TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

TeleTrusT-Informationstag "Blockchain"

**Tagungsband zum TeleTrusT-Informationstag "Blockchain"
am 13.07.2017 in Frankfurt am Main**

Redaktion
Martin Fuhrmann, TeleTrusT - Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer, TeleTrusT - Bundesverband IT-Sicherheit e.V.

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Impressum

Herausgeber:

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
https://www.teletrust.de

Dieser Tagungsband enthält die Referentenbeiträge der Veranstaltung TeleTrusT-Informationstag "Blockchain" in Frankfurt am Main am 13.07.2017, der von der TeleTrusT-Arbeitsgruppe "Blockchain" organisiert wurde. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung in der Arbeitsgruppe sowie für die aktive Mitgestaltung dieses Informationstages.

Projektleitung

Dr. André Kudra, esatus AG, Leiter der TeleTrusT-AG "Blockchain"

Referenten/Autoren

Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit if(is), TeleTrusT-Vorsitzender
Moderation und Begrüßung

Prof. Dr.-Ing. Volker Skwarek, Technische Informatik, Hochschule für Angewandte Wissenschaften Hamburg
Eröffnungsvortrag: "Was ist die Blockchain - Strategien und Möglichkeiten"

Dr. Hans Aschauer, Corporate Technology, CT RDA ITS SES-DE, Siemens AG
Dr. Jörn-Marc Schmidt, Senior Consultant, Division Homeland Security, secunet Security Networks AG
"Kryptografische und IT-Security-Perspektive auf Blockchain"

RA Dr. David Klein, LL.M, Taylor Wessing Partnerschaftsgesellschaft mbB
"Rechtliche Fragestellungen zu Blockchain"

Volker Jacumeit, Gruppenleiter "IT und IT-Sicherheit",
DIN Deutsches Institut für Normung e.V.
"Entwicklung der Standardisierung und Interoperabilität von Blockchain"

DI Dr. Christian Baumann, Vorstandsvorsitzender, WKO/AUSTRIAPRO
"Elektronische Zustellung – Anwendungsmöglichkeiten der Blockchain"

Dr. Martin Holland, Leiter Business Development und Strategie, PROSTEP AG
"Secure Additive Manufacturing-Konzept für 3D-Druckdaten"

Sebastian Stommel, Lead Researcher, CryptoTec AG
"Blockchain-basiertes Supply Chain Management"

Dr. André Kudra, Vorstand (CIO), esatus AG, Leiter der TeleTrusT-AG "Blockchain"
"Identity und Access"

Dr. Michael Kuperberg, Senior Software Architect, Deutsche Bahn AG
Bertalan Vecsei, External Blockchain Architect, Deutsche Bahn Energie
Sorin Simplaceanu, External Blockchain Business Consultant, Deutsche Bahn AG
Steffen Ortolf, Engagement Management, DB Systel GmbH
"Blockchain-basiertes System für geschäftliche Vereinbarungen"

Inhalt

1 Vorwort

Prof. Dr. Norbert Pohlmann, Institut für Internet-Sicherheit if(is),
TeleTrusT-Vorsitzender

Die "Blockchain" ist eine spannende und faszinierende IT-Technologie, die das Potential hat, Politik, Verwaltung und Wirtschaftszweige gewaltig auf den Kopf zu stellen. Die Blockchain-Technologie ist eine Querschnittstechnologie mit hohem disruptiven Potenzial für viele Wirtschaftsbereiche. Die Blockchain-basierten Systeme könnten in vielen Bereichen zentrale Instanzen ablösen, wie Banken, Notare oder Treuhänder. Das ist möglich, weil die Validierungsalgorithmen der Blockchain-Technologie ganz ohne solche Intermediäre die Vertrauenswürdigkeit der aufgezeichneten Transaktionsdaten garantieren. In der Zukunft werden sogenannte Smart Contracts umgesetzt, die eine vorprogrammierte, selbstausführende Vertragsabwicklung möglich machen.Wir glauben, dass die Blockchain-Technologie unsere Systeme effektiver und sicherer machen.

Die verschiedenen Disziplinen können die Blockchain-Technologie sehr unterschiedlich betrachten. Für einen Informatiker ist die Blockchain grundsätzliche eine einfache Datenstruktur, die Daten in einzelnen "Blöcken" verkettet und in einem verteilten Netz redundant verwaltet. Die Alternative wäre z.B. eine konventionelle Datenbank. Für die IT-Sicherheitsexperten hat die Blockchain den Vorteil, dass die Daten in den einzelnen "Blöcken" manipulationssicher gespeichert werden können, das heißt, die Teilnehmer an der Blockchain sind in der Lage, die Echtheit, den Ursprung und die Unversehrtheit der gespeicherten Daten zu überprüfen. Die Alternative wäre hier z.B. ein PKI-System. Für den Anwendungsdesigner bedeutet die Nutzung der Blockchain-Technologie eine vertrauenswürdige Zusammenarbeit zwischen verschiedenen Organisationen. Die Alternative könnte hier z.B. ein kostenintensiver Treuhändler sein.

Grundsätzlich sind Blockchains fälschungssichere, verteilte Datenstrukturen, in denen Transaktionen in der Zeitfolge protokolliert nachvollziehbar, unveränderlich und ohne zentrale Instanz abgebildet sind. Mit Hilfe der Blockchain-Technologie lassen sich Eigentumsverhältnisse direkter und effizienter als bislang sichern und regeln, da eine lückenlose und unveränderliche Datenaufzeichnung hierfür die Grundlage schafft.

Nach einer Studie, die der eco-Verband in Auftrag gegeben hat, glaubt der Mittelstand an die Blockchain. Die Blockchain setzt sich für bestimmte Anwendungsfälle und Branchen in der Breite durch – das denken 44 Prozent der Mittelständler. Neun Prozent der befragten Unternehmen planen bereits konkret den Einsatz einer Blockchain im eigenen Unternehmen. 17 Prozent der Befragten denken immerhin über den Einsatz in ihrem Unternehmen nach. Drei Prozent der Mittelständler nutzen die Blockchain bereits. Nur 26 Prozent glauben nicht an diese Technologie, 30 Prozent sind unschlüssig oder machen keine Angaben.

Die IT-Marktführer in den USA bauen ihre IT-Systeme und Dienstleistungen in der Regel auf zentrale Dienste auf. Dazu passt das Konzept der Blockchain-Technologie

nicht wirklich! Da wir in Deutschland und in der EU sehr viel mehr KMUs haben, ist die Blockchain eine ideale IT-Technologie, die eine vertrauenswürdige verteilte Zusammenarbeit ermöglicht. Daher bin ich mir sehr sicher, dass wir mit Hilfe der Blockchain-Technologie in vielen Bereichen den Digitalisierungsprozess beschleunigen, aber auch sicherer und vertrauenswürdiger umsetzen werden können.

Damit neue Geschäftsideen mit der Blockchain-Technologie positiv gestaltet werden können, haben wir den Informationstag "Bockchain" eingerichtet, um über die Möglichkeiten zu diskutieren und Blockchain Anwendungen aufzeigen. Dazu haben wir eine spannende Agenda mit interessanten Themen und hochrangigen Externen im Bereich Blockchain zusammengestellt.

Ich wünsche Ihnen beim Lesen der Ergebnisdokumentation des TeleTrusT-Informationstags "Blockchain" eine spannende Zeit und hilfreiche Erkenntnisse.

Prof. Dr. Norbert Pohlmann

Vorsitzender des TeleTrusT – Bundesverband IT-Sicherheit e.V
Leiter des Instituts für Internet-Sicherheit – if(is) der Westfälischen Hochschule, Gelsenkirchen

2 "Was ist die Blockchain - Strategien und Möglichkeiten"

Prof. Dr.-Ing. Volker Skwarek, Technische Informatik, Hochschule für Angewandte Wissenschaften Hamburg

Einleitung

Blockchains stellen einen aktuellen, sehr dynamischen IT-Innovationstrend dar, der sich nicht nur auf Computertechnik bezieht, sondern zudem eine Einflussnahme auf gesellschaftliche, politische und juristische Grundpfeiler verursacht (vgl. Voshmgir 2016, S. 8). Es wird hier auch von disruptivem Potenzial gesprochen. Dieses Potenzial besteht darin, dass alle Teilnehmer an einer Blockchain grundsätzlich über alle Daten verfügen und so Daten keiner zentralen Verwaltung und Kontrolle mehr unterliegen. Möglicherweise sind solche Daten nicht direkt lesbar, weil zusätzlich verschlüsselt. Dennoch kann eine Transaktion von niemandem angezweifelt, vorgetäuscht, verleugnet oder nachträglich modifiziert werden. Eine solche Modifikation wäre dann immer singulär und würde durch die erforderliche Konsensbildung über die Mehrheit der Teilnehmer immer entdeckt werden. Dieser Mechanismus wird auch als verteiltes Journal oder mit dem englischen Fachbegriff *Distributed Ledger* bezeichnet. Die Verkettung dieser Blöcke durch (kryptografische) Prüfsummen, wobei die Prüfsumme des vorherigen Blockes immer im nachfolgenden Block abgelegt wird, unterbindet darüber hinaus auch jede Modifikation der Reihenfolge und gibt der Blockchain-Technologie ihren eigentlichen Namen: verkettete Blöcke bzw. engl. *chain of blocks – Blockchain.* Somit müsste als korrekte Bezeichnung eigentlich der vollständige Begriff *Blockchain* and *Distributed Ledger* verwendet werden, wird im öffentlichen Sprachgebrauch aber als *Blockchain* abgekürzt. Mit dieser Bedeutung soll der Begriff Blockchain auch als deutscher Fachbegriff im Folgenden verwendet werden.

Dieser Beitrag widmet sich Basisbetrachtungen zu Blockchains: Dazu werden neben einem historischen Abriss auch kurz Grundlagen von Blockchains einschließlich entsprechender Sicherheitsaspekte ausgeführt. Weitere Aspekte sind dann Anwendungsfälle von Blockchains, bevor auf wirtschaftliche und politische Handlungsfelder eingegangen wird. Der Beitrag schließt mit einer Zusammenfassung und einem Ausblick.

Ursprung und Kerneigenschaften von Blockchains

Der Ursprung des Begriffes Blockchain wird oft fälschlicherweise auf eine Basispublikation von Nakamoto (vgl. Nakamoto 2008) zum Bitcoin-Dienst zurückgeführt. Hier taucht dieser Begriff selbst aber nicht auf, allerdings in seinem in 2007 kommentierten Code zu Bitcoin. Damit ist die Namensgebung wohl zurecht dem Autoren unter dem Pseudonym Nakamoto zuzuschreiben.

Allerdings handelt es sich hierbei nicht um die technologische Quelle. Diese beruht auf der Absicherung von Serverprotokollen gegen Manipulation nach Angriffen (vgl.

Haber und Stornetta 1991) bzw. auf der effizienten Bildung kryptografischer Checksummen (hashes) über eine große Zahl von Einzeldokumenten (vgl. Merkle 1989). Die Absicherung von Nachrichten über deren Verteilung und mehrheitsbasierte Überprüfung durch mehrere Kommunikationsrunden kann wiederum auf die byzantinische Fehlertoleranz (vgl. Lamport, Shostak, und Pease 1982) zurückgeführt werden.

Somit sind Blockchains zwar keine Erfindung von Nakamoto, sondern lassen sich in ihren Basiseigenschaften auf zahlreiche zu dieser Zeit schon langjährig implementierte Technologien zurückführen. Nichtsdestotrotz ist der Bitcoin-Entwicklung noch immer eine äußerst hohe Innovation zuzuschreiben, da diese Technologien in einem Umfang kombiniert und systematisiert wurden, dass sie die heutige Blockchain-Architektur mit dem entsprechend dahinterliegenden Protokoll erst ermöglichte.

Archetypische Blockchains stehen somit aufgrund der Eigenschaften ihrer Ursprungssysteme für

- verteilt: das Systemwissen einschließlich der gesamten Historie kann vollständig an jedem Knoten zur Verfügung stehen,
- manipulationsgeschützt: Verkettung der Transaktionen, Verteilung und Konsens erfordern einen >50%-Angriff, um eine Transaktion zu manipulieren,
- vertrauenswürdig: die Autorisierung von Transaktionen durch einen Nutzer ist durch kryptografische Verfahren sichergestellt und nachvollziehbar,
- systematisch und aufwandsgesteuert: Aufwand der Transaktionsabsicherung ist skalierbar,
- konsensbasiert: eine Transaktion gewinnt zunehmend an Zuverlässigkeit, je mehr Teilnehmer diese bestätigen.

Hierdurch entstehen neue Arten von IT-Anwendungen, die ohne diese Technologie nur mit sehr hohem Aufwand, mit einer vertrauenswürdigen Mittelsperson zur Datenhaltung oder sogar mit vertretbarem Aufwand gar nicht realisierbar gewesen wären. Beispiele dafür sind internationale Kunstwerkregister, Anwendungen zum Realitäts- und Identitätsnachweis oder auch öffentliche Wahlsysteme. Insbesondere letztere sind in die Kategorie der transparenten Verwaltungssysteme einzuordnen, die dann auch Potenzial für einen gesellschaftlichen Wandel haben: Es muss nicht mehr Personen vertraut werden, dass diese empfindliche Verwaltungsprozesse ohne Manipulation durchführen, sondern je nach Wahl des Systems sind alle Transaktionen öffentlich. So kann beispielsweise die Einführung von Demokratisierungsprozessen in Entwicklungsländern unterstützt werden.

Sicherheitsbetrachtungen in Blockchains
Die Sicherheit eines IT-Systems ist gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI) folgendermaßen definiert:

"IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit

ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind." (vgl. Bundesamt für Sicherheit in der Informationstechnik 2013 Stichwort "IT-Sicherheit")

Hieraus folgt, dass IT-Sicherheit ein Relativmaß in Bezug auf den Aufwand des unberechtigten Datenzugriffes darstellt. Somit sind auch Blockchains nicht absolut sicher, sondern müssen aufwandsbezogen betrachtet werden. Sicherheitsmaßnahmen in der Blockchain folgen genau diesem Konzept und leiten sich aus den nachstehenden Maßnahmen ab:

- *Distribution*: Die Informationen sind gleichartig an verschiedene Stellen des Systems kopiert, so dass ein lokaler, singulärer Angriff detektiert und behandelt werden kann.
- *Proof of Work/Proof of Stake*: Durch ein Aufwands- und Zufallsprinzip lässt sich nicht unmittelbar vorhersagen, welcher Teilnehmer der Blockchain den nächsten Transaktionsblock verifiziert. Somit lassen sich Manipulationen verhindern, bei denen immer derselbe Knoten eine Verifikation vornimmt und damit die Möglichkeit hat, Falschinformationen einzufügen.
- *Consensus*: Berechnete Transaktionsblöcke und Prüfsummen müssen erneut von den Teilnehmern der Blockchain bestätigt werden. Erst wenn mehr als die Hälfte der Knoten einen solchen Block bestätigt hat, besteht der Konsens und der Block gilt als korrekt.

Folglich ist es in einer Blockchain sehr aufwändig, Transaktionen konsistent zu fälschen, da solche Manipulationen an zahlreichen Knoten in einer Blockchain gleichzeitig erfolgen müssen., so dass ein >50%-Konsens über die manipulierten Informationen erreicht wird.

Genau in dieser Sicherheitsmaßnahme besteht aber auch die größte Sicherheitslücke von beispielsweise Bitcoin als bekannteste Implementierung: Wenn eine regional oder hierarchisch gehäufte Abhängigkeit von Minern – also Knoten, die zur initialen Blockverifikation berechtigt sind – besteht, so entstehen hier Manipulationsmöglichkeiten:

- Durch die zeitliche Verzögerung der Informationsausbreitung korrekt berechneter Blöcke, kennen räumlich um den erfolgreichen Miner herum konzentrierte Knoten das richtige Mining-Ergebnis schneller als weiter entfernte und können wiederum früher mit der Berechnung des nächsten Knotens beginnen. Es erfolgt also eine regionale Verzerrung der Verteilung erfolgreich berechneter Blöcke. Hierbei handelt es sich nicht nur um eine theoretische Gefahr, da derzeit ca. 60% der Mining-Kapazität auf 5 regionale Mining-Pools konzentriert sind (vgl. Blockchain Info 2017b).
- Die Bitcoin Blockchain basiert darauf, dass vollwertige Knoten über die gesamte Transaktionshistorie verfügen. Zum Zeitpunkt der Recherche September 2017 beträgt die Größe der Datei mit allen Bitcoin-Transaktionen

über 130 GB (Blockchain Info 2017a). Dadurch wird die Anzahl der Knoten, die eine solche Menge von Transaktionen verarbeiten kann, eingeschränkt.

Weitere mögliche Sicherheitslücken insbesondere der Bitcoin-Implementierung können mehreren Studien des Joint Research Centers und der Europäischen Union (vgl. Nai Fovino und Steri 2017; Muftic, Sanchez, und Beslay 2016, Kap. 6) entnommen werden.

Weiterhin soll aber festgehalten werden, dass Blockchain-Technologien für verteilte Technologien als vergleichsweise sicher gelten, da ein hoher Aufwand getrieben werden muss, um effiziente Angriffe zu starten.

Exemplarische Anwendungsfälle
Derzeit werden nahezu beliebige Anwendungsfälle zur Datenhaltung und –verarbeitung mit Hilfe von Blockchain-Technologien umgesetzt, auch wenn möglicherweise klassische Datenbanktechnologien mit geringerem Aufwand ein vergleichbares Ergebnis liefern würden: Zentrales Selektionskriterium für eine entsprechende Anwendung sollte die Notwendigkeit für einen Datenzugriff mehrerer Parteien mit einem untereinander eingeschränkten Vertrauensverhältnis sein. Ein solch eingeschränktes Vertrauensverhältnis liegt in der Regel in folgenden Fällen vor:

- Eine Partei kann zu Lasten einer anderen Partei durch das Behaupten der Unwahrheit einen erheblichen Vorteil erzielen. Beispiel: Transaktionsmanagement.
- Daten sind von öffentlichem Interesse, und durch einseitige Modifikation der Daten kann ein Vorteil erzielt werden. Beispiel: öffentliche oder zugriffsbeschränkte Register.
- Es handelt sich um Daten, die bei mehreren Partnern in gleicher Form vorliegen müssen, um damit beispielsweise ein komplexes System zu steuern. Beispiel: verzweigte/vernetzte technische Systeme.
- Eine große Anzahl von Partnern muss sequentiell auf die Daten zugreifen, um einen Prozess abzubilden. Hier lassen sich durch Blockchains die Anzahl der Schnittstellen, möglicherweise sogar der involvierten Partner reduzieren. Beispiel: internationaler Handel und Versand (engl.: supply chain management).

Umfangreiche Beispiele für Anwendungsmöglichkeiten können Publikationen wie (vgl. Boucher 2017; Muftic, Sanchez, und Beslay 2016; Fovino, Nordvik, und Masera 2015) entnommen werden. In allen Fällen muss über die ausschließliche Frage der technischen Realisierbarkeit hinaus auch beachtet werden, dass mögliche nationale oder internationale Rechtsvorschriften einer ausschließlichen Abbildung auf einer Blockchain entgegensprechen. Beispiele hierfür sind in Deutschland der Aktienhandel, für den es noch immer in Papierform hinterlegte Aktien geben muss, oder die Übertragung von Grundstückseigentum, das der Form eines notariellen Vertrages mit Eintrag in ein physisches Grundbuch bedarf.

Wirtschaftlich/politische Bedeutung und Handlungsfelder
Gerade durch die verteilte, möglicherweise sogar öffentliche, unmanipulierbare Datenhaltung besteht in der Blockchain-Technologie auch ein hohes Potenzial zur gesellschaftlichen Veränderung. An allen Stellen, insbesondere in der Verbreitung gesellschaftlich systemrelevanter Informationen mit hohem Transparenzbedarf wie Wahlergebnisse, juristische Personen (Vereins- und Handelsregister) oder persönliche Identitäten sind derartige öffentliche Register von hoher Bedeutung. So können durch die Einführung von Blockchain-Applikationen in Nationen mit geringer Verwaltungstransparenz Demokratisierungsprozesse vorangetrieben werden. Darüber hinaus werden hierdurch neue Anwendungen möglich: Beispielsweise könnte der digitale Personalausweis durch eine nationale, behördliche Identitäts-Blockchain verifiziert werden und durch den Zugriff weiterer Anwendungen darauf, wie beispielsweise von Banken, eine verbesserte Identifikation beim Eröffnen von Online-Konten bestehen.

Es entsteht hier also durch die Interaktion mehrerer Anwendungsbereiche mit Blockchains ein erheblicher gesellschaftlicher Mehrwert, der auch in weit entwickelten Demokratien noch zu einer Erhöhung der Transparenz durch eine bessere Verfügbarkeit und Zugreifbarkeit der Informationen führt. Damit verbunden können dann Kostenreduktionen durch eine geringere Anzahl von Schnittstellen und eine höhere Datendurchlässigkeit erzielt werden. Allerdings ist hier zu berücksichtigen, dass an dieser Stelle auch gesetzlich geregelte Verwaltungsprozesse tangiert werden und somit auch juristische Aspekte der Interaktion mit Blockchains in den Vordergrund kommen.

Smart Contracts:
Spätestens bei diesen Betrachtungen, also der Interaktion zwischen Computerprogrammen und Recht, liegt es nahe, den Begriff der *smart contracts* einzuführen, der in seinem Ursprung dem amerikanischen Computerwissenschaftler Nick Szabo (vgl. Szabo 1997) zugeschrieben wird. Hier beschreibt dieser, wie sich juristische Geschäftsprozesse durch Hardware und Software unangreifbar machen lassen. Dabei hatte Szabo selbst nicht vor, auch die juristische Verantwortung vom Bediener selbst zu nehmen. Er spricht in diesem Kontext von einer *vending machine*, also einem Verkaufsautomaten, dessen juristische Folgen sich dem Bediener zurechnen lassen müssen (vgl. Szabo 1997, Kap. Contracts Embedded in the World).
Ohne dieses Thema an dieser Stelle auch nur grundlegend diskutieren zu können, variieren die Perspektiven auf smart contracts von der Position, dass es sich hier um ausschließliche Prozessautomatisierungen ohne Rechtscharakter handelt – wie beispielsweise durch Nick Szabo vermittelt – bis hin zu unterschiedlichen möglichen Phasen nach Lessig, bei der die Phase 3 lautet "code is law" (vgl. Lessig und Lessig 2006) und neuesten, darüber hinausgehenden Publikationen, die sogar "law is code" (vgl. De Filippi und Hassan 2016) zur Diskussion stellen.

Dies zeigt, dass die technische und juristische Betrachtung von Smart Contracts sehr weit über eine automatisierte Bearbeitung vorher festgelegter Abläufe hinausgeht.

Hieraus entsteht dann gesetzgeberischer Handlungsbedarf, dass smart contracts regulatorische Randbedingungen einhalten müssen, um bei juristischen Auseinandersetzungen nicht als von vornherein ungültig erklärt zu werden.

Standardisierung:
In Anbetracht dessen, dass eine Auslegung von Smart Contracts als Programmcode, der Rechtsgeschäfte bewusst herbeiführt, mindestens möglich, wenn nicht sogar sehr wahrscheinlich ist, werden Smart Contracts auch technische Rahmenbedingungen einhalten müssen. Daher ist eine Standardisierung sinnvoll, um einen öffentlich akzeptierten Stand der Technik herbeizuführen und somit auch eine Rechtssicherheit innerhalb der technischen Entwicklung herzustellen. Da es sich bei Blockchains um grenzüberschreitenden Datenverkehr handelt, findet die Standardisierung sogar im Rahmen der International Standardisation Organisation (ISO) innerhalb von ISO/TC 307 statt (vgl. Brave Coin 2016). Da die offizielle Gründung erst zum 07.04.2017 erfolge, sind die Arbeiten zum Zeitpunkt dieser Texterstellung noch sehr grundlegend: Es wurden fünf study groups und eine working group gegründet. Standards werden in working groups erstellt, während study groups zu standardisierende Elemente vorschlagen und dann ggf. in working groups ausarbeiten. Die working groups bzw. study groups befassen sich dabei mit folgenden Themen: Terminologie, Referenzarchitektur, Ontologie und Taxonomie, Anwendungsfälle, Security/Privacy, Indentity, Smart Contracts.

Zusammenfassung und Ausblick
In diesem Beitrag wurde gezeigt, dass Blockchains (korrekt: Blockchain und Distributed-Ledger-Technologien) in unterschiedlichsten Bereichen zu neuartigen Lösungsansätzen führen. Dadurch verfügen sie tatsächlich über das disruptive Potential, das ihnen zugesprochen wird. Auch wenn Blockchains keine absolute Sicherheit versprechen können, liegt doch trotz oder gerade wegen der öffentlichen Datenhaltung ein sehr hohes Sicherheitsniveau vor. Allerdings konnte auch gezeigt werden, dass sich durch Ungleichverteilungen von Rechenkapazitäten und durch Konzeptgrenzen Sicherheitslücken öffnen.

Über verschiedene, generalisierte Anwendungsfälle wurden dann Smart Contracts eingeführt, die zu einer Automatisierung von (Geschäfts-)Prozessen innerhalb der Blockchain führen. Letztlich können daraus auch juristische Verbindlichkeiten entstehen, die den Smart Contracts direkt zuzuschreiben sind. Wenn sich diese Ansicht juristisch bestätigen sollte, dann ist an dieser Stelle auch mit gesetzlichen Regelungen zu rechnen. Um eine technische Vergleichbarkeit und Interoperabilität zu ermöglichen, wurde hier die internationale Standardisierung mit ISO/TC 307 aufgenommen, um daraus dann mögliche Standards für Architekturen, Terminologien oder auch Smart Contracts abzuleiten.

Literaturverzeichnis

Blockchain Info (2017a): "Blockchain Size", Blockchain.info; https://blockchain.info/blocks-size (Aufgerufen 01.09.2017)
Blockchain Info (2017b): "Hashrate Verteilung", Blockchain.info; https://blockchain.info/pools (Aufgerufen 01.09.2017)
Boucher, Philip (2017): "How Blockchain Technology Could Change Our Lives", In-depth-analysis PE 581.948. EPRS, European Parliament Research Service, Brüssel; Internet: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf (Aufgerufen 27.09.2017)
Brave Coin (2016): "Australia to lead ISO Blockchain standards endeavor"; Internet: http://bravenewcoin.com/news/australia-to-lead-iso-blockchain-standards-endeavor/ (Aufgerufen 31.10.2017)
Bundesamt für Sicherheit in der Informationstechnik (2013): "BSI - Glossar - IT-Grundschutz-Kataloge"; https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html (Aufgerufen 27.09.2017)
De Filippi, Primavera, Samer Hassan (2016): "Blockchain technology as a regulatory technology: From code is law to law is code"; First Monday 21 (12); Internet: https://journals.uic.edu/ojs/index.php/fm/article/view/7113 (Aufgerufen 27.09.2017)
Fovino, Igor Nai, Jean-Pierre Nordvik, Marcello Masera (2015): "Distributed Ledgers and European Energy Retail Market", Technical Report, Joint Research Center
Haber, Stuart, und W. Stornetta (1991): "How to time-stamp a digital document", Advances in Cryptology-CRYPT0'90, 437-455
Lamport, Leslie, Robert Shostak, und Marshall Pease (1982): "The Byzantine generals problem", ACM Transactions on Programming Languages and Systems (TOPLAS) 4 (3): 382-401
Lessig, Lawrence, und Lawrence Lessig (2006): Code. Version 2.0, New York: Basic Books
Merkle, Ralph C (1989): "A certified digital signature", In Conference on the Theory and Application of Cryptology, 218-238, Springer; Internet http://link.springer.com/10.1007/0-387-34805-0_21 Aufgerufen 27.09.2017)
Muftic, Sead, Ignacio Sanchez, und Laurent Beslay (2016): "Overview and Analysis of the Concept and Applications of Virtual Currencies", JRC Technical Report JRC 105207, JRC Technical Report, Ispra/Italy, JRC; Internet: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC105207/lbna28386enn.pdf Aufgerufen 27.09.2017)
Nai Fovino, Igor, und Gary Steri (2017): "Crypto Currencies - Cyber-Security Analysis of Current Architectures", 99976. JRC Technical Report, JRC
Nakamoto, Satoshi (2008): "Bitcoin: A peer-to-peer electronic cash system", http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Original.pdf Aufgerufen 27.09.2017)
Szabo, Nick (1997): "Formalizing and Securing Relationships on Public Networks; Internet: https://web.archive.org/web/20150919065258/http://szabo.best.vwh.net/formalize.html Aufgerufen 27.09.2017)
Voshmgir, Shermin (2016): "Blockchains, Smart Contracts und das Dezentrale Web", Technologiestiftung, Berlin

3 "Kryptografische und IT-Security-Perspektive auf Blockchain" (Proof of Stake)

Dr. Jörn-Marc Schmidt, Senior Consultant, Division Homeland Security,
secunet Security Networks AG

Ein essenzieller Bestandteil jeder Blockchain ist ein Konsensmechanismus, der bestimmt, welche Blöcke Teil der Kette werden. Der prominenteste Mechanismus, der beispielsweise aktuell bei Bitcoin und Ethereum eingesetzt wird, ist der Proof-of-Work (PoW). Um dabei einen neuen Block zu bestätigen, muss ein rechenintensives Problem gelöst werden. Die Parteien, die diese Probleme lösen um Blöcke zu erzeugen werden als Miner bezeichnet. Als Anreiz bekommt derjenige Miner, dessen Block in die Kette aufgenommen wird, eine Belohnung. Auf der einen Seite muss diese Belohnung im Verhältnis zum Einsatz der Miner stehen; auf der anderen Seite muss die Komplexität des zu lösenden Problems, und damit der nötige Aufwand der einzelnen Miner, an die verfügbare Rechenleistung aller Miner angepasst werden, um die Sicherheit der Blockchain aufrecht zu erhalten.

Ein vielversprechender alternativer Ansatz, der ohne energieintensives Suchen nach Lösungen auskommt, sind Proof-of-Stake- Verfahren (PoS). Mit Stake wird ein Anteil an der entsprechenden Blockchain bezeichnet. An Stelle von Rechenleistung der Miner tritt also der Besitz von Anteilen an der entsprechenden Blockchain. Um Blöcke verifizieren zu dürfen, hinterlegen sogenannte Validatoren Anteile; der Einfluss eines Validators steigt mit den hinterlegten Anteilen. Generell kann ein PoS realisiert werden, indem ein pseudo-zufälliger Algorithmus regelmäßig Validatoren auswählt, die einen Block erstellen dürfen. Ein alternativer Ansatz ist, dass die Validatoren über vorgeschlagene Blöcke in einem Abstimmungsverfahren die finalen Blöcke auswählen.

Die Grundidee des PoS ist nun, dass ein Validator, der nach Definition Anteile an der Blockchain hält (und hinterlegt hat), am Erhalt der Kette und ihrer Vertrauenswürdigkeit interessiert ist und daher nur korrekte Blöcke bestätigt, um nicht den Wert seiner Anteile zu mindern.

In der Praxis kann es für einen Validator jedoch ebenfalls lohnend sein, widersprüchliche Blöcke zu erstellen oder zu bestätigen, um seinen möglichen Gewinn zu maximieren. Dies wird als "Nothing at Stake"-Problem bezeichnet: Während das Bestätigen eines Blocks beim PoW Rechenleistung erfordert und sich ein Miner somit im eigenen Interesse immer für den vielversprechendsten Block entscheidet, kann ein Validator beim PoS ohne signifikante Kosten mehrere Blöcke für valide erklären (vgl. Ethereum 2017b).

Dies ist bei PoS-Verfahren, die nur erfolgreiche Validatoren belohnen – zu denen viele der ersten PoS-Ansätze zählen – problematisch. Um dies zu verhindern, kann ein entsprechendes Regelwerk eingesetzt werden. Dieses Regelwerk bestraft ent-

weder Validatoren, die widersprüchliche Blöcke bestätigen oder sogar alle Validatoren, die sich für Blöcke entscheiden, die nicht in die Blockchain aufgenommen werden. Ein Validator, der gegen das Regelwerk verstößt, riskiert seine eingesetzten Anteile zu verlieren. Der Anreiz ist beim PoS somit ein anderer als beim PoW. An Stelle des Aufwendens von Energie tritt nun der mögliche Verlust von (ökonomischen) Werten (vgl. Vitalik Buterin 2016).

Während die Grundidee des PoW nur wenige Parameter benötigt und ein inhärentes Regelwerk vorgibt, muss dies beim PoS explizit definiert werden. Dies erlaubt bei der Implementierung eines solchen Regelwerks viele Freiheiten, so dass beispielsweise Ansätze aus der Spieltheorie umgesetzt werden können, um Kartellbildung zu verhindern. Denn ähnlich eines 51%-Angriffs auf eine PoW-basierte Blockchain kann auch beim PoS ein Kartell einen negativen Einfluss auf die Kette ausüben. So könnten sich die Validatoren des Kartelles beispielsweise weigern, Blöcke zu finalisieren und somit keine (oder langsamer) neue Transaktionen zu zulassen oder aber Blöcke mit einer bestimmten Transaktion nicht zu finalisieren und diese somit zu zensieren (vgl. Ethereum 2017b).

Der Nachteil dieser Freiheiten ein Regelwerk zu definieren liegt darin, dass dies das Design und die Implementierung im Vergleich zum PoW sehr komplex und somit potenziell fehleranfällig macht.

Um die Auswirkungen von möglichen Fehlern zu minimieren, sind auch hybride Verfahren, die PoW und PoS einsetzen, denkbar. So soll beispielsweise das von Ethereum-Entwicklern forcierte PoS-Verfahren CASPER den PoW nicht komplett ersetzen, sondern in einem ersten Schritt nur jeden hundertsten Block finalisieren. CASPER selbst wird derzeit implementiert und soll als Smart Contract unter Ethereum veröffentlicht werden (vgl. Ethereum 2017a).

In Summe eröffnet der Einsatz von Proof-of-Stake-basierten Konsensmechanismen interessante Möglichkeiten, die einen Proof-of-Work ergänzen oder sogar ablösen könnten. Die Sicherheit hängt jedoch direkt von dem konkreten Design und dessen Implementierung ab. Erst nach einer ausführlichen Betrachtung der Vor- und Nachteile kann eine verlässliche Aussage über die Sicherheit einer spezifischen Umsetzung getroffen werden.

Literaturverzeichnis

Vitalik Buterin (2016): A Proof of Stake Design Philosophy.
Internet: https://medium.com/\@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51 (Aufgerufen 30.08.2017)
Ethereum (2017a): Casper Version 1 Implementation Guide; Internet:
https://github.com/ethereum/research/wiki/Casper-Version-1-Implementation-Guide (Aufgerufen 30.08.2017)
Ethereum (2017b): Proof of Stake FAQ;
Internet: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ (Aufgerufen 30.08.2017)

4 "Rechtliche Fragestellungen zu Blockchain"

RA Dr. David Klein, LL.M, Taylor Wessing Partnerschaftsgesellschaft mbB

Rechtliche Herausforderungen der Blockchain
Die Blockchain-Technologie, in ihrer Abstraktheit, wirft eine Vielzahl rechtlicher Fragen auf, die nicht zuletzt darin begründet sind, dass die Blockchain als technisches Rückgrat in vollkommen unterschiedlichen Szenarien eingesetzt werden kann.

Smarte Verträge oder nicht?
Grundlegende Herausforderungen betreffen insbesondere marktreife Implementierungslösungen, die als sogenannte "Smart Contracts" bekannt sind. Solche "intelligenten" Verträge erlauben eine automatisierte, unkomplizierte und zügige Abwicklung von Rechtsbeziehungen in unterschiedlichsten Konstellationen auf verschiedene Art und Weise, etwa im Rahmen einer Car-Sharing-Plattform (Zugang zum Fahrzeug gegen Authentifizierung und direkter Bezahlung) oder bei kleinteiligen Transaktionen im Energiesektor (Stromzukäufe/-verkäufe im Cent-Bereich).

Ausgehend von solchen Geschäftsmodellen stellt sich als erstes die Frage, welche rechtliche Qualität der Smart Contract zwischen den Parteien überhaupt hat: Begründet der Smart Contract an sich ein Rechtsverhältnis? Und integriert der Smart Contract Vertragsschluss, Vertragsdurchführung und Beendigung? Diese Auffassung würde dazu führen, dass nicht nur Unklarheiten darüber bestehen, wie der Vertragsschluss und vor allem zwischen wem stattfindet (z.B. im Rahmen einer "anonymen" Blockchain), sondern auch wie die Abwicklung unvollständiger oder fehlerhafter Verträge auf der Blockchain abzubilden sind. Beispielsweise lässt sich eine Anfechtung, die bei Erfolg eine Willenserklärung ex tunc, also rückwirkend beseitigt, in einer Blockchain technisch kaum oder nur äußerst schwierig darstellen. Die Transaktion, die die angefochtene Willenserklärung beinhaltet, müsste gelöscht und aus der Kette entfernt werden, alle Folgeblöcke wären damit erst einmal fehlerhaft und müssten durch eine neue Kette ersetzt werden. Alternativ wäre eine Korrektur durch eine neue Transaktion möglich, die die ursprüngliche Transaktion umkehrt. Ein solches Konstrukt wiederum wäre juristisch jedoch eher als ein sogenanntes Rückgewährschuldverhältnis einzuordnen, das rechtlich von der Anfechtung streng zu unterscheiden ist.

Einfacher und zielführender ist es daher, Smart Contracts nicht als Verträge im juristischen Sinne zu begreifen, sondern als technische Umsetzung eines bereits zwischen den Parteien bestehenden juristischen Vertrages. Die Parteien einigen sich also vor "Abschluss" eines Smart Contracts bereits im realen Leben und legen die Parameter für die Vertragsdurchführung fest. Der formaljuristische Vertrag besteht damit und wird lediglich über den Smart Contract abgewickelt. So können dann bestimmte Leistungspflichten im Rahmen eines Smart Contracts abgebildet werden, ebenso wie die Abwicklung der Gegenleistung.

Damit entledigt man sich auch elegant der Frage, ob die Programmierung eines Smart Contracts eine Rechtsdienstleistung darstellt, die nur von berechtigten Personen nach dem Rechtsdienstleistungsgesetz durchgeführt werden darf. Ist der Smart

Contract lediglich die tatsächliche Umsetzung eines Vertrages, der vorher zwischen den Parteien vereinbart wurde, unterfällt er selbstverständlich nicht dem Gesetz über Rechtsdienstleistungen.

Datenschutz

Ein weiterer wesentlicher Punkt bei der rechtlichen Bewertung von Blockchains ist der Datenschutz. In diesem Bereich gibt es diverse Herausforderungen, die insbesondere in Bezug auf die jeweilige Ausgestaltung der Blockchain unterschiedlich ausfallen können. Je nachdem, ob z. B. eine eindeutige Identifizierung der jeweiligen Teilnehmer im Vorfeld notwendig ist oder nicht, ist zu überlegen, ob tatsächlich ein Personenbezug der Transaktionsdaten auf der Blockchain besteht. Ist die Blockchain verschlüsselt, wäre dieser Personenbezug wohl aufgehoben, nicht jedoch dann, wenn die Entschlüsselung jedenfalls durch die Teilnehmer der Blockchain möglich wäre. Gerade in Bezug auf die Historie einer Transaktion, die ja dem Wesen nach die Gesamtheit der bisherigen Transaktionen für den jeweiligen Gegenstand beinhaltet, etwa bei der Lizensierung eines Fotos mithilfe der Blockchain die bislang eingeräumten Nutzungsrechte und die Lizenzkette an diesem Foto, wäre eine transparente Blockchain womöglich nicht datenschutzkonform, jedenfalls nicht notwendig, um die Funktionalität der Blockchain zu gewährleisten.

Zu klären ist auch zwingend, wer überhaupt der Verantwortliche im datenschutzrechtlichen Sinne ist, denn diesen treffen die maßgeblichen Pflichten des Datenschutzrechts. Da die Blockchain theoretisch auch als vollkommen autonomes System funktionieren kann, d. h., ohne eine einzelne Person, die hierfür verantwortlich ist, oder nur ein Konsortium aus verschiedenen Teilnehmern, die jedoch auf die konkrete Verarbeitung der Blockchain selbst keinen Einfluss haben, lässt sich diese Frage nicht in ihrer Absolutheit beantworten. Soweit ein Unternehmen ein Blockchain-basiertes Geschäftsmodell startet, das sie selbst kontrolliert und in gewissem Maße Einschränkungen für den autonomen Charakter der Blockchain in Kauf nimmt, dürfte aber dieses Unternehmen als verantwortliche Stelle zu klassifizieren sein, insbesondere bei privaten Blockchains, wo der Zugang zu der Blockchain durch besagtes Unternehmen reguliert wird.

Dieser Verantwortliche sieht sich diversen Pflichten nach der Datenschutzgrundverordnung ausgesetzt. Umfassende Informations- oder Auskunftsrechte z.B. können ebenso wie das gesetzlich eingeräumte "right to be forgotten" auf der Blockchain dann nicht umgesetzt werden, wenn nicht bereits bei ihrer Konfiguration dafür Sorge getragen wurde, dass etwa die Transaktions- und Metadaten der Blockchain selbst so verschlüsselt sind, dass ein Personenbezug nicht besteht. Dies stellt aber je nach Geschäftsmodell einen Spagat dar, der nicht immer gewährleistet werden kann. Da die Rechte aus der Datenschutzgrundverordnung in dieser Hinsicht jedoch indisponibel sind, scheidet eine vertragliche Lösung mit den Betroffenen aus: diese können nicht vorab einwilligen, dass sie auf ihre gesetzlichen Rechte verzichten.

Bankenregulierung, ICO & Co.

Bei der rechtlichen Bewertung von Blockchain-basierten Geschäftsmodellen ist die Frage nach dem Austausch von "Werten", d. h., von E-Geld, virtuellen Währungen oder wie auch immer der jeweilige werthaltige Transaktionsgegenstand bezeichnet werden soll (üblicherweise als "Token" bezeichnet), von hoher Bedeutung. Wert und "Währung" des Tokens bestimmen grundsätzlich diejenigen, die die Blockchain und das jeweils auf ihr laufende Geschäftsmodell ins Leben gerufen haben. Die tatsächliche Herausforderung stellt sich dann, wenn der Token, mit dem Transkationen auf der Blockchain ermöglicht oder belohnt werden, in eine echte Währung außerhalb der Blockchain getauscht werden soll. In diesem Falle unterliegt zumindest der Handel mit diesen virtuellen Währungen der Erlaubnispflicht nach dem Kreditwesengesetz. Wird über die Blockchain echtes E-Geld ausgegeben, also eine Währung, die auch bei anderen Stellen als beim sogenannten Emittenten eingelöst werden kann, dann ist diese Emission lizenzpflichtig nach dem Zahlungsdiensteaufsichtsgesetz.

Neben diesen eher grundsätzlichen Themen können weitere rechtliche Fragestellungen auftauchen, die in dem jeweiligen Geschäftsmodell ihren Ursprung finden. Neben Vorschriften zur Geldwäsche sind dies insbesondere steuerrechtliche Aspekte.

Ein weiterer Sonderfall stellt der "Börsengang" über die Blockchain dar, das sogenannte *Initial Coin Offering* oder kurz ICO. Plakativ formuliert kann ein Unternehmen auf diesem Wege die Blockchain benutzen, um Wagniskapital zu beschaffen, ohne mit lästigen Formalia wie Finanzierungsrunden, Banken oder Krediten kämpfen zu müssen. Nach derzeitigem Stand ist nicht vollends geklärt, ob in diesem Falle nicht Prospektpflichten greifen, die Unternehmen auch z.B. bei anderen Finanzierungsmodellen treffen würde. Die Kosten für die Erstellung eines solchen Prospektes sind nicht unerheblich und könnten ein solches Finanzierungsmodell über ICO unattraktiv machen.

Summary

Die Blockchain als Technologie bietet aus rechtlicher Sicht eine Vielzahl komplexer technisch-juristischer Herausforderungen. Die wesentliche Erkenntnis sollte sein, dass diese rechtlichen Herausforderungen sehr unterschiedlich sein können, von Geschäftsmodell zu Geschäftsmodell bzw. von Anwendungsfall zu Anwendungsfall variieren und am besten frühestmöglich adressiert werden.

Während in bestimmten Bereichen die Anforderungen aus rechtlicher Sicht eher gering sind, können bei komplexeren Projekten ganz erhebliche Hürden bestehen. Insbesondere bei Berührungen mit den Bereichen Bankenregulierung und Datenschutz drohen empfindliche Bußgelder und unter Umständen auch die persönliche Haftung der jeweilig verantwortlichen Person, sodass eine frühe juristische Begleitung dieser Projekte angezeigt ist.

5 "*Entwicklung der Standardisierung und Interoperabilität von Blockchain*"

Volker Jacumeit, Gruppenleiter "IT und IT-Sicherheit",
DIN Deutsches Institut für Normung e.V.

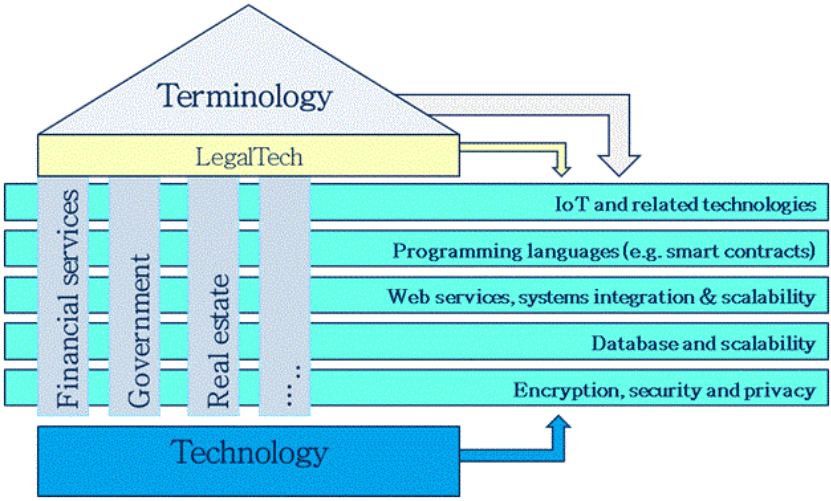
Vielzahl möglicher Anwendungen
Es ist genau der Wegfall der Intermediäre, die Blockchain and distributed ledger technologies eine schier unendliche Vielzahl von Anwendungsfällen eröffnet.

- Für den Transfer von Geld benötigen wir keine Banken mehr
- Für den Kauf von Grundstücken benötigen wir keine Notare mehr
- Musiker verkaufen ihre Werke ohne Verlage und Gema

Aber die Technologie steckt noch in den Anfängen. Themen wie Stornos oder gegenseitige Verrechnungen zwischen Blockhains sind noch nicht geregelt, was für die Finanzwelt wichtige Funktionen sind. Außerdem stehen große Investitionen an, um die Technologie in der gesamten Breite einzuführen. Hinzu kommt, dass dies Intermediäre in der Regel auch beratende und nicht nur technisch vermittelnde Aufgaben haben und diese kann die Blockchain nicht ersetzen. So ist zurzeit nicht davon auszugehen, dass die Banken und Notare kurzfristig von Blockchains abgelöst werden.

Es ist davon auszugehen, dass es kleine, private Blockchain-Systeme geben wird, die nur von einem begrenzten Kreis von Berechtigten genutzt werden – etwa von Banken und ausgewählten Großkunden oder im Industriebereich von großen Konzernen wie den Automobilherstellern und ihren Zulieferern. Durch das Entstehen von vielen privaten Blockchains wächst die Forderung nach Interoperabilität.

Paradigmenwechsel
Blockchain und Distributed Ledger Technologies fordern ein komplettes Umdenken im Umgang mit den bisherigen Internettechnologien. Und diese sind ja selber noch nicht besonders alt. Es ist auch noch nicht absehbar, was diese neue Technologie alles ermöglicht und ob alles, was technisch damit möglich ist, auch ethisch, moralisch und politisch gewollt ist. Bei den Smart Contracts muss man sich schließlich fragen, ob man bewährte Prinzipien wie der Wahrung des Besitzstandes letztlich aufgeben will. Fest steht aber, hier müssen die unterschiedlichsten Fachrichtungen zusammen an Lösungen arbeiten und bereit sein vorauszudenken, was in wenigen Jahren mit Blockchain alles realisiert werden kann. Technik-Konvergenz, Geschäftsfeld-Konvergenz und eine direkte Verschmelzung von Programm-Code und Verträgen erfordern ein bisher nicht dagewesenes Zusammenarbeiten. Die Basis dafür ist ein gemeinsames Verständnis, eine Terminologie und Ontologie, damit diese hochkomplexen Systeme erstellt und nicht nur von wenigen "Nerds" verstanden werden. Damit muss sich auch Normung und Standardisierung heute mit Technologien befassen und Rahmen definieren für etwas, was es heute noch nicht gibt.



Notwendigkeit der Normung

Auch wenn die Technologie in vielen Punkten nicht ausgereift ist und der Einsatz von Blockchains und verteilten Journalen für Brachen und Geschäftsfelder noch nicht eindeutig definiert ist, sollte dennoch an Normung und Standardisierung auch zu Blockchains gedacht werden. Ein sehr wichtiger Punkt von Normung und Standardisierung, insbesondere bei Technik konvergenten und Systemintegration ist Terminologie und Governance. Immer dann, wenn Experten aus unterschiedlichen Bereichen zusammenarbeiten, ist die Verständigung auf gemeinsame Definition, Begriffe und einer Ontologie wichtig. Hinzu kommt bei Lösungen mit einem starken systemintegrativen Ansatz die Notwendigkeit der Verständigung auf einen Technologierahmen (Technology Framework), in dem auch Schnittstellen definiert werden, um sowohl die Interoperabilität nach außen wie innen zu gewährleisten. Bei Blockchains bedeutet dieses z.B. festzulegen, wie private Blockchains interagieren, oder wie Blockchains in bestehende Systeme integriert werden können. Der Technologierahmen definiert aber auch welche bestehenden Normen und Standards vorhanden sind und ggf. ergänzt werden müssen. Schließlich ist auch diese Technologie eine Weiterentwicklung von Bestehendem und ja nicht vom Himmel gefallen. Folglich sind insbesondere ISO-IEC JTC 1 Normen im Bereich IT-Sicherheit, Skalierbarkeit, Webservices und IoT zu referenzieren.

Bei ISO wurde ein neues Technical Committee (TC) für "Blockchain and disributed ledger technologies" im April 2017 geschaffen, um diese Aspekte von Anfang an zu berücksichtigen. Es ist das ISO/TC 307, das sich in folgende Arbeitsgruppen aufteilt:

- WG 1 Terminology
- "Study Group on Smart Contracts" unter der Leitung von Deutschland

- "Study Group on Reference Architecture, Taxonomy, and Ontology" unter der Leitung der USA
- "Study Group on Use Cases" unter der Leitung von Japan
- "Study Group on Security and Privacy" unter der Leitung von Russland
- "Study Group on Identity" unter der Leitung von Korea

Das deutsche Spiegelgremium bei DIN, der NIA Arbeitsausschuss NA 043-02-04 AA "Blockchain und Technologien für verteilte Journale" befasst sich daher unter anderem mit folgenden Punkten:

Zum Thema Terminologie wird die Erarbeitung einer entsprechenden DIN-SPEC, die aus dem DIN-Connect-Wettbewerb hervorgegangen ist, in die Arbeit des neuen Ausschusses und vor allem in die Arbeit des TC 307 einfließen. Bei Technologien ist es wichtig, über eine Sammlung von bestehenden Technologien und Vorschlägen für Bewertungskriterien von Blockchains ein Framework zu erarbeiten. Dieses Framework muss auch die Interoperabilität zwischen Blockchains ermöglichen und für eine entsprechende Systematisierung sorgen. Zu den Technologien gehört die Möglichkeit der Synchronisation von Blockchains. Abgeleitet von sektorspezifischen Use Cases sollen Archetypen von Use Cases entwickelt werden. Diese sollen anhand eines Templates in einem Use-Case-Repository festgehalten werden. Auf diese Weise soll sichergestellt werden, dass Doppelarbeiten und Überlappungen bei der Normung auf der Ebene der Sektoren wie Industrie, Finanzwirtschaft, Government u.a. vermieden werden und so viel Gemeinsamkeit wie möglich die Komplexität verringert.

Blockchain und Distributed Ledger werden auch als Web 3.0 bezeichnet. Wer hätte von uns vor 15 Jahren geahnt, wohin uns das Web 2.0 geführt hat? Wer kann heute erahnen, wohin uns Web 3.0 führen wird? Eines aber steht fest: Wir müssen bei der Gestaltung von Anfang an dabei sein, um auch in Zukunft gestalten und mitwirken zu können.

6 "Elektronische Zustellung – Anwendungsmöglichkeiten der Blockchain"

DI Dr. Christian Baumann, Vorstandsvorsitzender, WKO/AUSTRIAPRO

Im Rahmen der AUSTRIAPRO, der Standardisierungs- und Expertenplattform in Zusammenarbeit mit der WKO (Wirtschaftskammer Organisationen in Österreich), wurde seit mehreren Jahren das System der sog. privatwirtschaftlichen elektronische Zustellung ausgearbeitet und in Folge von Unternehmen umgesetzt, die nun als Systembetreiber aktiv sind. Das System basiert auf der behördlichen elektronischen Zustellung, die seit ca. 2005 zur Übermittlung von behördlichen Dokumenten an Unternehmen und Bürger eingesetzt wird. Die privatwirtschaftliche Zustellung wurde um diverse Funktionen erweitert und erlaubt eine gesicherte und nachweisliche Zustellung von Dokumenten zwischen Personen und Firmen, in den letzten Jahren wurde eine spezielle Erweiterung für Anwälte und Notare geschaffen. Das System wird auch als "eingeschriebene E-Mail" bezeichnet.

Die Sicherheit basiert auf folgenden drei Säulen:

- Nachvollziehbarkeit: Es gibt eine garantierte (digital signierte) Übermittlungsbestätigung bzw. eine entsprechende Mitteilung bei Misserfolg.
- Rechtliche Sicherheit: Der Einsatz einer sicheren Signatur laut Signaturgesetz entspricht der Gleichstellung mit der eigenhändigen Unterschrift.
- Technische Sicherheit: Die Datenübertragung ist grundsätzlich immer verschlüsselt, die Dokumente können zusätzlich digital signiert und/oder verschlüsselt sein.

Im Rahmen eines jahrelangen Systembetriebes haben sich einige Themenbereiche gezeigt, die nicht zur Gänze optimal laufen:

Da die Komponenten des Zustellsystems (Versandservice, Zustelldienst) von unterschiedlichen Anbietern betrieben werden können, die jeweils Verzeichnisse ihrer eigenen Kunden führen, existiert ein Meta-Verzeichnisdienst, der den Austausch der Adressierungsinformationen zwischen den Diensten ermöglicht. Dieser Dienst muss sehr aufwändig (teuer) betrieben werden, da er einen single point of failure darstellt.

Der Absender einer e-Zustellung hat eine Gebühr zu entrichten (vergleichbar mit einem Briefporto). Diese Gebühr muss zwischen den beteiligten Services entsprechend aufgeteilt werden, was ein komplexes Clearing/Billing erfordert.

Die Metadaten der e-Zustellungen (Sender, Empfänger, Zeitstempel, Hashwerte der Dokumente, signierte Bestätigungen etc.) werden vom Diensteanbieter gespeichert, damit die Übermittlung zu einem späteren Zeitpunkt gegebenenfalls nachgewiesen werden kann. Wenn ein Anbieter aus irgendeinem Grund (Insolvenz, Übernahme …) wegfällt, wären diese Daten verloren oder zumindest stark gefährdet.

Durch die massive Weiterentwicklung der Blockchain-Technologien in der letzten Zeit ist es naheliegend, zu evaluieren, in welchen Bereichen der e-Zustellung diese Tech-

nologien sinnvoll eingesetzt werden können. Da Blockchains erstmals im Zusammenhang mit Kryptowährungen – allen voran dem Bitcoin –weite Verbreitung gefunden haben, bietet es sich an, das Thema "Intrabilling" (also die "peer to peer" Verrechnung der Diensteanbieter untereinander) mittels einer Kryptowährung abzuwickeln. Ob das eine bestehende Kryptowährung ist, oder eine neu für diesen Zweck geschaffene, ist zu diskutieren. Im Falle der ersten Variante könnte man auch das "Interbilling" (also die Verrechnung gegenüber den Versendern) per Micropayment mittels Kryptowährung integrieren.

Die Verwaltung von Systemteilnehmern mittels Verzeichnisdiensten bzw. die Authentifizierung der Teilnehmer an ihren jeweiligen Diensten könnte durch blockchainbasiertes "Identity und Access-Management" optimal ersetzt werden. Gemäß der Devise BYOI (bring your own identity) verwalten User ihre digitalen Identitäten selbst. Und zwar als "extrinsische" Identitäten, d.h. ohne für jedes System spezifische Identitäten anlegen und pflegen zu müssen. Im Kontext der e-Zustellung könnte das bedeuten, dass die Serviceprovider dieselbe Sicht auf die Adressierungsinformationen aller Teilnehmer haben und damit kein zentraler (Meta-)Verzeichnisdienst mehr notwendig ist.

Um Daten – in diesem Zusammenhang Metadaten von e-Zustellungen, die möglicherweise in der Zukunft zu Beweiszwecken benötigt werden – unabhängig von Betreibern und manipulationssicher zu speichern, bietet sich eine erweiterte "Notarization" an. Bei der Notarization wird der Hashwert eines Dokumentes gemeinsam mit dem Zeitstempel und anderen Informationen in einer Blockchain gespeichert, derzeit z.B. im Bitcoin oder Ethereum System. Über diesen Vorgang wird also sichergestellt, dass zu einem späteren Zeitpunkt nachgewiesen werden kann, dass das betreffende Dokument zu dem bestimmten Zeitpunkt in dieser bestimmten Form existiert hat. Beim Einsatz im Bereich der e-Zustellung müsste dieses Verfahren geringfügig erweitert werden, etwa um die oben aufgelisteten Metadaten des Zustellvorganges.

Bei der Form der Speicherung von (Meta-)daten in Blockchains gibt es mehrere Möglichkeiten, abhängig davon, wie öffentlich die Daten sein sollen. Die Daten können unverschlüsselt (d.h. für alle Teilnehmer lesbar) gespeichert werden. Das macht beispielsweise bei Informationen, die ohnehin veröffentlicht werden müssen, Sinn. Wenn die Daten verschlüsselt abgelegt werden, muss jemand für den Schlüssel verantwortlich sein, typischerweise der Urheber der Daten, mit allen Risken. Die Möglichkeit, dass die Daten "offchain" gespeichert werden und nur der Hashwert "onchain", entspricht der oben beschriebenen Notarization.

Soweit die Ansätze, mit welchen man die Blockchaintechnologien in Systemen wie dem der elektronischen Zustellung zum Einsatz bringen könnte. Aktuell läuft bei uns ein Projekt, welches die prototypische Umsetzung dieser Ansätze zum Ziel hat. Damit werden wir Vor- und Nachteile praktisch evaluieren können.

Abschließend noch die Warnung, dass der aktuelle Hype, Blockchains (und übrigens auch Smart Contracts) fast zwanghaft in allen möglichen Bereichen einsetzen zu müssen, unbedingt kritisch zu betrachten ist. In manchen Bereichen machen diese Technologien nämlich gar keinen Sinn.

7 "Secure Additive Manufacturing-Konzept für 3D-Druckdaten"

Dr. Martin Holland, Leiter Business Development und Strategie,
PROSTEP AG

Im Rahmen von "Industrie 4.0" zeichnet sich die 3D-Druck-Technologie als eine der disruptiven Innovationen ab. Kunden-Lieferanten-Beziehungen werden durch Wertschöpfungsnetzwerke abgelöst. Durch die räumlich verteilte Entstehung von gedruckten Bauteilen z. B. für die schnelle Lieferung von Ersatzteilen ergeben sich – besonders bei sicherheitskritischen Produkten - neue Herausforderungen bei Feststellung von "Originalteil", "Kopie" bzw. "Raubkopie". Markenartikel und Produkte bekommen dabei die Charakteristik von Lizenzmodellen wie wir sie aus den Bereichen Software und digitale Medien kennen. Hinzu kommt, dass 3D-Drucker für Kunststoffe schon sehr günstig geworden sind (vgl. Holland, M. 2016a). Durch den Einstieg von Microsoft in dieses Thema wird dieser Trend noch weiter verstärkt. Hierdurch hat man den Eindruck, dass dieses Verfahren schon zur Commodity geworden ist.

Von daher ist es wichtig, dass das Thema Plagiate und der Schutz vor Plagiaten eine entsprechende Aufmerksamkeit bekommt. Zumal Produktfälschungen und Markenpiraterie Milliardenschäden bei deutschen Firmen verursachen (vgl. Süddeutsche Zeitung 2015).

So warnt der Branchenverband Spectaris z.B. "Der 3-D-Druck erhöht die Gefahr von Fälschungen in der Medizintechnik ganz erheblich". Auch Technikrechtler warnen vor Plagiatsgefahren durch 3D-Drucker (vgl. Weckbrodt 2015). Und wenn der Preis von Kopiertechnologien stetig sinkt, dann steigt das Plagiate-Risiko deutlich an (vgl. Dierig 2016).

Das bedeutet, dass die Weitergabe von Konstruktionsdaten für den 3D-Druck und die dezentrale Erstellung von Objekten durch 3D-Druck nur dann wirtschaftlich sinnvoll ist, wenn es entsprechende Sicherheitsmechanismen gibt und ein entsprechendes digitales Lizenzmanagement vorhanden ist, welches sicherstellt, dass die Inhaber der Rechte angemessen entlohnt werden und dass diese kontrollieren können, wer Exemplare des entsprechenden 3D-Objekts erstellt. Dies ist besonders wichtig, weil durch die lokale Herstellung eines additiv gefertigten Bauteils, eine Kontrolle durch den Zoll vermehrt schwierig wird.

An die Integration von additiven Fertigungsverfahren in den Produktionsprozess und den gesamten Lebenszyklus eines Produktes knüpfen sich von daher wesentliche Fragen wie zum Beispiel (vgl. Schmoll, A. 2015, S1041ff. / Redeker, S.; Klett, K.; Michel, U. 2015, S58ff.).

- Wie lässt sich sicherstellen, dass beim Austausch von Produktdaten nur autorisierte Parteien Zugriff erhalten?
- Wie lässt sich absichern, dass 3D-Druckdaten nur von autorisierten Kunden und Dienstleistern für die vereinbarte Anzahl an herzustellenden Teilen verwendet werden (vgl. Deutsche Bundesregierung 2016)?

- Wie sind im Fall der Produktion mit 3D-Druck Originalteile von Raubkopien zu unterscheiden?
- Wie gestalten sich der Schutz des geistigen Eigentums, die Produkthaftung und die Gewährleistung?

Im Consumer Bereich gilt auch für additiv vom Endverbraucher hergestellte Teile, dass Privatkopien für den privaten und sonstigen eigenen Gebrauch nach §53 UrhG auch bei urheberrechtlich geschützten Werken ohne die Zustimmung des Urhebers zulässig sind. Es dürfen auch Vorlagen anderer Urheber – beispielsweise Vorlagen aus dem Internet - gedruckt werden. Dafür gelten einige Bedingungen: Die Anzahl der Vervielfältigungsstücke muss klein gehalten werden. Bei einer Stückzahl von maximal 7 Kopien gingen die Gerichte bisher von einer privaten Nutzung aus. Diese Vervielfältigungsstücke dürfen auch an Freunde und Verwandte unentgeltlich weitergereicht werden. Allerdings darf der Druckende keine Gegenleistung für die Werkstücke erhalten, da die Werkstücke sonst einem Erwerbszweck dienen. In diesem Fall würde es sich um ein Plagiat handeln. Außerdem darf die Druckvorlage nicht aus einer offensichtlich rechtswidrigen Quelle stammen (vgl. Lott 2016).

Was im Consumer Bereich für den Eigenbedarf rechtens sein kann, wird schnell zum Risiko im B2B Bereich. Von daher ist es wichtig, sich den Fragen des IP- und Plagiatschutzes zu stellen und entsprechende Schutzmaßnahmen zu ergreifen. Das Thema Plagiatschutz sollte in eine unternehmensweite Initiative zum Produkt und Know-How-Schutz eingebunden sein. Abbildung 1 zeigt die hierbei zu betrachtenden Möglichkeiten, um den Plagiatschutz möglichst hoch zu heben.

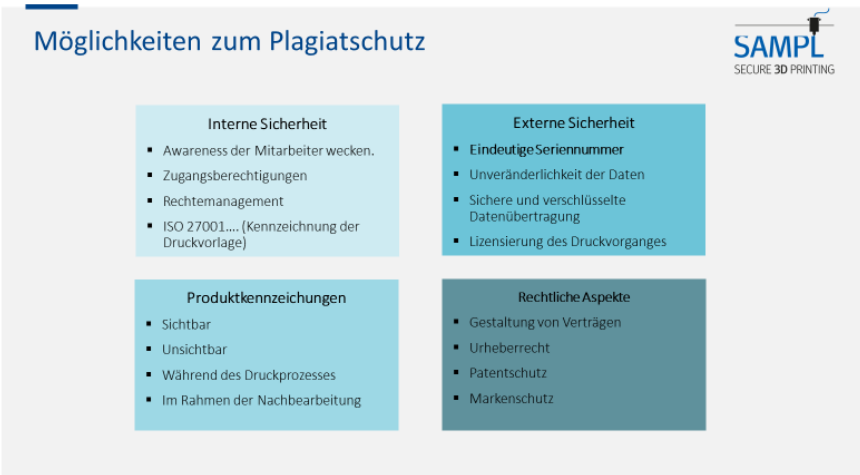


Abbildung 1: Möglichkeiten zum Plagiatschutz

Aufgrund der Besonderheiten im 3D-Druck wird derzeit über die Etablierung einer "Chain of Trust" nachgedacht. Hierbei wird die Idee verfolgt, durch den Einsatz entsprechender Technologien die möglichen Risiken auf ein Minimum zu reduzieren. Derzeit gibt es verschiedene primär kryptografische Ansätze, um die Authentizität von Druckdaten sicherzustellen und die unbefugte Nutzung von Druckdaten zu unterbinden (vgl. Holland 2016a).

Eine Möglichkeit bietet die Verschlüsselung und Lizensierung der Daten unter Nutzung der Blockchain-Technologie. Hierbei werden die relevanten Daten zum einen verschlüsselt und zum anderen erfolgt die Identifizierung der Druckvorlage und die Lizensierung des Druckvorganges über die Blockchain-Technologie. Blockchain ist bislang vor allem aus der Finanzwelt bekannt. Es handelt sich um ein kryptografisches Verfahren, um die Authentizität von finanziellen Transaktionen beim digitalen Zahlungsverkehr nachzuweisen. Eine konkrete Blockchain-Anwendung ist beispielsweise die Kryptowährung Bitcoin. Die Blockchain-Technologie ist aber grundsätzlich auch für die Abbildung von Transaktionen im Sinne von Lizenzvergaben anzuwenden. Hier erhält man statt Bitcoins die Lizenz, ein Bauteil entsprechend oft drucken zu dürfen (vgl. Holland 2016a).

Die nachfolgende Abbildung zeigt, wie die Transaktion "Alice genehmigt Bob ein bestimmtes Produkt viermal zu drucken" in einer Blockchain repräsentiert werden kann. Ein sogenannter Smart Contract legt die Lizenzinformationen in der Blockchain ab und stellt sicher, dass nur Alice und Bob diese lesen können. Bobs Drucker prüft später die Lizenz, bevor er den Druckvorgang für das Bauteil startet. Ergänzend lassen sich auch die Seriennummern der einzelnen gedruckten Bauteile in der Blockchain abbilden, um nachzuweisen, welche und wie viele Teile lizenzgemäß hergestellt wurden (vgl. Holland 2016a).

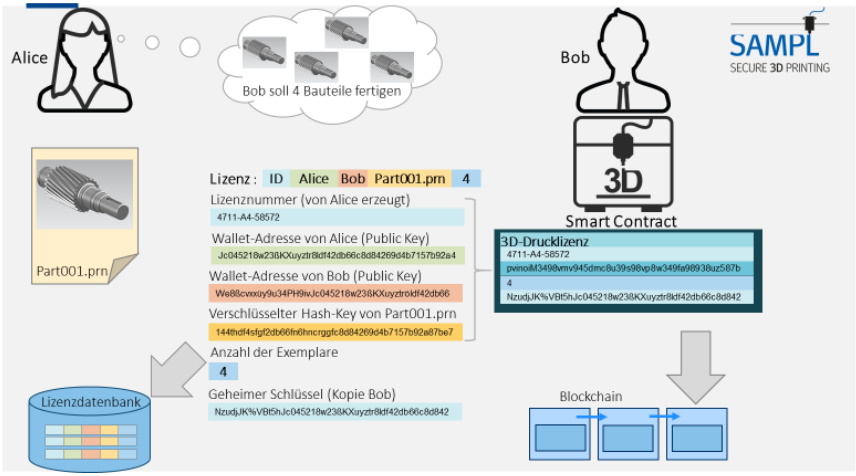


Abbildung 2: Lizenzinformationen abgebildet über Blockchain-Technologie (vgl. Holland 2016b)

Um die Chain of Trust vollständig zu schließen, ist die Einbeziehung der Maschinen und Steuerungshersteller notwendig. Hierdurch lassen sich dann ähnliche Konzepte, wie sie schon bei der Herstellung von Kopierern angewandt werden, realisieren. Ähnlich wie das Kopieren von Geldnoten verhindert wird, lassen sich durch den Einbau von sogenannten Secure Elements in Maschinen aus dem additiven Fertigungsbereich entsprechende vertrauenswürdige Drucker realisieren, die dann mit der Blockchain kommunizieren. Hierdurch lässt sich dann eine vollständige Chain of Trust vom Rechteinhaber bis hin zum Dienstleister aufbauen. Neben der Zertifizierung eines Partners ist der Einsatz zertifizierter Drucker ("Blockchain Ready") eine weitere Möglichkeit den Plagiatschutz noch eine Ebene höher zu legen (vgl. Holland 2016a).

Diese Ideen werden derzeit im vom BMWI geförderten Projekt Secure Additive Manufacturing Plattform (SAMPL, www.SAMPL-3D.de) verfolgt. Das Projekt hat eine Laufzeit von November 2016 bis Oktober 2019. Ziel des Projektes ist die Entwicklung einer durchgängigen Chain of Trust, für additive Fertigungsverfahren. Hierbei wird der gesamte Prozess von der Entstehung der digitalen 3D-Druckdaten über den Austausch mit einem 3D-Druckdienstleister und seinen durch spezielle Secure Elements abgesicherten trusted 3D-Druckern bis zur Kennzeichnung der gedruckten Bauteile mittels RFID-Chip betrachtet. Dazu soll in Ergänzung zu den heute verfügbaren Mechanismen für die Verschlüsselung von 3D-Daten ein digitales Lizenzmanagement auf Basis der Blockchain-Technologie in eine Managed-File-Transfer-Datenaustauschlösung (MFT) für den globalen Datenaustausch integriert werden. Die folgende Abbildung veranschaulicht die Systemarchitektur (vgl. Holland 2016a).

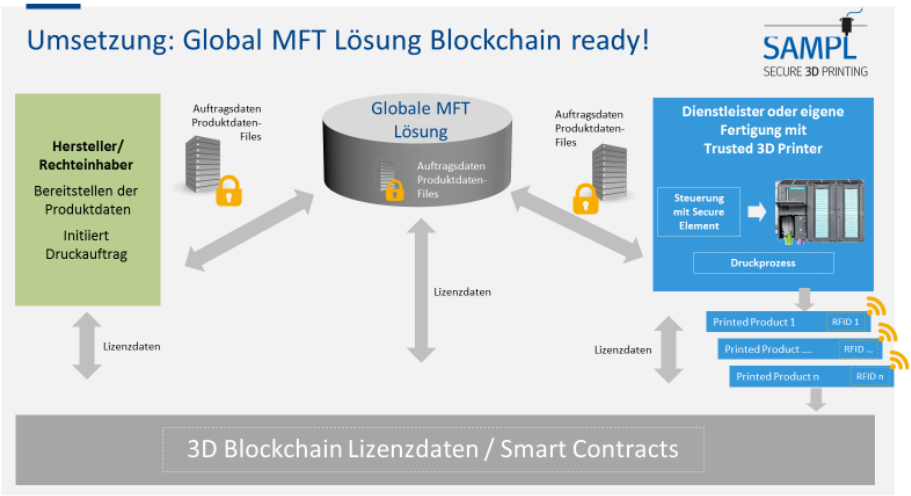


Abbildung 3: SAMPL-Systemarchitektur (vgl. Holland, M. 2016a)

Alle 3D-gedruckten und mit RFID oder anderen Identifizierungsmethoden gekennzeichneten Bauteile könnten entlang Ihres Lebenszyklus verfolgt werden. Dies ist zum einen wichtig, um durch den Verwendungsnachteils eines Bauteils Plagiate identifizieren zu können. Darüber hinaus können die so identifizierbaren Produkte zu smarten Produkten werden. Daten entlang des Lebenslaufs dieser Produkte von Ihrer Herstellung bis zum Recycling könnten die Basis für die Generierung großen Nutzens darstellen. So könnte zum Beispiel die Auswertung der Nutzung von Produkten, die Analyse typischer Schadensbilder oder spezifische Reparaturerfordernisse zu einer gezielten Weiterentwicklung und Verbesserung führen. Der heute bei vielen Produkten nicht geschlossene Regelkreis über den Produktlebenszyklus hinweg könnte so geschlossen werden und neue Innovationen ermöglichen. Diese über die reine Lizensierung des Druckes hinausgehenden Anwendungsmöglichkeiten der Blockchain werden derzeit auch im SAMPL-Projekt betrachtet.

Das in Abbildung 3 dargestellte Szenario wurde im Rahmen eines Demonstrators realisiert und erstmals auf der Hannover Messe Industrie 2017 gezeigt. Hierbei zeigte sich ein großes Interesse an der Lösung. Erste Anwendungen durch Kunden sind derzeit in Abstimmung und eine kontinuierliche Weiterentwicklung wird erfolgen.

Die mit der dargestellten Systemarchitektur verfolgten Ansätze haben zum Ziel, konkrete Nutzenpotenziale für eine Reihe von Stakeholdern zu erschließen:

- Druckerhersteller: Differenzierungsmerkmal "trusted" 3D-Drucker, Integration eines Moduls zum Urheberrechtsschutz ermöglicht Absicherung für Dienstleister und Anwender
- Urheber: IP-Schutz, Vermeidung von Raubkopien, Rechte durchsetzbar machen, Nachvollziehbarkeit der Verwendung, nutzungsabhängige Abrechnung
- OEM: sichere on-demand-Fertigung, Reduzierung von Lager- und Transportkosten, geringere Kapitalbindung, Sicherstellung von Qualität, optimierte Ersatzteilversorgung
- Druckdienstleister: reduzierte Transaktionskosten durch den Einsatz vertrauenswürdiger 3D-Drucker, Unterstützung für die Qualitätssicherung, Rechtssicherheit und Wettbewerbsvorteil
- Endkunde: verifizierbare Echtheit, Manipulationssicherheit des Designs, genaue und sichere Abrechnung, Vertrauen in das Werk, Vorteile bei Garantieansprüchen

Literaturverzeichnis

Dierig, C. (2016): "Darum gefährden 3-D-Drucker unsere Gesundheit"; unter: https://www.welt.de/wirtschaft/article153540762/Darum-gefaehrden-3-D-Drucker-unsere-Gesundheit.html (Aufgerufen 27.09.2017)
Deutsche Bundesregierung (2016): "Entwurf eines Gesetzes zur verbesserten Durchsetzung des Anspruchs der Urheber und ausübenden Künstler auf angemessene Vergütung"; (BT-Drs. 18/8625), Berlin; Internet: http://dipbt.bundestag.de/dip21/btd/18/086/1808625.pdf (Aufgerufen 27.09.2017)

Holland, M. (2016a): SAMPL Secure Additive Manufacturing Platform, Darmstadt; Internet: https://www.tuhh.de/fks/010_research/projects/sampl/de/index.html (Aufgerufen 27.09.2017)
Holland, M. (2016): "PROSTEP interne Mitteilungen"; Darmstadt.
Lott, A. (2016); "Urheberrecht beim privaten 3D-Druck – Plagiat oder Privatkopie?"; Aktuelles Wirtschaftsrecht; Hochschule für Wirtschaft und Recht; Berlin; Internet: https://wirtschaftsrecht-news.de/2016/01/urheberrecht-beim-privaten-3d-druck-plagiat-oder-privatkopie/ (Aufgerufen 27.09.2017)
Redeker, S.; Klett, K.; Michel, U. (2015) "Teil 6: IP-Recht in der digitalen Welt", [Buchverf.] T. Klindt und Peter Bräutigam, "Digitalisierte Wirtschaft/Industrie 4.0 - ein Gutachten der Noerr LLP im Auftrag des BDI zur rechtlichen Situation, zum Handlungsbedarf und zu ersten Lösungsansätzen", S. 58-72, BDI, Berlin
Schmoll, A. (2015): "Dreidimensionales Drucken und die vier Dimensionen des Immaterialgüterrechts : ein Überblick über Fragestellungen des Urheber-, Design-, Patent- und Markenrechts beim 3D-Druck"; Gewerblicher Rechtsschutz und Urheberrecht, S. 1041-1050; Berlin
Süddeutsche Zeitung (2015): "Plagiate verursachen Milliardenschäden bei deutschen Firmen"; Internet: http://www.sueddeutsche.de/news/wirtschaft/unternehmen-plagiate-verursachen-milliardenschaeden-bei-deutschen-firmen-dpa.urn-newsml-dpa-com-20090101-151213-99-293010 (Aufgerufen 27.09.2017)
Weckbrodt, H. (2015): "Technikrechtler warnen vor Plagiatsgefahren durch 3D-Drucker-Trend"; Internet: http://oiger.de/2015/06/12/technikrechtler-warnen-vor-plagiatsgefahren-durch-3d-drucker-trend/126537 (Aufgerufen 27.09.2017)

8 "*Blockchain-basiertes Supply Chain Management*"

Sebastian Stommel, Lead Researcher, CryptoTec AG

Blockchain in der Supply Chain
In einer zunehmend globalisierten und digitalisierten Welt macht die Trennung zwischen physischer Supply Chain (Lieferkette) und digitaler Supply Chain (Informationssicherheit) immer weniger Sinn. Ist die IT blockiert, stehen auch Maschinen und Transporter still. Die Blockchain bietet die sichere medienbruchfreie Infrastruktur, um Material-, Informations- und Geldflüsse innerhalb einer Organisation zu bündeln und zwischen Organisationen zu sichern. Dabei ist egal, ob Menschen oder Maschinen interagieren. Das wird erheblich verändern, wie Wertschöpfung erzielt und übertragen wird – wohl nicht innerhalb der nächsten zwei, aber sicher innerhalb der nächsten fünf bis zehn Jahre. Es geht dabei um die Erhöhung der Transaktionssicherheit bei gleichzeitiger Senkung der Transaktionskosten. Diese Kombination kann durch Blockchain-Technologie gelingen.

Vorteile (Interoperabilität, Prozessautomatisierung und IT-Sicherheit)
Die Supply Chain heute hat viele sichere Inseln innerhalb von Organisationen geschaffen, wird aber geplagt von den zahlreichen Piraten, die genau an den Übergabepunkten zwischen Organisationen angreifen. Die Übergabepunkte zwischen Organisationen sind dabei häufig einerseits mit besonders hohen Transaktionskosten und andererseits mit erhöhtem Betrugsrisiko verbunden. Dies gilt auch in anderen Branchen wie etwa Versicherungen, die zum Beispiel bei Schadensfällen mitunter viele Dienstleister mit hohem manuellen Aufwand koordinieren müssen.

Interoperabilität: Blockchains können Interoperabilität durch verteilte Datenspeicherung mit geteiltem Schreibzugriff erreichen, ohne aufwändige Konfiguration von Firewall- oder VPN. So gibt es auch niemanden mehr, der die Datenhoheit hat, sondern alle Teilnehmer der Blockchain können den Datensatz zunächst anhand der festgelegten Regeln verifizieren und erst dann akzeptieren.

Prozessautomatisierung: Blockchains erlauben auch die Prozessautomatisierung zwischen Parteien, die sich wiederum nicht unbedingt vertrauen, weil Blockchains keine zentrale Vertrauensinstanz benötigen. Das ermöglicht überhaupt erst, Prozesse zwischen Unternehmen zu automatisieren, indem vereinbarte Vorgänge gemäß vorab definierter Akzeptanzkriterien vollautomatisch durch Smart Contracts ausgeführt werden. Transparenz und Nachvollziehbarkeit führen häufig zudem auch insgesamt zu erhöhter Prozessdisziplin.

IT-Sicherheit: In vielen Unternehmen ist ein wichtiges Ziel, die Kosten für IT-Bestandssysteme zu senken, die Interoperabilität zu erhöhen und die Sicherheit zu verbessern. Hierfür können Blockchains eine Lösung sein, denn Blockchains sind erheblich resilienter gegenüber Cyberangriffen als zentralisierte IT-Infrastrukturen. Überaus schmerzhaft musste dies der Logistikriese Maersk erfahren, der mit einem

Schaden in Höhe von 200-300 Millionen US-Dollar (Golem 2017) aufgrund der Angriffe durch den Trojaner Not-Petya rechnet. Blockchains schützen etwa vor den meisten typischen Angriffen auf Webanwendungen (vgl. OWASP 2013).

Anwendungsfälle für Blockchain in der Supply Chain
Die Anwendungsfälle im Bereich Supply Chain sind nicht unbedingt absolut trennscharf, denn es ist sinnvoll, etwa die ersten drei Beispiele Dokumentenflüsse, Track and Trace und Fälschungsschutz miteinander zu verbinden. Dennoch sollten diese Anwendungsfälle zunächst getrennt voneinander betrachtet und möglicherweise auch erst nacheinander umgesetzt werden.

Anwendungsfall 1: Schiffslogistik und Digitalisierung des Dokumentenflusses
Maersk ist mit seinem Gemeinschaftsprojekt mit IBM wohl der Marktteilnehmer mit der höchsten Sichtbarkeit für sein Blockchain-Projekt im Bereich Supply Chain. Es gibt aber dutzende weitere Projekte in diesem Feld. Im besagten Projekt geht es darum, den Dokumentenfluss für Schiffslogistik auf einer Blockchain zu handhaben und Geschäftsprozesse über Smart Contracts abzubilden. Indem dieser Dokumentenfluss auf eine Blockchain gebracht wird, sollen erheblich Zeit- und Effizienzgewinne erzielt werden. Beim Transport von Blumen von Kenia nach Rotterdam zählte Maersk beispielsweise 200 Kommunikationsprozesse, die für diesen Transport notwendig waren. Durch verteilten Lese- und Schreibzugriff inklusive der Möglichkeit der Freigabe von Dokumenten soll dieser Overhead für Dokumentation massiv reduziert werden.

Anwendungsfall 2: Digitale Nachverfolgung von Gütern (Track and Trace)
Im zweiten Anwendungsfall geht es nicht nur darum, den Dokumentenfluss auf einer gemeinsamen Plattform zu handhaben, sondern konkret jedes Produkt auf seinem Weg durch die Supply Chain nachzuverfolgen. Dies kann mehrere Gründe haben: Man will frühzeitig von Lieferverzögerungen erfahren, man will es Fälschern schwerer machen, Produktfälschungen einzuspielen oder man will die Bedingungen während des Transports genauer kontrollieren. Insbesondere für die Überwachung von Transportbedingungen bieten sich Smart Contracts an: So kann etwa vereinbart werden, dass empfindliche Medikamente während des Transports nur einem bestimmten Temperaturbereich ausgesetzt sein dürfen. Diese Temperatur wird während des Transports gemessen und auf einer Blockchain hinterlegt. Bleibt die Temperatur im vereinbarten Bereich, wird die Bezahlung über einen Smart Contract ausgelöst.

Anwendungsfall 3: Fälschungsschutz für Diamanten oder Krebsmedikamente
Die Blockchain ermöglicht durch einen digitalen "Proof of existence" den Nachweis, dass ein bestimmter Datensatz zu einem bestimmten Zeitpunkt existiert hat. Das ist aber nicht gleichzusetzen mit einem tatsächlichen Herkunftsnachweis eines physischen Objekts, das digital beschrieben wird. Denn dafür ist es nötig, eine unfälschbare Verbindung zwischen physischem Objekt und seiner digitalen Beschreibung herzustellen. Diamanten sind von ihrer physikalischen Beschaffenheit her einmalig und dabei quasi unveränderbar und unkopierbar. Deshalb genügt die digitale Beschreibung dieser einmaligen Eigenschaften, um die digitale Beschreibung und das

Objekt miteinander zu verbinden. Das gilt aber für die wenigsten Güter. Daher kann man alternativ chemische Marker wie fälschungssichere Spezialtinten verwenden, die auch bei Geldscheinen oder Reisepässen zum Einsatz kommen oder RFID-Chips. So werden Herkunftsnachweise und damit Fälschungsschutz möglich. Dieser Ansatz ist auch interessant im Bereich Ersatzteilehandel, vor allem bei hochwertigen Ersatzteilen in den Bereichen Automobilbau oder Luft- und Raumfahrt, wo man von bis zu zehn Prozent gefälschten Ersatzteilen ausgeht. Ein besonderer Punkt kann hier das Recall-Management für Automobilhersteller sein, um nachvollziehen zu können, welche Komponente genau wo verbaut wurde, wenn Fälschungsschutz mit Track and Trace verbunden wird.

Anwendungsfall 4: 3D-Druck
Das Beispiel 3D-Druck veranschaulicht sehr gut, wie Blockchain Material-, Informations- und Wertefluss zusammenbringen kann. Im 3D-Druck ist die Supply Chain fast komplett digitalisiert und fast der gesamte Wert des Produkts ist in den Konstruktionsplänen gebündelt. Ein Druck kann so zum Beispiel via "Pay per Use" über einen Smart Contract ausgelöst werden. Gleichzeitig besteht Interesse am Fälschungsschutz der Ausgangsmaterialien, da mit dem Konstruktionsplan problemlos gleich aussehende Stoffe mit minderwertigen Materialien erzeugt werden könnten. Hier wird offensichtlich, warum es nicht länger genügt, allein die physische Lieferkette abzusichern. Der sichere Fluss von Material, Informationen und Werten wird immer essenzieller in einer Wirtschaft, die zunehmend auf Kopfarbeit beruht.

Anwendungsfall 5: Transportversicherungen
Ein weiteres Anwendungsgebiet sind Banken- und Versicherungsdienstleistungen rund um die Logistik. Möglich sind etwa ein sogenannter Letter of credit (LoC) oder Transportversicherungen, die an Track and Trace gekoppelt werden. Vergleichbar mit der Temperaturüberwachung könnten auch Leasing-Verträge mit Smart Contracts implementiert werden, bei denen Mietbedingungen an die Einhaltung gewisser Rahmenbedingungen geknüpft sind.

Technische Herausforderungen
Herausforderungen für Anwendungen im Bereich Internet-of-Things (IoT) gelten insbesondere auch für Blockchain in der Supply Chain, was im Kern eine IoT-Anwendung ist. Die Verbindung zwischen digitaler Identität und physischem Objekt muss zuverlässig hergestellt werden. Die einfachste Lösung hierfür ist ein QR-Code, der aber sehr leicht kopiert werden kann. Alternativen sind RFID-Chips, Hologramme oder Spezialtinten. Die Blockchain ist zudem eine sehr junge Technologie. Darüber hinaus muss man sich bei Blockchain-Lösungen im konkreten Anwendungsfall entlang der Achsen *public vs. private* und *permissionless vs. permissioned* orientieren (siehe hierzu die TeleTrusT-Publikation zu Blockchain, vgl. TeleTrusT 2017) und die jeweiligen Trade-Offs gegeneinander abwägen. Den Daten-Payload wird man häufig z.B. off-chain vorhalten wollen, um die Datenintegrität durch Blockchains zu schützen, nicht aber den Inhalt selbst öffentlich einsehbar zu machen. Da Blockchains kryptographische Protokolle sind, benötigt man außerdem Lösungen zur Schlüsselverwaltung.

Ausblick

So wie man sagen kann "Das Internet überträgt Daten", gilt hier "Die Blockchain überträgt Werte", was sie für die Supply Chain besonders interessant macht. Auch vor dem Internet konnte man Daten übertragen, z.B. via IPX, Diskettenlaufwerke oder den Postbrief. All das wurde jedoch bei der Datenübertragung vom Internet in den Schatten gestellt. Als Analogie für den Reifegrad der Blockchain-Technologie mag ebenfalls das Internet dienen. Die ersten breitentauglichen Browser kamen Mitte der 90er Jahre auf den Markt. Google wurde 1998 gegründet, ist mit rund 500 Milliarden USD Börsenwert mittlerweile das wertvollste Internet-Unternehmen der Welt und das zweitwertvollste insgesamt (genaugenommen gilt dies für die Holding-Gesellschaft Alphabet Inc., der Google mittlerweile gehört) und stellt mit Chrome auch den populärsten Browser.

Im Moment kommt die Blockchain so langsam in die Phase der breitentauglichen Wallets als "Blockchain-Browser". Gleichzeitig profitiert sie davon, dass sie als weiterer Layer basierend auf dem Internet ausgerollt werden kann, diese Infrastruktur also nicht erst selbst zu schaffen braucht. Ein Zitat von Bill Gates besagt, dass meist überschätzt wird, wie viel sich in den nächsten zwei Jahren verändern wird, aber deutlich unterschätzt wird, wie viel sich in den nächsten zehn Jahren verändern wird (vgl. Nancy Weil and IDG NEW. S SERVICE 2018). Dies könnte sich bei der Blockchain erneut bewahrheiten. Die Supply Chain gehört voraussichtlich zu den geeignetsten Einsatzgebieten, denn dort bietet die Blockchain eine Art Prozess-Werkbank für die sichere Digitalisierung und Automatisierung von Prozessen zwischen Unternehmen anstatt nur innerhalb von Unternehmen. So können unternehmensinterne Datensilos in sichere Datenschnittstellen verwandelt werden, um die Transaktionskosten zu senken und die Transaktionssicherheit zu erhöhen.

Literaturverzeichnis

Golem (2017): Not-Petya-Angriff kostet Maersk 200 Millionen US-Dollar; Internet: https://www.golem.de/news/ransomware-not-petya-angriff-kostet-maersk-200-millionen-us-dollar-1708-129525.html (Aufgerufen 28.09.2017)

OWASP (2013): OWASP Top 10 – 2013, The Ten Most Critical Web Application Security Risks; Internet: https://www.owasp.org/images/f/f8/OWASP_Top_10_-_2013.pdf (Aufgerufen 28.09.2017)

TeleTrusT (2017): TeleTrusT-Positionspapier "Blockchain", Handreichung zum Umgang mit der Blockchain; Internet: https://www.teletrust.de/fileadmin/docs/publikationen/broschueren/Blockchain/2017_TeleTrusT-Positionspapier_Blockchain__.pdf (Aufgerufen 28.09.2017)

Nancy Weil and IDG NEW. S SERVICE (2008): The Quotable Bill Gates, in: abcNews; Internethttp://abcnews.go.com/Technology/PCWorld/story?id=5214635 (Aufgerufen 28.09.2017)

9 "*Identity und Access*"

Dr. André Kudra, Vorstand (CIO), esatus AG,
Leiter der TeleTrusT-AG "Blockchain"

Digitale Identität im Umbruch

So stark im Wandel wie das Internet selbst ist auch das Konzept der digitalen Identität. Vom Management zahlreicher Einzel-Accounts mitsamt dazugehörigen Passwörtern bis hin zu Bündelung von Diensten – und damit auch Nutzerdaten – in den Händen weniger Anbieter: Eine zufriedenstellende Lösung der Problematik wird immer greifbarer. Mit der zunehmenden Sensibilisierung für das Thema Blockchain und Distributed Ledger Technology gewinnt auch der Begriff der *self-sovereign identity* zunehmend an Gewicht. Dies ist kein Zufall, sieht man doch diese Technologie als das Mittel der Wahl zur deren Umsetzung. Die dezentrale, verteilte Natur der Blockchain und das starke kryptografische Fundament ermöglichen einen vollkommen neuen Identitätsstandard.

In dessen Mittelpunkt steht der Nutzer, der selbst die Kontrolle über seine Daten und die Zugriffsrechte darauf besitzt. Die Etablierung einer solchen digitalen Blockchain-Identität bei Online-Diensten, Unternehmen und öffentlichen Institutionen würde den Nutzern ein echtes "Bring Your Own Identity" (BYOI) ermöglichen und bisherige Modelle überflüssig machen. Auch bevorstehenden Änderungen des rechtlichen Rahmens im Zuge der EU-Datenschutz-Grundverordnung kann mit einem solchen konzeptionellen Neuanfang womöglich besonders gut entsprochen werden.

Die Angleichung der technischen Möglichkeiten im Bereich Blockchain an die Erfordernisse professioneller Identity-and-Access-Lösungen ist gut zu beobachten.

I&A-Projekte

Umsetzungen einer digitalen Identität auf Basis von Blockchain-Technologie bestehen bereits, haben aber zum derzeitigen Stand noch eine geringe Verbreitung. Das Projekt Blockstack (https://blockstack.org) verfolgt eine Bindung digitaler Daten an Public Keys einer Public Permissionless Blockchain (austauschbar, aktuell Bitcoin Blockchain). Diese zugrundeliegende Blockchain dient als Taktgeber einer virtuellen Blockchain mit größerer Speicherkapazität, die ihrerseits Verweise auf Zonefiles in einem Routing Layer liefert, wo wiederum auf Daten in einem Storage Layer verwiesen wird. Vorrangiges Ziel dieses mehrschichtigen Aufbaus ist die Schaffung eines dezentralen DNS und damit eines manipulations- und zensurresistenten Internets, jedoch sind auch digitale Identitäten ein fester Bestandteil der Agenda.

Das von Consensys entwickelte uPort (www.uport.me) verwirklicht digitale Identitäten mithilfe von Smart Contracts in der (Public Permissionless) Ethereum Blockchain. Während ein sehr kurz gehaltener Proxy Contract das einzig unveränderliche Identifikationsmerkmal in der Blockchain darstellt, dient ein vorgeschalteter Controller Contract, der unter anderem die Austauschbarkeit von Private Keys ermöglicht, als Schnittstelle zum User. Ein Registry Contract bindet Hashverweise auf außerhalb der Blockchain ("off chain") gespeicherte Identitätsdaten an den Proxy Contract. Anderen

Ethereum-App-Entwicklern steht es frei, diese uPort-Identitäten in ihren Produkten zu verwenden.

Sovrin (Public Permissioned), ein Projekt der gemeinnützigen Stiftung selben Namens (https://sovrin.org), begegnet dem Identitätsproblem mit einem von ausgewählten Organisationen betriebenen Distributed Ledger. Diese ausgewählten "Stewards" verpflichten sich vertraglich zu ordnungsgemäßem Betrieb ihres Nodes. Auf Basis dieses gegenseitigen Vertrauens wird auf Konsensfindung mittels schnellen RBFT-Algorithmen (Redundant Byzantine Fault Tolerance) statt auf den ressourcenintensiven Proof of Work gesetzt. Verarbeitung der Transaktionen und die öffentliche Bereitstellung des Lesezugriffs auf den Ledger sind auf die Steward-Rollen der Observer und Validators verteilt, wobei die Observer zugleich die Arbeit des Validators kontrolliert und bei Bedarf für diesen einspringen kann.

Prototyping

Mit der Umsetzung eines eigenentwickelten I&A-Prototypen auf Basis von Ethereum offenbaren sich aktuelle Möglichkeiten, als auch technische Schwierigkeiten dieses Ansatzes. Eine selbstverwaltete digitale Identität kann über die Logik von Smart Contracts verwirklicht werden. Eine solche Blockchain ID, bestehend aus persönlichen Daten und vergebenen Zugriffsberechtigungen, kann mit verschiedenen vordefinierten Instanzen wie Einwohnermeldeamt, Bank oder Lieferdienst wechselwirken und in diesem Rahmen ein "Bring Your Own Identity" verwirklichen. Die Korrektheit der Daten findet in einem Validierungssystem Ausdruck, entsprechend privilegierten Instanzen werden außerdem Änderungsvorschläge an einzelnen Attributen eingeräumt.

Für in Anspruch genommene Rechenleistung auf der Ethereum Blockchain muss je nach Komplexität und Umfang der Operationen aufgekommen werden. Schreibzugriffe und insbesondere die Einbettung von Smart Contracts in die Public Ethereum Blockchain verursachen Kosten, die wegen der momentan fixen Bindung an die Ethereum-eigene Kryptowährung Ether erheblich gestiegen sind. Zwecks Einsparung dieser Kosten und auch einfacherer Anpassung der Blockgröße an umfangreichere Smart Contracts scheint das Ausweichen auf eigene private Ethereum Blockchain sinnvoll.

Oft darf auch aus der weiten Verbreitung der gängigsten Lösungen im Ethereum-Umfeld nicht auf Ausgereiftheit geschlossen werden. So genießt die meistverwendete Programmiersprache Solidity (JavaScript-ähnliche Syntax) mitunter einen zweifelhaften Ruf. Und auch die Node Software geth (https://geth.ethereum.org) verdankt ihre Spitzenstellung ihrer Pionierrolle und nicht der Zuverlässigkeit, wie sie z. B. das weniger bekannte Parity (https://parity.io) bietet. Unvollständige oder wegen des rasanten Entwicklungstempos veraltete Dokumentationen müssen ebenso in Kauf genommen werden.

Ausblick

Den im Vergleich zu Krytowährungen komplexeren Anforderungen einer digitalen Identität muss mit entsprechendem Ideenreichtum begegnet und der anfängliche Ansatz der Public Permissionless Blockchains weitergedacht werden. Doch der immer

häufiger betonte Oberbegriff der Distributed Ledger Theory bezeichnet nicht nur die gedankliche Abgrenzung von der ursprünglichen Blockchain nach Bitcoin-Muster, sondern auch die technische. Längst muss die Verarbeitung von Transaktionen nicht mehr dem starren Blockmuster folgen, Transaktionen müssen keine Stunden mehr auf Bestätigung warten und es ist nicht jederzeit eine Spaltung der Chain im Sinne eines Hard Forks zu befürchten. Die Erschließung weiterer Anwendungsfelder für und mittels Blockchain setzt die Akzeptanz der fortwährenden Evolution ebenjener voraus.

Dieser Erfindergeist ist auch im Bereich Blockchain Identity & Access nötig und erkennbar. Insgesamt ist gerade im Bereich der digitalen Identität eine Verständigung auf einheitliche Standards und die ausreichende Marktdurchdringung von Identitätskonzepten von hoher Bedeutung, will man von den gewohnten Insellösungen wegkommen. Public-Permissioned-Architekturen könnten ein erster Schritt in die gewünschte Richtung sein. Sie kombinieren die Robustheit der Public Permissionless Blockchains mit der Effizienz privater Architekturen. Betreiberkonsortien könnten hier, auch in eigenem Interesse, diese Entwicklung weiter vorantreiben.

Viele bestehende Projekte steuern zielsicher ihrer Erprobung in der Praxis entgegen. Die gemachten Erfahrungen wiederum werden das weitere Vorgehen beeinflussen und die Idee der digitalen Identität weiter formen.

10 "Blockchain-basiertes System für geschäftliche Vereinbarungen"

Dr. Michael Kuperberg, Senior Software Architect, Deutsche Bahn AG
Bertalan Vecsei, External Blockchain Architect, Deutsche Bahn Energie
Sorin Simplaceanu, External Blockchain Business Consultant, Deutsche Bahn AG
Steffen Ortolf, Engagement Management, DB Systel GmbH

Motivation
Bei der Deutschen Bahn AG schließen die einzelnen Konzerntöchter Tausende von geschäftlichen Vereinbarungen, z.B. Werkverträge für Software-Entwicklung. Trotz zunehmender IT-Unterstützung bestehen hier noch zahlreiche Optimierungspotenziale, gerade dort wo noch die klassische "Schriftform" eingesetzt wird, um der Nachweispflicht zu genügen. Beim Prozess-Redesign geht es dabei nicht nur um Verschlankung und die Beseitigung von Medienbrüchen, sondern auch um die Usability für die Nutzer und um stärkere Einbindung der Controller.

Für ein konkretes Szenario aus dem Bereich der IT-Beauftragung stellte sich die Aufgabe, eine solche Verbesserung herbeizuführen – ausdrücklich mit dem Wunsch, sowohl fachlich als auch technisch Ansätze miteinzubeziehen – durchaus auch disruptiv. Dabei sollte die Lösung auch so generalisierbar sein, dass daraus ein "Service Procurement Marketplace" weiterentwickelt werden könnte, mit Fokussierung auf B2B-Szenarien.

Die konkreten fachlichen Anforderungen umfassten dabei auch die "append only"-Semantik der einzelnen Schritte: es soll stets möglich sein, alle in der IT ausgeführten Schritte vollständig nachzuvollziehen und exakt genauso auch zu wiederholen.

Fachliche und technische Analyse
Geschäftliche Vereinbarungen spielen im Alltag eine zentrale Rolle: auf Basis eines Bedarfes wird ein Angebot ausgehandelt und abgeschlossen. Anschließend wird die Leistung erbracht und verrechnet – dazu kommen oft genug auch Anpassungen des Umfanges, des zeitlichen Rahmens und der Kosten.

Bei vielen Geschäftsbeziehungen ist es üblich, dass sich die beiden Parteien nicht allzu sehr vertrauen, und daher einen vertrauenswürdigen Intermediär einschalten, z.B. einen Notar. Die Vereinbarungen werden dann notariell beurkundet (z.B. bei einem Hauskauf) und der Notar kann gerade in strittigen Fällen (Verzug, Minderleistung, …) eine Vermittlerrolle spielen. Zum Beispiel wird ein Notaranderkonto eingesetzt, auf welches der Kunde einen Teilbetrag einzahlt; dieser Betrag wird erst dann vom Notar an den Dienstleister weitergereicht, wenn der Kunde die Fertigstellung des entsprechenden Leistungsteils bestätigt – und andererseits weiß der Dienstleister, dass der Kunde den Teilbetrag nicht willkürlich zurückbehält.

Der Einsatz eines solchen vertrauenswürdigen Intermediärs ist mit Kosten und zusätzlichem Aufwand verbunden. Außerdem wird im echten Leben der Notar oft vom Dienstleister ausgesucht, was seine Unparteilichkeit in Frage stellt.

Ein Versprechen des Blockchain-Konzeptes besteht ja darin, dass die Blockchain solche Intermediäre ersetzen/ergänzen kann. Dabei wird argumentiert, dass eine öffentliche Blockchain ein eignerloses, kryptografisches Peer-to-Peer-Netzwerk ist, welches nur schwer zu kompromittieren ist. Aber selbst mit einer nichtöffentlichen Blockchain (z.B. mit einer Konsortial-Blockchain) ist es möglich, ein höheres Vertrauen zwischen Parteien zu erreichen, die sich tendenziell misstrauen: dazu bekommt jede Partei einen Blockchain-Knoten und somit kann ein Smart Contract auf einem beliebigen Node zur Ausführung kommen. Eine angemessene Anzahl an Nodes vorausgesetzt, wäre eine "Verschwörung" einer Mehrheit an Nodes notwendig, um eine rechtmäßige Transaktion (etwa die Ausführung eines Smart Contracts) zu verhindern.

Ein weiterer Blockchain-Vorteil beim Einsatz für geschäftliche Vereinbarungen ist die "Write-once-read-many"-Eigenschaft: nachträgliche Änderungen in bereits geschriebenen Blöcken können zweifelsfrei detektiert und von Blockchain-Nodes zurückgewiesen werden. Damit adressiert man die Auditierfähigkeit der IT-gestützten Prozessverarbeitung und die Aufbewahrungsfristen.

Des Weiteren gab es die Anforderung nach Datenschutz und Mandantenfähigkeit – gleichzeitig sollte jeder berechtigte Teilnehmer sich einen Abzug "seiner" Daten ziehen können. Zusätzlich sollte die Umsetzung hochredundant und damit auch repliziert/verteilt sein.

Wir haben uns daher entschlossen, die Blockchain-Lösung von Hyperledger Fabric als ersten Kandidaten einer Verprobung zu unterziehen, nachdem die "Make-buy-reuse"-Prüfung ergab, dass wir kein anderes WORM-System als Alternative zu einer Blockchain kaufen oder nachbauen wollten. Konkret ausschlaggebend für Hyperledger Fabric war für uns die native Unterstützung von privaten Channels, die Verfügbarkeit des Quellcodes und die IBM-Unterstützung des Projektes, sowie die Aussicht auf eine weitere Verbreitung in der Industrie. Außerdem gab es auf Seiten des Auftraggebers großes Interesse, die noch verhältnismäßig junge Blockchain-Technologie auf Reife, Performance und Entwicklungskosten "abzuklopfen".

Vorgehen

Zunächst haben wir ein "Minimum Viable Product" definiert und zwei konzerninterne Fachbereiche als Early Adopters gewinnen können, um mit einer niedrigen zweistelligen Anzahl von Fachanwendern zu starten. Wir haben die Anbindung an produktive Bezahlsysteme zunächst ebenso ausgeklammert wie die "assetization", also die Repräsentation von Fiat-Geld durch Kryptowährungen.

Um Endanwender für das neue System zu begeistern, muss das Frontend sowohl in Bezug auf Usability als auch auf optische Gefälligkeit optimiert sein: es reicht nicht, im Backend (unsichtbar für die Endanwender) eine neue Technologie einzuführen. Deshalb ist das neue System von vorneherein gleichermaßen auf mobile Geräte wie auf klassisches Bürorechner ausgerichtet.

Auch mit dem Thema Betriebsführbarkeit muss man sich bei der Blockchain-Technologie sorgfältig beschäftigen: denn bei herkömmlichen Konzepten wächst die Kette

solange, wie neue Datenblöcke angefügt werden und der Genesis-Block zur Konsistenz vorgehalten werden muss. Auf diese Art und Weise landen z.B. bei der Bitcoin-Blockchain mehr als 100GB auf dem Datenträger eines Nodes – und im geschäftlichen Umfeld sind bei Verträgen Vorhaltezeiten von 10 Jahren nicht unüblich. Daher beschäftigen wir uns nicht nur mit der Umsetzung eines Rollover-Konzeptes, sondern auch mit Skalierbarkeit der Lösung auf Basis einer mandantenbezogenen Segmentierung.

Erfahrungen und Zusammenfassung
Während unserer Entwicklung zeigte sich, dass Hyperledger Fabric stark von Veränderungen geprägt war. So wurden signifikante Features ohne Ankündigung entfernt (z.B. die Java-Unterstützung in Version 1.0.0), allerdings verbessert sich mit Release 1.1.0 diese Situation. Gleichwohl waren intensive Kontakte zu Entwicklern notwendig, um eine Korrektur von Bugs in Gang zu setzen – bei Open-Source-Software wie Fabric gibt es ja keinen "Wartungsvertrag".

Hyperledger Fabric setzt auf moderne Technologien wie Docker auf, und überdies haben wir den MEAN-Stack (MongoDB, Express.js, Angular.js und Node.js) eingesetzt, sowie die Frameworks für (hybride) App-Entwicklung. Damit ergab sich natürlich eine gewisse Komplexität, die sich aber als beherrschbar herausgestellt hat.

Im Sinne eines "Learning by doing" beschäftigen wir uns natürlich auch mit den essentiellen Blockchain-Qualitätsaspekten wie Skalierbarkeit, Datenmigration, Stabilität, Auswirkung der gewählten Consensus-Algorithmen, Penetration-Tests und Transaktionalität. Wir erwarten aber nicht nur Fortschritte bei den einzelnen Produkten, sondern eine Entwicklung des Blockchain-Ansatzes hin zu "commodity", also zu "Blockchain as a Service"; die ersten Ansätze dazu sind z.B. auch schon bei namhaften Cloud-Anbietern zu beobachten. Außerdem erwarten wir eine wachsende Testbarkeit von Hyperledger-basierten Anwendungen und Verbesserungen beim Aufsetzen von Ausführungsumgebungen.

Danksagungen
Die Autoren bedanken sich bei allen Unterstützern innerhalb von DB Energie GmbH und DB Systel GmbH für konstruktive Projektmitarbeit und für die offene Zusammenarbeit bei den Blockchain-Themen.

TeleTrusT - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.