239 Abs. 3 HGB unzulässig. Bei unverschlüsselter Ablage von personenbezogenen Daten auf einer öffentlichen Blockchain muss daher vorab sichergestellt sein, dass es eine Rechtspflicht oder ein dauerhaftes berechtigtes Interesse Dritter gibt, die Daten dauerhaft öffentlich zugänglich zu speichern. Bei der Ablage von personenbezogenen Daten mittels Chamäleon-Hashfunktion sind diese veränderbar und löschbar. Falls die Daten – während sie öffentlich zugreifbar waren – unabhängig kopiert wurden, kommt zur eigenen Löschpflicht eine Informationspflicht hinzu (Art. 17 Abs. 2 DS-GVO). Bei verschlüsselten Daten kann dem Recht auf Löschen auch durch Vernichtung der dazugehörigen Schlüssel nachgekommen werden, solange dadurch der Personenbezug sicher entfällt.[30]

4. Fazit

Eine datenschutzkonforme Ablage von Daten auf öffentlichen Blockchains ist nicht nur möglich, sondern kann auch vorbildlich datenschutzfreundlich gestaltet werden. Abhängig vom Löschkonzept und davon, wer Einsicht in die Daten haben soll, muss das richtige technische Verfahren ausgewählt werden. Die Auswahl geht dabei von einer direkten unveränderlichen öffentlichen Speicherung über Chamäleon Hashfunktionen, Verschlüsselung und Reduzierung auf Hashwerte bis zu ZK-Proofs. Dabei ist große Sorgfalt sowohl bei der Erstellung des Datenschutzkonzepts, als auch bei der Auswahl der passenden Technik sowie der Implementierung erforderlich. Repersonalisierungsmöglichkeiten können leicht übersehen werden und Korrekturen auf der Blockchain sind meistens nicht möglich. Daher ist die Ablage auf einer öffentlichen Blockchain mit einem hohen Haftungsrisiko verbunden und sollte nur dann gewählt werden, wenn die erreichbaren Vorteile dies rechtfertigen.

5. Literatur

Artikel 29 Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10. April 2014, 0829/14/DE, S. 9.

Bennett, Martha/Matzke, Pascal/Hoppermann, Jost, Don't Dismiss Accenture's Blockchain Redaction Solution — You May Need It One Day, 4. April 2017, Forrester Report, https://kloudrydermcaasicmforrester.s3.amazonaws.com/mcaas/Reprints/RES137814.pdf.

Bitcoin-Wiki, Full node, https://en.bitcoin.it/wiki/Full_node.

[27] Jotzo, 2009, 232, 233.

[28] Ausführlich Erbguth/Fasching, 2017, 560; Martini/Weinzierl, 2017, 1251, 1253, abzulehnen dagegen Finck, 2017, S. 16.

[29] Winnefeld, 1997, Rn. 410–419.

[30] Feil, 2011.

Blum, Manuel/Feldman, Paul/Micali, Silvio, Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract), Proceedings of the twentieth annual ACM symposium on Theory of computing, 1988, S. 103–112.

Bowe, Sean/Gabizon, Ariel/Green, Matthew D., A multi-party protocol for constructing the public parameters of the Pinocchio zk-SNARK, 2017, http://eprint.iacr.org/2017/602.

BSI, Technische Richtlinie 03125 Beweiswerterhaltung kryptographisch signierter Dokumente TR-ESOR, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html.

Buterin, Vitalik, STARKs, Part I: Proofs with Polynomials, Vitalik Buterin's webiste, 9. November 2017, http://vitalik.ca/general/2017/11/09/starks_part_1.html.

Erbguth, Jörn, Weblaw Webinar 16. August 2017, https://legaltech.weblaw.ch/events/brownbag_archiv/smart_contracts.

Erbguth, Jörn/Fasching, Galileo, Wer ist Verantwortlicher für eine Bitcoin-Transaktion? Anwendbarkeit der DS-GVO auf die Bitcoin-Blockchain, ZD 2017, 560.

Ethereum Blog, Byzantium Hard Fork Announcement, 12. Oktober 2017, https://blog.ethereum.org/2017/10/12/byzantium-hf-announcement/.

Hofmann, Johanna/Johannes, Paul, DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs, ZD 2017, 221.

Jotzo, Florian, Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232, 233.

Feil, Thomas, Verschlüsseln statt Löschen, 26. April 2011, ChannelPartner, https://www.channelpartner.de/a/verschluesseln-statt-loeschen,2383663.

Fiat, Amos/Shamir, Adi, How to prove yourself: Practical solutions to identification and signature problems, 1986, CRYPTO '86, S. 186–194, 190 ff., https://link.springer.com/content/pdf/10.1007%2F3-540-47721-7_12.pdf.

Finck, Michèle, Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation and Competition Research Paper No. 18–01, 2017, S. 12 ff.

Goldwasser, Shavi/Micali, Silvio/Rackoff, Charles, The Knowledge Complexity of Interactive Proof Systems, SIAM Journal on Computing 18(1), S. 186–208.

Huqing Wang/Zhixin, Sun, Research on Zero-Knowledge Proof Protocol, IJCSI, Vol. 10, Issue 1, No 1, Januar 2013, https://pdfs.semanticscholar.org/864e/d40c169ddf67a52ba08483d6cb68da58fc05.pdf.

Klosowski, Thorin, How to Securely Dispose of an SSD, lifehacker, 16. März 2017, https://lifehacker.com/how-to-securely-dispose-of-an-ssd-1793336156.

Kraeczyk, Hugo Mario/Rabin, Tal, Chameleon Signatures, NDSS 2000, http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/042.pdf, 2000.

Lewinski, Kai von, BeckOK DatenschutzR, DS-GVO Art. 22 Rn. 12–13.

Martini, Mario/Weinzierl, Quirin, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251, 1254 f.

Nakamoto, Satoshi (Pseudonym), A Peer-to-Peer Electronic Cash System, 2008, u.a. bei Bitcoin.org, https://bitcoin.org/bitcoin.pdf, 2008.

Tanvashi, Anand/Shravani, B., Cloud Computing Data Security in Cloud Computing for Banking, AJIT, Vol. 2, Issue 1, April 2015, http://www.adarshjournals.in/index.php/ajoit/article/download/91226/68403.

What are zk-SNARKs, z-cash Reference, https://z.cash/technology/zksnarks.html.

Wikipedia deutsch, Hashfunktion, Kryptologische Hashfunktion, Salt (Kryptologie), Hash-Bäume, https://de.wikipedia.org/wiki/.

Wikipedia englisch, z-cash, https://en.wikipedia.org/wiki.

Winnefeld, Robert, Bilanz-Handbuch, 5. A., Kapitel A: Handels- und steuerrechtliche sowie internationale Buchführungspflicht Rn. 410–419, 2015.

z-Cash, Paramgen Reference, Parameter Generation, https://z.cash/technology/paramgen.html.