

BLOCKCHAIN

Technologien, Forschungsfragen und Anwendungen

Editoren: W. Prinz (FIT), A. Schulte (IML)

Autoren: J. Schütte (AISEC), G. Fridgen, W. Prinz, T. Rose, N. Urbach (FIT), T. Hoeren, N. Guggenberger (FIT, Univ. Münster), C. Welzel (FOKUS), S. Holly (IDMT), A. Schulte, P. Sprenger, C. Schwede (IML), B. Weimert (INT), B. Otto (ISST), M. Dalheimer (ITWM), M. Harz (MEVIS), M. Kreutzer (SIT)

Version 1.0, 20. März 2017

Abstrakt

In dem vorliegenden Positionspapier der Fraunhofer-Gesellschaft erfolgt – basierend auf den wesentlichen Grundlagen und Eigenschaften – eine Einordnung der Blockchain-Technologie in die Forschungslandschaft sowie eine Identifikation der noch offenen Forschungsfragen. Das vielfältige Potential dieser neuen Technologie wird illustriert durch eine Darstellung der bereits existierenden aber auch denkbaren zukünftigen Anwendungsmöglichkeiten. Abschließend wird aufgezeigt welchen Beitrag die Fraunhofer-Gesellschaft, auf Basis ihrer spezifischen Kompetenzen, bei der weiteren Entwicklung und Implementierung der Technologie leisten kann.

Inhalt

1	Einführung	4
1.1	Motivation	4
1.2	Blockchain-Grundlagen	6
2	Einordnung in die Forschungslandschaft	8
2.1	Kryptographie	8
2.2	Konsistenz und Skalierung verteilter Systeme	9
2.3	P2P Netzwerke	11
2.4	Konsensbildung und Validierung	11
2.5	Smart Contracts	13
2.6	Vertrauenswürdigkeit und Sicherheit von Smart Contracts	14
2.7	Geschäftsmodelle.....	15
3	Anwendungsfelder	16
3.1	Internet der Dinge	17
3.2	Smart Grid	18
3.3	Herkunftsnachweise.....	18
3.4	Supply Chain Management und Einkauf	19
3.5	Medizintechnik	20
3.6	Finanzbranche.....	21
3.7	Medienindustrie	23
3.8	Öffentlicher Sektor	24
3.9	Juristischer Sektor	26
3.10	Darknet.....	28
3.11	Kriterien für einen Blockchain-Einsatz.....	29
4	Beitrag und Kompetenzen der Fraunhofer-Gesellschaft	30
4.1	Blockchain Lab - Konzeption, Entwicklung und Evaluation	30
4.2	Blockchain Security Lab - Sicherheit.....	31
4.3	Cybersicherheitsberatung.....	32
4.4	Forensikberatung	34
4.5	Wirtschaftlichkeit	34
4.6	Industrial Data Space IDS	36
5	Zusammenfassung	37
6	Literatur	38

1 Einführung

1.1 Motivation

Seitdem Satoshi Nakamoto 2008 sein White Paper [14] veröffentlichte und Anfang 2009 die ersten Bitcoins geschöpft wurden, haben sowohl Kryptowährungen als auch die ihr zugrundeliegende Basistechnologie der Blockchain große Aufmerksamkeit erfahren. Die Entwicklung der Blockchain-Anwendungen wird dazu oft in drei Phasen unterteilt: Blockchain 1.0 umfasst die Kryptowährungen, Blockchain 2.0 im Wesentlichen Smart Contracts im Finanzsektor und in der Blockchain 3.0 werden Smart Contracts zu dezentralen autonomen Organisationseinheiten weiterentwickelt, mit eigenen Gesetzmäßigkeiten und einem hohen Autonomiegrad und das in nahezu allen Lebensbereichen. Aktuell erschließen sich entsprechend in einem rasanten Tempo zahlreiche neue Anwendungsfelder und Umsetzungsmöglichkeiten im Umfeld der Blockchain-Technologie, die weit über eine virtuelle Währung hinausgehen.

Grundlage für dieses Interesse sind die folgenden Eigenschaften und Potenziale des Blockchain-Konzepts:

- Die Technik der **verteilten Konsensbildung** kann in Geschäftsprozessen die Rolle eines vertrauenswürdigen Dritten in den Bereichen Prozessdurchführung und Authentifizierung ersetzen. Dies betrifft sowohl Intermediäre als auch Aufsicht. Somit werden Geschäftsmodelle vieler Organisationen und Institutionen in Frage gestellt, welche heute diese Rolle ausüben. Es ergeben sich allerdings auch neue Geschäftsmodelle, die ohne die Blockchain-Technologie nicht wirtschaftlich abbildbar gewesen wären. Das Vertrauen in einen Dritten wird abgelöst durch Vertrauen in ein Kollektiv, eine Technologie und die Kryptographie.
- In der Blockchain können **Werte** abgebildet werden, deren Zugriffsrechte eindeutig und dauerhaft von einem Nutzer an einen anderen transferiert werden können. Daher wird die Blockchain als Grundlage des **Internet-of-Value** und als Ergänzung des bisherigen Internet-of-Information gesehen. Kryptowährungen sind dabei nur die naheliegendste Anwendung. Auch Rechte an **realweltlichen Werten** können digital in der Blockchain abgebildet und so gehandelt werden. Damit erweitert sie das Internet von einer Plattform des Kopierens und Teilens in eine Plattform, die Herkunft und Besitz von Werten protokolliert und transparent nachvollziehbar macht.
- Auch wenn es sich dabei nicht um Verträge im rechtlichen Sinne handelt, ermöglicht das Konzept der **Smart Contracts** durch Regeln und Ausführungsanweisungen vorgegebene Prozesse auf der Blockchain automatisiert und dezentral auszuführen. Damit eröffnet sich ein enormes **Automatisierungspotenzial**. Das Anwendungsspektrum erstreckt sich von der Logistik über den Handel bis hin zum Internet der Dinge (IoT), mit dem beispielsweise intelligente Gegenstände ihre Nutzung selbstständig verhandeln und abrechnen können.
- Grundsätzlich sind die in einer Blockchain repräsentierten Transaktionen allen Teilnehmern im Netzwerk sichtbar und damit **nachvollziehbar**. Zudem garantiert die Blockchain **Irreversibilität**, d.h. Transaktionen in der Blockchain können nachträglich nicht manipuliert oder gar gelöscht werden. Um eine Transaktion rückgängig zu machen, kann lediglich – wieder im Konsens – die entsprechende Gegentransaktion in der Blockchain hinterlegt werden. Im Kern werden dadurch

Herkunftsnachweise und Transaktionen für abgebildete Werte revisionssicher. Dies eröffnet vielfältige Möglichkeiten im Bereich der Compliance bis hin zu automatisierten Prüfung bisher manuell durchgeführter Prozesse, wodurch die Geschäftsmodelle von Wirtschaftsprüfern hinterfragt werden. Ist keine vollständige Transparenz erwünscht, existiert zum einen die Möglichkeit privater Blockchains, zu denen nur ein eingeschränkter Nutzerkreis Zugang hat. Zum anderen gibt es mittlerweile Mittel und Wege auch in öffentlichen Blockchains die Nachvollziehbarkeit einzuschränken – mit allen Vor- und Nachteilen (beispielsweise im Darknet).

In den vergangenen Jahren führten diese Eigenschaften zu einer explosionsartigen Entwicklung immer neuer Anwendungsfälle und zu einer unüberschaubaren Anzahl an Akteuren. Diese reichen von diversen StartUps über Technologie-Unternehmen z.B. IBM, SAP sowie auf unterschiedlichen Ebenen neu gebildeten Konsortien, z.B. Hyperledger, Project. Aber auch Individuen, Regierungen, NGOs, Universitäten, Forschungsorganisationen und Wagniskapitalgeber forschen und entwickeln an der nächsten „Killer-App“, die für die Blockchain wird, was der Browser für das Internet war [15].

Dieser Hype kann nicht darüber hinwegtäuschen, dass es derzeit sehr viel mehr Visionen, Theorien und Konzepte als real existierende, funktionierende Beispiele gibt. Denn die noch junge und gleichzeitig komplexe Technik bringt facettenreiche Herausforderungen sowohl im Bereich der IuK-Grundlagen als auch im Bereich der Anwendungen und auch der Angriffsszenarien mit sich. Es fehlt der Technologie aktuell noch an Infrastrukturen für den jeweiligen Einsatz, an adäquaten Kapazitäten, der Skalierbarkeit und kurzen Reaktionszeiten, einem stimmigen Governance-Modell und dem entsprechenden Rechtsrahmen.

Eine Kernherausforderung der Wissenschaft und damit auch der Fraunhofer-Gesellschaft ist vor diesem Hintergrund die kritisch analytische Bewertung dieser Technologie. Die Frage, ob es sich um einen Hype handelt oder die Technologie genügend disruptives Potenzial besitzt, hängt von vielen Faktoren ab, die es systematisch zu untersuchen gilt. Dabei spielen Fragen eine Rolle wie z.B.: Welche Chancen und Risiken sind mit der Technologie (für wen) verbunden? Was sind die Hindernisse und Treiber der Umsetzung? Welche Effekte wird die Technologie auf die Wirtschaft haben und wie können sich Unternehmen - bei aller Ungewissheit - heute am besten vorbereiten? Dazu gehört neben einer Identifikation der technischen Forschungsfragen die Identifikation der Branchen in denen als erstes bzw. die größten Veränderungen zu erwarten sind.

An dieser Schnittstelle von Technologie und Anwendung ist gerade die wissenschaftliche Expertise der Fraunhofer-Gesellschaft gefragt. Institutsübergreifend existiert ein einmaliger Erfahrungsschatz von der Entwicklung bis zur umfassenden Bewertung neuer Technologien - von technischen Details bis hin zur wirtschaftlichen Bewertung. Die Fraunhofer-Gesellschaft bietet sich dadurch als Ansprechpartner für die Wirtschaft an, wenn es darum geht, frühzeitig ausreichendes Know-how aufzubauen, um die Blockchain-Technologie im jeweiligen eigenen Umfeld besser einzuschätzen und fundierte Entscheidungen über zukünftige Investitionen aber auch politische Rahmenbedingungen zu treffen.

In dem vorliegenden Positionspapier der Fraunhofer-Gesellschaft erfolgt – basierend auf den wesentlichen Grundlagen und Eigenschaften – eine systematische Einordnung in die Forschungslandschaft sowie eine gesammelte Darstellung der bereits existierenden aber auch denkbaren zukünftigen Anwendungsmöglichkeiten der Blockchain-Technologie. Des Weiteren wird aufgezeigt welchen Beitrag die Fraunhofer-Gesellschaft, auf Basis

ihrer spezifischen Kompetenzen, bei der weiteren Entwicklung und Implementierung der Technologie leisten kann.

1.2 Blockchain-Grundlagen

Die Eigenschaft der Blockchain, Transaktionen irreversibel zu speichern und die Hoheit einer zertifizierenden Autorität auf eine verteilte Konsensfindung zu delegieren, basiert auf der Kombination unterschiedlicher Techniken in folgendem vereinfacht dargestellten Ablauf [16].

Zunächst wird die Transaktion, wie z.B. die Überweisung einer Kryptowährung oder Registrierung eines Dokuments, von dem Sender erzeugt und digital signiert. Diese Transaktion wird an das Netzwerk gesendet und an die beteiligten Knoten verteilt.

Die Knoten des Netzwerks überprüfen die Gültigkeit der Transaktion und fügen diese in die Blockchain ein. Bei diesem Prozess werden die Transaktionen in Blöcken gespeichert, die durch Hashfunktionen in ein standardisiertes Format überführt werden. Zunächst werden dazu alle einzelnen Aussagen in Hashwerte kodiert und anschließend hierarchisch verdichtet. Diese hierarchische Verdichtung der einzelnen Aussagen wird als Hash- oder Merkle-Baum bezeichnet, mit denen sich ein Block von Aussagen eindeutig repräsentieren lässt. Die Kodierung der Aussagen ist gegenüber Manipulationsversuchen sicher, da die Änderung bereits einer Aussage den Hashwert des Blocks verändern würde, und somit der Hashbaum nicht mehr konsistent wäre.

Blöcke werden durch Verkettung mit der bereits bestehenden Historie der Blöcke verbunden, so dass eine Kette (Block Chain) entsteht. Um einen neuen Block in die bestehende Verkettung als neues Element aufzunehmen, ist bei Bitcoin ein kryptografisches Rätsel zu lösen: welche Zeichenkette liefert einen ähnlichen Hashwert wie die Kodierung des neu aufzunehmenden Blocks. Die Ähnlichkeit beider Werte ist durch die Anzahl der übereinzustimmenden Stellen im Hashwert definiert. Der Schwierigkeitsgrad der Ähnlichkeit ist dadurch variierbar.

Da die Hashfunktion nicht umkehrbar ist, existiert derzeit (noch) kein konstruktives Verfahren für die Ableitung der zu erratenden Zeichenfolge für den gegebenen Hashwert. Es sind somit eine Vielzahl von Zeichenfolgen zu probieren, was entsprechende Rechenkapazitäten erfordert. Wenn ein Knoten, d.h. ein Teilnehmer des Blockchain-Netzwerks, eine entsprechende Zeichenfolge gefunden hat (Mining), wird der neue Block als neues Element in die Kette aufgenommen (Blockchain) und damit zum letzten gültigen Block. Für jeden anderen Knoten im Netzwerk ist die Korrektheit einfach nachzuvollziehen, indem lediglich ein Hashwert zu berechnen ist.

Somit lässt sich eine korrekte Verkettung von Blöcken zu einer Blockchain realisieren. Für die Persistenz werden diese Ketten nun über eine Vielzahl von Knoten verteilt, d.h. alle Knoten haben dasselbe Basiswissen. Entstehen in einzelnen Knoten nun neue Blöcke als Ergänzung der bestehenden Blockchain, so ist im gesamten Netz ein Konsens über die Änderung zu erzielen. Für diese Konsensfindung dient das kryptografische Rätsel. Sobald ein Knoten ein Rätsel gelöst hat, wird die Lösung von allen geprüft und übernommen. Blöcke, die noch auf Konsensfindung warten, sind in einer Nachrückerliste organisiert, in der ebenfalls Blöcke parallel entstandener Verkettungen aufgenommen werden, um sie wieder in die eine globale Blockchain zu integrieren.

Somit lässt sich eine Blockchain mit ihren einzelnen Blöcken in einem Netzwerk von Knoten verwalten. Über die Konsensfindung wird jeweils festgelegt, welcher Block als nächstes Element in die globale Blockchain übernommen wird. Ursprünglich wurde das kryptografische Rätsel für die Erzeugung neuer Blöcke (Mining) genutzt, das als Proof-

of-Work bezeichnet wird. Für unterschiedliche Vertraulichkeits- und Sicherheitsanforderungen kann die Schwere des Rätsels angepasst werden. Ein Dokumentationssystem für die Verteilung von Stromverbräuchen in einem Smart Grid z.B. kann mit einfachen Rätseln arbeiten und somit auch die Rechenleistung der Steuerungsknoten berücksichtigen.

Weitere Arten der Konsensfindung (siehe 2.4) können beispielsweise Anteilsscheine an einem System berücksichtigen. Ein Konsens ist erzielt, wenn die Mehrheit der Anteilsinhaber zum gleichen Ergebnis kommt (Proof-of-Stake). Alternativ können Knoten als Miner für die Konsensfindung ausgezeichnet (Umpires) werden oder es kann eine lotterie-orientierte Auswahl erfolgen. Darüber hinaus gibt es weitere Möglichkeiten und auch Kombinationen aus den genannten Arten der Konsensfindung sind möglich.

Blockchains lassen sich damit vereinfacht als verteilte Datenbanken beschreiben, die durch die Teilnehmer im Netzwerk organisiert werden. Gegenüber zentralen Ansätzen sind Blockchains sehr viel weniger fehleranfällig und beugen insbesondere Byzantinischen Fehlern vor¹. Allerdings bringen diese Systeme auch verschiedene Herausforderungen mit sich. Besonders kritisch wird derzeit die hohe Redundanz der Daten diskutiert. Durch vielfaches Vorhalten der gleichen Daten im Netzwerk wird sehr viel Speicherplatz benötigt. Weiterhin beschränken die Konsensmechanismen häufig die Performance der Blockchain. Der Tatsache zum Trotz, dass die Blockchain-Technologie noch am Anfang ihrer Entwicklung steht, hat sie in der jüngeren Vergangenheit diverse Veränderungen erfahren, die vor allem die Nutzung in einem geschlossenen Unternehmenskontext betreffen. Es besteht ein grundsätzlicher Unterschied - auch aufgrund der unterschiedlichen Zielsetzungen - zwischen öffentlichen (public) und nicht öffentlichen (private) Blockchains.

Public Blockchains sind öffentliche Systeme auf die jeder, der eine Kopie besitzt, zugreifen kann. Das ist nicht gleichbedeutend mit dem automatischen Lesen und Schreiben auf einer Blockchain. Dies erfolgt über sogenannte Fullnodes, die die genehmigungsfreien Anfragen eines Users bearbeiten. Beispiele für öffentliche Systeme sind z. B. Ethereum oder die First Generation Blockchain hinter Bitcoins.

Private bzw. nicht öffentliche Blockchains beschreiben Systeme, die nur für ein abgeschlossenes Konsortium z. B. von Organisationen verfügbar sind. Eng verbunden mit dem Öffentlichkeitscharakter sind die Zugriffsrechte. Während auf public Blockchains grundsätzlich jeder User Zugriffsrechte besitzt und Daten schreiben lassen kann, werden bei private Blockchains Zugriffsrechte i. d. R. administriert bzw. auf ein Konsortium beschränkt (Consortia Blockchain). In den meisten Fällen handelt es sich um genehmigungsbasierte Blockchain-Systeme. Populäre Beispiele für private Blockchains sind das Hyperledger-Projekt mit den OpenSource Lösungen „fabric“, „iroha“, „sawtooth“ sowie das Projekt „MultiChain“.

¹ Unter Byzantinischen Fehlern werden informationstechnische Fehler verstanden, die aufgrund der Weitergabe von falschen bzw. manipulierten Daten in Netzwerken zu falschen Ergebnissen/Systemzuständen führen. So können defekte bzw. manipulierte Netzwerkressourcen falsche bzw. fehlerhafte Daten kommunizieren ohne, dass dies anhand der Struktur bzw. an den Daten selbst erkannt wird. Byzantinische Fehler beschreiben ein potentielles Manipulationsrisiko für Kommunikationsnetzwerke.

2 Einordnung in die Forschungslandschaft

Die Blockchain Technologie basiert auf verschiedenen bekannten aber auch neuen Technologien, die in einem neuen Gesamtsystem kombiniert werden. Dies sind Komponenten aus den Bereichen der verteilten Systeme wie P2P-Netzwerke, Sicherheit und Kryptografie aber auch der Prozessmodellierung. Diese einzelnen Komponenten werden in diesem Kapitel kurz im Hinblick auf ihren Beitrag aber auch noch notwendige Forschungsarbeiten beschrieben.

2.1 Kryptographie

Die Kryptographie ist ein wesentlicher Grundpfeiler von Blockchain-Technologie. Sie ist die Grundlage für das Mining von Blöcken, die Integrität der Blockchain selbst, sowie die Authentizität aller Transaktionen und Teilnehmer. Ohne zuverlässige kryptographische Primitive, wie z.B. Hashfunktionen, sind Blockchains in jedweder Form daher undenkbar. Die an den Maßstäben kryptographischer Forschung gemessen noch junge Blockchain-Technologie stellt die Wissenschaft vor einige Herausforderungen. Zwar verwenden die meisten Blockchains erprobte kryptographische Primitive für das Signieren von Transaktionen und das Erzeugen von Proof-of-Works. Jedoch lässt sich über die zukünftige Sicherheit von kryptographischen Primitiven häufig keine Aussage treffen. Im Laufe der Zeit werden zunehmend effiziente Angriffe auf Kryptographische Algorithmen entwickelt, die einem Angreifer zur Verfügung stehende Rechenleistung steigt kontinuierlich, und zuvor für unrealistisch gehaltene Angriffsszenarien bekommen plötzlich Relevanz, wie etwa Logjam¹ und SHAttered². Hinzu kommt, dass die Sicherheit kryptographischer Systeme bei weitem nicht nur in der Auswahl geeigneter Algorithmen abhängt. Vielmehr zielt ein Großteil der Angriffe auf die Art und Weise ihrer Verwendung und die konkrete Implementierung. Beispiele hierfür gibt es zuhauf, von trivialen Implementierungsfehlern wie Heartbleed³, die auch über Jahre hinweg unerkannt bleiben können, über ausgefeiltere Angriffe, die Abweichungen im Systemverhalten als sog. "Orakel" nutzen, um Informationen über kryptographische Schlüssel zu erhalten, bis hin zu Seitenkanal-Angriffen, die bspw. das Timing-Verhalten von Implementierungen auswerten.

Ein Großteil der heutigen Blockchain-Technologien vernachlässigt diese Angriffsmöglichkeiten und setzt fast ausschließlich auf kryptographische Primitive, die nach heutigem Stand als sicher erachtet werden. Da jedoch gerade Blockchain-Anwendung zum Teil auf äußerst lange Lebensdauern ausgelegt sind - man denke etwa an eine Notarfunktion - ist es essentiell, dass diese Systeme in der Zukunft mit neuen Angriffen und ggf. gebrochenen kryptographischen Primitiven umgehen können. Für sichere Kommunikationsprotokolle setzt man hier in der Regel auf eine Auswahl

¹ Logjam ist ein Angriff der es ermöglicht mittels eines Downgrades auf 512-bit Restklassengruppen während eines Diffie-Hellman-Schlüsselaustauschs den Schlüssel in effizienter Zeit zu brechen.

² SHAttered ist ein Angriff der es ermöglicht in der Praxis SHA1 Kollisionen zwischen zwei unterschiedlichen PDF Dokumenten zu erstellen.

³ Heartbleed ist ein schwerwiegender Programmfehler in älteren Versionen der Open-Source-Bibliothek OpenSSL, durch den über verschlüsselte TLS-Verbindungen private Daten von Clients und Servern ausgelesen werden konnten.

mehrerer kryptographischer Algorithmen, die für jeden Verbindungsaufbau zur Auswahl stehen, so dass unsicher gewordene Algorithmen problemlos ausgetauscht werden können. Für Blockchains existiert eine solche "Krypto-Agilität" bislang nicht. Vielmehr wurde durch aktuelle Forschung gezeigt [6], dass bspw. die Bitcoin-Blockchain nicht gegen mögliche Angriffe auf einige kryptographische Komponenten resistent ist: Sollte es in der Zukunft möglich werden, ECDSA¹-Signaturen zu fälschen, so ließen sich damit Bitcoins entwenden. Sollte es möglich werden, die SHA256²-Hashfunktion zu invertieren, so könnte ein Angreifer u.a. den Proof-of-Work effizient berechnen und die Kontrolle über die Blockchain übernehmen.

Gegenmaßnahmen gegen solche Angriffe - sollten sie irgendwann möglich werden - sind äußerst komplex. Zwar kann das Protokoll unter Verlust der Rückwärtskompatibilität eine neue Hashfunktion einführen, jedoch müssen designbedingt alte Blöcke mit Blockhashes aus der alten, unsicheren Hashfunktion erhalten bleiben. Infolgedessen müssten die neuen Clients somit nun zwei Proof-of-Works lösen statt nur einem.

Die Wissenschaft steht hier also vor mehreren Herausforderungen.

- Erstens, der Entwicklung von kryptographischen Primitiven, die auch gegen zukünftige Angriffe, z.B. durch Quantencomputer, resistent sind.
- Zweitens, dem Entwurf von Blockchain-Protokollen, die Krypto-Agilität unterstützen und auch im Falle von wirksamen kryptographischen Angriffen auf einzelne Primitive noch Sicherheitsgarantien für Transaktionen bieten.
- Drittens, der Entwicklung von Verfahren, mit denen sich kritische Operationen in Blockchain-Protokollen beweisbar korrekt umsetzen lassen, um fatale Implementierungsfehler wie sie zuletzt gehäuft in OpenSSL auftraten zu vermeiden.

2.2 Konsistenz und Skalierung verteilter Systeme

Unter verteilten Systemen fasst man all diejenigen Computersysteme zusammen, die mehrere Computer nutzen, um eine gemeinsame Aufgabe zu erledigen. Ein einfaches Beispiel hierfür ist ein Webbrowser, der über das Internet eine Webseite von einem Server abrufen. Komplexere Systeme sind z.B. die Transaktionssysteme einer Börse oder Flugbuchungssysteme: Hier sind schon aus Lastverteilungsgründen mehrere Rechner notwendig. Gleichzeitig muss jedoch sichergestellt sein, dass eine Überweisung ähnlich einer Datenbanktransaktion exakt einmal ausgeführt wird. Dabei darf es keine Rolle spielen, ob die Systeme zu jedem Zeitpunkt korrekt funktionieren: Ein Softwarefehler oder Hardwaredefekt darf keine Überweisung verändern.

Dieses Problem ist in der Informatik unter dem Stichwort "Byzantinische Generäle" bekannt [10]: Man stelle sich eine Stadt vor, die von mehreren Armeen unter der Führung jeweils eines Generals umzingelt ist. Die Armeen sind nur mit einem gemeinsamen Angriff in der Lage, die Stadt einzunehmen. Um den Angriff zu koordinieren schicken die Generäle Boten mit Nachrichten zu den anderen Armeen.

¹ Elliptic Curve Digital Signature Algorithm (ECDSA)

² SHA (Secure Hash Algorithm) 256 ist eine spezielle kryptographische, d.h. kollisionsresistente Hashfunktion.

In diesem Gedankenexperiment ist es leicht, verschiedene Fehlerzustände aus verteilten Systemen zu rekonstruieren: Was passiert, wenn ein Bote unterwegs abgefangen wird? Was, wenn ein Bote die Nachricht böswillig verändert? Oder zufällig? Ein "byzantine fault tolerant"-System ist eines, das trotz derartiger Fehler stabil bleibt und z.B. die Transaktionseigenschaften garantiert. Die Blockchain ist ein Beispiel eines solchen Systems.

Allerdings erkaufte die hochverteilte P2P-Natur der Blockchain diese Robustheit mit zeitlichen Verzögerungen: Es dauert z.B. in der Bitcoin-Blockchain im Durchschnitt 10 Minuten, um einen Block zu finden – und erst nach sechs Blöcken kann man wirklich sicher sein, dass die eigene Transaktion korrekt in der Blockchain verbucht wurde. Um diesen Nachteil auszugleichen könnte man diesen Aspekt der Blockchain aber auch wieder zentralisieren.

Dazu würde das P2P-Netzwerk gegen eine kleinere Anzahl von Dienstservern ersetzt, die miteinander – wie die Generäle in obiger Analogie – in Kontakt stehen. Diese Server kommunizieren untereinander und bieten eine hinreichend redundante Ausführung der Blockchain. Um sie gegen falsche Nachrichten, Nachrichtenverluste etc. abzusichern können Verfahren wie Raft [11] zum Einsatz kommen. Außerdem vereinfacht diese Teil-Zentralisierung das Einspielen von Updates und Bugfixes enorm.

Für den Unternehmenseinsatz bietet die Blockchain-Technologie viele Potentiale. Allerdings lassen sich Aspekte wie Compliance oder zeitnahe Bugfixes nur schwer in die hochverteilte Struktur der derzeitigen Blockchain-Systeme integrieren. Eine Aufgabe für die Zukunft wird sein, diese Systeme so anzupassen, dass auch die Anforderungen des Unternehmenseinsatzes erfüllt werden können.

Im Hinblick auf die verteilte Datenhaltung beruht das Blockchain-Konzept auf der Speicherung und Replikation aller verwalteten Transaktionen, d.h. des gesamten Datenbestands in allen beteiligten Knoten des P2P Netzwerks. Mit der Lebensdauer einer Blockchain wächst somit kontinuierlich der replizierte Datenbestand, was zu einer kritischen Bewertung der Skalierbarkeit führt. Um das rasante Wachstum der Blockchain zu vermeiden werden daher in der Blockchain keine großen Datenobjekte gespeichert, sondern vorrangig nur die wesentlichen Transaktionsinformationen sowie bei Bedarf Referenzen auf die dazugehörigen Datenobjekte. Diese werden in einer externen Datenbank abgelegt, wenn das Datenobjekt direkt über die Transaktion abrufbar sein soll. Alternativ kann an Stelle einer Referenz auch ein Fingerabdruck des Datenobjekts in Form eines Hash-Werts gespeichert werden. Bei dieser Alternative kann der Hash-Wert gleichzeitig zum Retrieval aus einer externen Datenbank und zur Prüfung der Integrität genutzt werden, in dem der Fingerabdruck des rekonstruierten Objekts mit dem in der Blockchain gespeicherten Fingerabdruck verglichen wird (siehe auch Kapitel 3.3).

Aber auch dieses Verfahren kann bei der Nutzung einer Blockchain für die Verwaltung hochfrequenter Transaktionen, wie sie z.B. im Internet der Dinge bei Sensordaten auftreten können, verhindern, dass die Blockchain kontinuierlich wächst und damit die Anforderungen an die Rechen- und Speicherkapazität der Knoten in dem verteilten System wachsen. Aus diesem Grund sind weitere Forschungsarbeiten erforderlich, um zu vermeiden, dass diese technischen Anforderungen zu einer ungewollten Zentralisierung führen. Ein Lösungsansatz dazu ist die Konsolidierung der Blockchain auf den „Unspent Transaction Output“ (UTXO), d.h. eine Art Saldenbildung wodurch die Größe der Blockchain reduziert werden kann, da Transaktionen die nicht mehr zur Bestimmung des Guthabens eines Nutzers beitragen, gelöscht werden. Ein weiterer Lösungsansatz besteht in der Partitionierung (sharding) der Blockchain, wobei die Knoten nur Teile der Blockchain verwalten, aber dennoch die Integrität der gesamten Kette garantiert bleiben

muss. Trotz dieser ersten Lösungsansätze liefern die Skalierungsherausforderungen hinsichtlich Größe und Transaktionsdurchsatz für die Zukunft interessantes Forschungspotential.

2.3 P2P Netzwerke

In Peer-to-Peer-Netzwerken (P2P) existieren nur gleichberechtigte Rechnerknoten, d.h. im Gegensatz zu Client-Server-Architekturen können alle Teilnehmer am Netzwerk die gleichen Funktionen ausüben. Dies führt dazu, dass P2P-Netzwerke sehr robust gegenüber Ausfällen sind, da ja alle Rechnerknoten alle für die Funktion des Netzwerkes notwendigen Funktionen ausüben können. Weiterhin sind Aspekte der Lastverteilung und Selbstorganisation aufgrund der Struktur eines P2P-Netzwerkes recht einfach lösbar. Dadurch erreichen große P2P-Netzwerke z.B. auf der Basis des BitTorrent-Protokolls und der hohen Anzahl von angeschlossenen Rechenknoten einen sehr hohen Durchsatz [13].

Gleichzeitig führt diese Architektur aber auch zu einer höheren Komplexität. Die grundsätzlichen Herausforderungen von P2P-Netzwerken sind [4]:

1. Absichtliche Manipulation: Knoten im P2P-Netzwerk müssen nicht unbedingt alle das gleiche Ziel verfolgen und können versuchen, die Funktionsweise des Netzwerks bösartig zu ihren Gunsten zu beeinflussen. Wird das Netzwerk z.B. zur Zahlungsabwicklung benutzt, so könnte ein Knoten versuchen, eine Zahlung vorzutäuschen, die es tatsächlich aber nicht gegeben hat. Derartige Falschinformationen müssen von allen anderen Knoten detektiert und abgewiesen werden.
2. Fehlerhafte Informationen z.B. durch Softwarefehler oder Kommunikationsprobleme können ebenso wie absichtliche Manipulationen zu Problemen im Netzwerk führen. Diese müssen – genau wie Manipulationsversuche – detektiert und entsprechend verarbeitet werden.
3. Für viele Anwendungen muss zudem sichergestellt sein, dass eine Transaktion in dem P2P-Netzwerk genau einmal und vollständig durchgeführt wird – also die Eigenschaften einer Datenbanktransaktion besitzt.

Die Blockchain löst diese Probleme, indem es einen Konsens sicherstellt. Im Gegensatz zu hochkomplexen Konsensalgorithmen wie z.B. Paxos [12] sichert die Blockchain durch die Konstruktion der Datenstruktur die Integrität der Informationen innerhalb der Blockchain zu. Diese Konstruktion löst alle oben beschriebenen Herausforderungen.

Nachteilig an einem P2P-Netzwerk ist allerdings, dass die Programmlogik in allen beteiligten Rechnerknoten hinterlegt ist. Wird z.B. ein Fehler gefunden so müssen alle Rechnerknoten ein Update einspielen. Insbesondere bei Ethereum kam es durch einen Protokollfehler zum fehlerhaften Verbuchen von Kontoständen, die nur durch einen Hard Fork und eine nicht abwärtskompatible Softwareversion behoben werden konnten [8].

2.4 Konsensbildung und Validierung

Die Technik der Konsensbildung ist ein weiterer Grundpfeiler der Blockchain. Dabei verwendeten Verfahren beruhen auf Konzepten, die im in Kontext verteilter Netzwerke [3] und verteilter Systeme [10] bereits seit längerem untersucht werden. Das aktuell bekannteste von einer Blockchain-Implementierung verwendete Verfahren ist der Proof-

of-Work der Bitcoin-Blockchain. Das eigentliche Proof-of-Work Konzept wurde schon 1993 zur Eindämmung von Junk-E-mails vorgeschlagen [5]. Es basiert auf einem asymmetrischen Ansatz, bei dem ein Dienstanutzer, d.h. der Email-Absender Arbeit leisten muss, die von einem Dienstanbieter, d.h. dem Email-Netzprovider ohne großen Aufwand überprüft werden kann. Im Blockchain-Kontext sind die Nutzer die Miner, die den Proof-of-Work aufwändig berechnen und die Anbieter alle Knoten, die ohne großen Aufwand prüfen, ob der erfolgreiche Miner den Proof-of-Work ordnungsgemäß berechnet hat. In der Bitcoin-Blockchain basiert der Proof-of-Work Algorithmus auf dem von Adam Back als Hashcash [2] präsentierten Verfahren [14]. Das Ziel des Algorithmus ist es, eine Zahl zu finden (nonce = number used only once), die in Kombination mit dem neuen Block, der an die schon existierende Blockchain angehängt werden soll, einen Hashwert ergibt, der aus einer bestimmten Anzahl von führenden Nullen besteht. Finden mehrere Miner gleichzeitig einen solchen Wert, und hängen diesen an die Blockchain, so führt dies bei der Verteilung dieses neuen Blocks an alle Knoten des P2P-Netzwerks, zu einer Verzweigung der Blockchain. Finden z.B. 3 Knoten nahezu zeitgleich einen passenden nonce, dann würde sich durch das Anhängen der neuen Blöcke die existierende Blockchain in 3 Zweige aufteilen. Um diese Aufteilung wieder zu konsolidieren, gilt die Mehrheitsentscheidung, dass der Zweig ausgewählt wird, der die längste Kette repräsentiert, d.h. die meisten Transaktionen bzw. die meiste Arbeit repräsentiert. Die beiden anderen Blöcke verfallen und die darin enthaltenen Transaktionen, die nicht in dem angehängten Block enthalten sind, werden wieder in den Pool der noch zu validierenden Transaktionen aufgenommen.

Dieses Proof-of-Work Verfahren ist CPU-basiert, d.h. die Rechengeschwindigkeit der Knoten hat maßgeblichen Einfluss darauf, wer das Rätsel löst und einen passenden nonce Wert findet. Da die Miner für das Finden des nonce mit neuen Bitcoins belohnt werden, entsteht ein Wettbewerb, der dazu führt, dass diese in immer mehr Rechenleistung investieren. Damit würde sich die Zeitdauer zum Auffinden eines gültigen nonce zwar reduzieren, was jedoch einer Regel des Bitcoin Netzwerks widerspricht, dass nur ca. alle 10 Minuten ein neuer Block generiert werden sollte. Dies hängt damit zusammen, dass die Belohnung des erfolgreichen Miners mit so genannten neu geschöpften Bitcoins erfolgt. Würden sich die Intervalle, in denen neue Blöcke generiert werden verkürzen, würde sich die Geldmenge zu schnell erhöhen. Aus diesem Grund wird die Schwierigkeit des Rätsels immer dann erhöht, wenn sich die Zeitdauer durch neu hinzugekommene Rechenkapazitäten verkürzt. Dies bedeutet für die Miner, die die Rechenknoten betreiben einen erhöhten Aufwand bei geringeren Erfolgsaussichten. Da der Aufwand neben der Investition in die Rechenleistung i.W. in der verbrauchten Energie besteht, ist dieser Ansatz nicht für alle Blockchain- Anwendungen sinnvoll. Dies gilt vor allem für private Blockchain-Lösungen, bei denen ein solcher Wettbewerb nicht erforderlich ist. Aus diesem Grund wurden alternative Proof-of-Work Verfahren entwickelt, die entweder Speicher-basiert oder Netzwerk-basiert sind. Bei Speicher-basierten Ansätzen kann das Rätsel nicht durch Rechenleistung sondern durch eine entsprechende Anzahl von Speicherzugriffen gelöst werden [1]. Bei dem Netzwerk-basierten Ansatz nur durch die Kommunikation mit anderen Netzknuten, z.B. um von dort Informationen zu sammeln, die zur Lösung des Rätsels erforderlich sind [18].

Ein alternatives Verfahren, das vor allem für private Blockchains relevant ist, ist das Proof-of-Stake Verfahren bei dem Knoten, die einen neuen Block validieren können, nach Ihren Anteilen an der Kryptowährung [9] oder über ein Zufallsverfahren [[19] ausgewählt werden. Eine Kombination von Proof-of-Work mit Proof-of Stake Verfahren ist zusätzlich möglich.

Die Auswahl des am besten geeigneten Verfahrens ist vom konkreten Anwendungsfall und dem Einsatz der Blockchain Lösung, als privat oder öffentlich bzw. genehmigungsfrei oder genehmigungspflichtig, abhängig. Ein weiterer wichtiger Aspekt ist die

Skalierbarkeit bzgl. der Transaktionsanzahl vor allem bei Anwendungen im Bereich des Internets der Dinge. Daraus ergeben sich u.a. folgende Forschungsfragen:

- Welche Proof- Verfahren bieten abhängig vom Einsatzgebiet die beste Lösung bzgl. Sicherheit, Kosten, Skalierung und Performanz?
- Wie sieht eine Kosten/Nutzen-Rechnung bei unterschiedlicher Gewichtung der Anforderungen aus?
- Welche Proof-Verfahren sind zukunftssicher unter Berücksichtigung wachsender Rechenleistung bzw. neuer Technologien?

2.5 Smart Contracts

Eine Blockchain ermöglicht nicht nur eine Dezentralisierung des Transaktionsmanagements, sondern auch die Automatisierung von Prozessen, Regularien und Organisationsprinzipien. Die Transaktionen lassen sich um Regeln für die Konsistenzwahrung ergänzen und werden dann zu so genannten Smart Contracts. Sie spezifizieren, was bei einer Transaktion zu prüfen ist und welche Folgeaktivitäten zu initiieren sind. Häufig genannte Beispiele für Smart Contracts sind z.B. elektronische Türschlösser die automatisch prüfen, ob der Nutzer die Nutzungsgebühr bezahlt hat und noch in Besitz der notwendigen Legitimation wie z.B. eines Führerscheins ist.

Durch Smart Contracts und die damit verbundene Automatisierung lassen sich viele Prozesse im Rahmen eines Re-Engineering radikal verbessern und teilweise auch um zertifizierte Prüfinstanzen erleichtern, wenn die Konsistenz der Information durch einen Smart Contract und die revisionssichere Speicherung gewährleistet ist. Klassische Prinzipien des Re-Engineering Manifesto von Hammer und Champy [7] wie beispielsweise das „capture only once ...“ lassen sich somit auf natürliche Weise mit Blockchain als Enabler umsetzen. Ist Information einmal bestätigt, ist sie revisionssicher dokumentiert und kann in mannigfaltigen Kontexten eingebunden werden. Somit ist die Blockchain aus technologischer Sicht ein natürliches Hilfsmittel für die Prozessoptimierung. Wenn beispielsweise das Einspielen eines Videos in einer Communityplattform nur bei Besitz der entsprechenden Audiorechte möglich ist, können die gesamten Kontroll- und Überwachungsprozesse entfallen. Diese Konsistenz ist aber einfach durch Smart Contracts zu wahren.

Die Technologie der Blockchain hat somit nicht nur vielfältige Auswirkungen auf die Prozesse, sondern auch auf Strukturen der Governance, welche die Aufgabenverteilung zwischen Prozessbeteiligten signifikant ändern kann. Durch die neue Aufgabenverteilung und Änderung der Governance ergibt sich auch die Frage nach neuen Geschäftsmodellen für die neue Value Chain nach Re-Engineering des Prozesses.

Wegen des disruptiven Potentials der Blockchains erscheinen klassische Formen der Prozessoptimierung eher ungeeignet. Ein Revival der klassischen Re-Engineering Methoden erscheint möglich, da sie Prozesse aus strategischer Sicht und als Kundenwert analysiert haben. Auch werden im Re-Engineering Rollenwechsel der Stakeholder berücksichtigt. Da die Prozessmodellierung mit der Entwicklung neuer Strukturen der Governance und Geschäftsmodellierung integriert werden muss, stellen sich Fragen nach:

- Bisherige Modellierungssprachen für Prozesse sind stark kontrollfluss-orientiert. Die Frage ist, wie können neue Formen der Zertifizierung durch Aufsichtsbehörden in die Modellierungsmethode integriert werden? Kann

dieses über neue Rollenkonzepte erfolgen oder können Prozessmuster im Sinne von Control Flow Patterns Alternativen neuer Governance in Bibliotheken anbieten.

- Wie können Wertschöpfungsketten aus der Prozessmodellierung mit denen der Geschäftsmodellierung kombiniert werden? Wertschöpfungsketten-orientierte Methoden der Geschäftsmodellierung wie e3-Value sind stark an dem Prozess orientiert, vernachlässigen aber die verschiedenen Stakeholder und die Value Proposition für den Kunden.
- Wie könnte eine Methode mit Modellierungssprache aussehen, mit der notwendige gesellschaftliche, wirtschaftliche und industrielle Leistungen durch innovative Prozesse auf der Blockchain nachhaltig gestaltet werden?

2.6 Vertrauenswürdigkeit und Sicherheit von Smart Contracts

Smart Contracts sind kleine Programme, die als Bestandteil einzelner Transaktionen in der Blockchain während der Validierung von Transaktion durch die Peers ausgeführt werden. Erst Smart Contracts machen aus einer Blockchain mehr als nur einen verteilten sicheren Speicher und ermöglichen automatisierte und vertrauenswürdige Modifikation von Informationen in der Blockchain. So können in Bitcoin Smart Contracts dazu verwendet werden, verschiedene Arten von Transaktionen wie z.B. Escrow zu realisieren. Während Smart Contracts in Bitcoin nur aus wenigen Operationen bestehen dürfen und keine Schleifen realisieren können, bietet die Ethereum-Blockchain eine "quasi-Turing-vollständige" Sprache an, deren Ausführung in einer dedizierten virtuellen Maschine "Gas" kostet. Auf diese Weise ist sichergestellt, dass ein Smart Contract terminiert, obwohl die Sprache selbst Turing-vollständig ist und daher Endlosschleifen erlaubt. Die Hyperledger-Blockchain geht noch weiter und erlaubt die Ausführung von fast beliebigen Programmen. Diese werden Chaincode genannt, der in verschiedenen Hochsprachen wie Java oder Go geschrieben werden kann und von vertrauenswürdigen "Validating Peers" ausgeführt wird. Während der Ausführung hat der Chaincode Zugriff auf die in der Blockchain gespeicherten Informationen und kann sie auslesen oder weitere Informationen speichern. Des Weiteren ist Chaincode bei der Ausführung lediglich durch Docker-Container vom restlichen Environment isoliert, d.h. die Ausführung findet nicht in einer virtuellen Maschine, sondern direkt auf dem Prozessor des Peers statt.

Die Korrektheit von Smart Contracts ist von äußerster Wichtigkeit, da im Gegensatz zu bspw. Desktop- oder Webanwendungen kontinuierliche Updates von Smart-Contracts nicht ohne weiteres möglich sind. Dies bedeutet, dass einmal eingesetzter Smart-Contract-Code nicht mehr revidiert werden kann, ohne die Integrität der in der Blockchain gespeicherten Daten in Frage zu stellen. In der Tat wurden in der Vergangenheit immer wieder Angriffe auf Smart Contracts bekannt, die zum Teil durch schwer zu erkennende Programmierfehler im Smart Contract ermöglicht wurden (unchecked-send, reentrancy, solarstorm). Darüber hinaus sind jedoch auch die Ausführungsumgebungen für Smart Contracts teilweise unsicher. So kann Hyperledger derzeit nicht garantieren, dass Chaincode terminiert¹. Da gleichzeitig die ausführende Umgebung unbegrenzte CPU-Ressourcen des validierenden Peers nutzen kann, können Smart Contracts so leicht als Denial-of-Service-Angriff auf den Peer genutzt werden. Des

¹ <https://github.com/hyperledger-archives/fabric/issues/2232>

Weiteren ist Chaincode nicht auf Kommunikation mit der Blockchain begrenzt, sondern kann auch externe Dienste aufrufen und somit sind auch schädliche Smart Contracts denkbar, die z.B. Spam verschicken oder als Bots innerhalb der Blockchain agieren.

Beim Einsatz von Smart Contracts müssen also zwei Dinge sichergestellt sein: zum einen muss der Smart Contract selbst korrekt und sicher gegen Angriffe wie Reentrancy sein. In der Praxis ist dies nicht trivial sicherzustellen, wie der DAO-Angriff gezeigt hat. Zum anderen muss sichergestellt werden, dass keine böartigen Smart Contracts in die Blockchain gelangen. Dies gilt insbesondere für Blockchains mit mächtigen Smart-Contract-Sprachen wie Hyperledger und Ethereum. Zwar geht Ethereum mit einer Unterstützung von formaler Verifikation von Smart Contracts durch das why3-Framework erste Schritte in die richtige Richtung, doch noch sind solche Verfahren für die meisten Entwickler zu aufwändig und setzen für einen sinnvollen Einsatz zu viel Hintergrundwissen voraus.

Generell besteht noch hoher Bedarf an Forschung und Entwicklung im Bereich sicherer Smart Contracts - sowohl beim Einsatz formal verifizierbarer Sprachen, als auch in der Unterstützung von Entwicklern und der Validierung von Code vor der Aufnahme in die Blockchain.

2.7 Geschäftsmodelle

Aufgrund der spezifischen Eigenschaften der Blockchain – vor allem verteilte Konsensbildung, digitaler Transfer von Werten, Automatisierung und Irreversibilität – hat die Technologie auf der einen Seite das Potenzial, ganze Geschäftsmodelle vieler Organisationen und Institutionen in Frage zu stellen. Auf der anderen Seite bietet sie aber auch die Möglichkeit neuer Geschäftsmodelle, die ohne Blockchain nicht – oder zumindest nicht wirtschaftlich – abbildbar wären.

Das Potenzial der Blockchain wird für verschiedenste Kontexte und Anwendungsbereiche erkannt. Gleichzeitig besteht derzeit Unklarheit darüber, welche strukturellen Eigenschaften Geschäftsmodelle aufweisen, die im besonderen Maße von den Vorzügen des Blockchain profitieren, und wie diese wirtschaftlich zu gestalten sind.

Vor diesem Hintergrund ergeben sich zahlreiche Fragestellungen für die akademische Forschung zur Geschäftsmodellen und Wirtschaftlichkeit von Blockchain-Lösungen:

- Was sind – auch wirtschaftlich – tragfähige Anwendungsfälle für die Blockchain-Technologie und wie sind diese auszugestalten?
- Was sind – vom spezifischen Anwendungsfall abstrahiert – Eigenschaften von Geschäftsmodellen, die von einer Umsetzung mit Blockchain profitieren können?
- Wie lassen sich die Auswirkungen einer Blockchain-Implementierung auf etablierte Geschäftsmodelle prognostizieren – z.B. beim potenzielle Wegfall von Intermediären?
- Wie lässt sich die wirtschaftliche Vorteilhaftigkeit von Blockchain-Lösungen gegenüber herkömmlichen Umsetzungen ermitteln?
- Wie lassen sich wirtschaftlich sinnvolle Blockchain-Geschäftsmodelle modellieren und umsetzen?

- Welchen Einfluss wird die Technologie über einzelne Unternehmen hinaus auf bestehende Branchen oder die Wirtschaft insgesamt haben?
- Welche Chancen und welche Risiken ergeben sich daraus für die Wirtschaft Deutschlands und der Europäischen Union?

Eine wissenschaftliche Beantwortung dieser Fragen würde dazu beitragen, das Potenzial der Blockchain in spezifischen Realweltszenarien zur Entfaltung kommen zu lassen. In vielen Fällen gehen heutige Anwendungsfälle nicht über den Prototypenstatus hinaus. Erst eine fundierte Auseinandersetzung mit geeigneten Geschäftsmodellen und deren Wirtschaftlichkeit wird der Blockchain zum endgültigen Durchbruch in tragfähigen Anwendungsfällen verhelfen.

3 Anwendungsfelder

Derzeit sind sicherlich die meisten praktischen Anwendungsfälle der Blockchain im Finanzsektor zu finden. Eine Übersicht über konkrete Blockchain Lösungen verdeutlicht allerdings, dass verschiedene Projekte sich den folgenden Anwendungsbereichen zuordnen lassen.

- Kryptowährungen: Blockchain-Anwendung als Transaktionsprotokoll für verschiedene Kryptowährungen wie z. B. Bitcoin (BTC), Ethereum (ETH) und Monero (XMR).
- Business-Networks: Blockchain-Anwendungen im Bereich Smart Contracting und Datenaustausch wie z.B. Ethereum (Smart Contract Applications), Hyperledger und MultiChain
- Banking: Blockchain-Anwendungen im Bereich Finanztransaktionen wie z. B. Corda und Ripple.

Die Blockchain-Technologie findet bei verschiedenen FinTechs Einsatz. So hat z.B. der Finanzdienstleister Bitbond Ende des Jahres 2016 eine BaFin-Lizenz erhalten und wickelt das Kreditgeschäft zwischen Privatpersonen (P2P Lending) mit Hilfe der Blockchain Technologie ab. R3 CEV leitet ein Konsortium bestehend aus 75 der weltweit führenden Finanzinstitutionen, das an der Implementierung eines Blockchain-basierten Systems zur Abwicklung von Finanztransaktionen zwischen Finanzinstituten ("Global Fabric for Finance") arbeitet. Sie setzen dabei auf die Blockchain Lösung Corda. In diesem Zusammenhang liefert Ripple ein Kommunikationsprotokoll für Banken basierend auf der Blockchain Technologie ähnlich dem SWIFT-Protokoll (Society for Worldwide Interbank Financial Telecommunication)

Blockchains können in all den Bereich Anwendung finden, die eine Erfassung, einen Nachweis oder Transaktionen jeglicher Art von Kontrakten oder Objekten zum Gegenstand haben [9, 11]]. So hat IBM vor kurzem das Blockchain-basierte Handelsregister präsentiert. An einen außergewöhnlichen Anwendungsfall arbeitet Everledger. Das Unternehmen erstellt bzw. verwaltet digitale Dokumente zum Ursprung, zur Identifizierung und zu Besitzverhältnissen von Diamanten und schreibt diese in eine Blockchain mit dem Ziel, den Betrug im Diamantenhandel einzugrenzen.

In Bereichen B2B-Trading und Supply Chain Management entwickelt das Unternehmen Skuchain verschiedene Blockchain-basierte Lösungen z. B. zur echtzeitnahen Nachverfolgung von Rechnungen und Transaktionen sowie der Dokumentation von

Bauteilhistorien in der Supply Chain [12]. Auch im Handel wird auf die Blockchain gesetzt. Walmart wird Anfang 2017 ein Blockchain-System zur Nachverfolgung von Lebensmitteln testen. Gartner prophezeit, dass der aktuelle Hype um das Thema Blockchain seinen höchsten Stand fast erreicht hat und dass die Anzahl an Blockchain-Implementierungen in den nächsten fünf Jahren rasant steigen werde [10]. Die folgenden Kapitel betrachten einige der Anwendungsfelder und Branchen für diese Lösungen genauer.

3.1 Internet der Dinge

Ein wesentliches Element des Internet-der-Dinge ist die digitale Vernetzung aller physischen smarten Objekte über smarte Services. Dabei wird das Ziel verfolgt, die Qualität der Interaktion von Mensch und Maschine oder auch von Maschinen untereinander zu verbessern. Da eine zentrale Koordination des Internet der Dinge wohl nahezu unmöglich wäre, wird dabei auch eine weitgehende Autonomie der intelligenten Gegenstände angestrebt. Diese Autonomie kann an mehreren Stellen durch die Blockchain-Technologie unterstützt werden.

Für die Logistik als eine der Hauptanwendungsdomänen bedeutet das, dass sich Ressourcen und Güter miteinander vernetzen, ihre Zustände austauschen und im Sinne einer optimalen Wertschöpfung spezifische Interaktionen aushandeln. Die hierdurch resultierenden wertschöpfenden Tätigkeiten müssen nachgehalten und transparent für alle beteiligten Akteure gespeichert werden. Hierbei ist es unerheblich, ob es sich um unternehmensinterne Prozesse (z.B. Auslastungsbestimmung der Ressourcen, Nachvollziehbarkeit im Fall eines Qualitätsmangels, ökologischer Fußabdruck oder Prozesskostenrechnung) oder unternehmensübergreifende Prozesse (z.B. Kostenverteilung, Abrechnung, Verwendungsnachweis) handelt. In jedem Fall müssen die durchgeführten Wertschöpfungsprozesse dokumentiert und der Bezug zwischen den Gütern und den verwendeten Ressourcen und Arbeitsmitteln allen Beteiligten manipulationsfrei zur Verfügung gestellt werden. Im Falle des Verwendungsnachweises eines Produktes oder des ökologischen Fußabdruckes gilt dies auch für den Kunden, der ein besonderes Interesse an nicht manipulierbaren Informationen hat.

Die Blockchain kann hier einen Ansatz bieten, der in diesem im Grundsatz auf Dezentralität aufgebautes System eine zentrale Instanz ersetzen kann, deren Implementierung schwierig ist und im Wesentlichen auch nicht dem Interesse der Beteiligten entspricht. Eine große Herausforderung liegt hier in der (sicheren) Verbindung der physischen Objekte und deren z.B. mit Sensorik erfassten Daten und den entsprechenden Einträgen in der Blockchain. Es muss sichergestellt werden, dass virtuelle Einträge (der Blockchain) und physische Objekte, wie Güter, eindeutig miteinander verbunden sind und zugeordnet werden können.

Smart Contracts bieten im Internet der Dinge die Möglichkeit, mit Maschinen Vereinbarungen zu treffen, deren Einhaltung in beide Richtungen gewährleistet wird. Im Sinne des Internet-of-Value können Maschinen ihre Dienstleistungen dann direkt mit ihrem Nutzer abrechnen und verdientes Geld dezentral in einem eWallet speichern. Vertrag und Abrechnung können auch dann zustande kommen, wenn eine Maschine zu diesem Zeitpunkt nicht mit dem Internet verbunden ist. Sie werden erst später über die Blockchain synchronisiert.

So wären zukünftig beispielsweise Geschäftsmodelle denkbar, in denen Hersteller autonom arbeitende Maschinen (z.B. autonome Fahrzeuge) völlig frei ihre Dienstleistungen (z.B. Taxifahrten) anbieten lassen. Maschinen verdienen dann direkt ihr Geld (z.B. durch Personentransport), melden Wartungsbedarf selbstständig an und

rechnen in beide Richtungen direkt ab. Überschüsse werden schließlich an den Hersteller gebucht. Selbst die gerade politisch diskutierte Besteuerung der Arbeit von Robotern wäre damit einfach zu realisieren. Wie menschliche Arbeitnehmer, würde ein Teil des Einkommens der Maschine an den Staat und damit an die Allgemeinheit abgeführt.

3.2 Smart Grid

Das Smart Grid ist im Grunde genommen eine Instanz des Internet der Dinge, birgt aufgrund der Komplexität des Stromnetzes weitreichendere Herausforderungen. Der Energiesektor ist aktuell von zwei wesentlichen Trends geprägt: Erstens erfordern erneuerbare Energien mit ihrer volatilen Einspeisung eine verbesserte Koordination von Angebot und Nachfrage im Netz. Zweitens erfolgt diese Einspeisung häufig nicht mehr – wie früher – an wenigen, zentralen Punkten (Großkraftwerken), sondern dezentral in der Fläche. Die Dezentralität ist dabei nicht nur räumlich zu verstehen, sondern auch organisatorisch: Statt wenigen Kraftwerksbetreibern kann heute jeder Eigenheimbesitzer mit Photovoltaikanlage am Strommarkt teilnehmen.

Ein höherer Koordinationsbedarf und ein Trend zur Dezentralisierung legen nahe, dass die Koordination selbst ebenfalls weiter dezentralisiert werden könnte. Konkret wird beispielsweise diskutiert, dass Prosumer verbrauchten oder selbst erzeugten Strom nicht mehr mit ihrem jeweiligen Stromanbieter handeln, sondern mit anderen Prosumern im Netz. Im Sinne des oben beschriebenen Internet der Dinge könnte dies sogar direkt auf einzelne Geräte bezogen werden, beispielsweise könnte eine Photovoltaikanlage ihren Strom direkt an ein Elektroauto liefern und abrechnen. Aufgrund der begrenzten Vertrauenswürdigkeit solch beliebiger Akteure in einem dezentralisierten Strommarkt ist die Blockchain-Technologie mit ihrer Möglichkeit der Wertübertragung eine ideale Basis.

Alternativ stünden jedoch auch weiterhin zentralisierte Lösungen zur Auswahl. Beispielsweise könnten Verteilnetzbetreiber den dezentralen Handel koordinieren und damit eine dezentral zentrale Vertrauensinstanz darstellen. Daher bleibt abzuwarten, inwieweit Lösungen im Smart Grid im gut ausgebauten und stark regulierten Strommarkt Anwendung finden werden oder inwieweit sie insbesondere in anderen oder spezielleren Anwendungsfällen zum Tragen kommen.

3.3 Herkunftsnachweise

Die Bereitstellung, Prüfung und Wahrung von Herkunftsnachweisen (Provenance) stellt heute einen bedeutenden Wirtschaftsfaktor dar. Nicht nur Wirtschaftsprüfungsgesellschaften, Auditoren oder Zertifizierer sind von dem Änderungspotential einer Blockchain betroffen, sondern auch Hersteller in der Verfolgung ihrer Produkte.

Systeme wie Everledger ermöglichen die Nachverfolgung der Eigentümer und der Besitzerwechsel beispielsweise für Diamanten. Everledger dokumentiert für jeden Diamanten alle eigentumsrelevanten Transaktionen. Somit lässt sich die Eigentumshistorie zurück bis zur Registrierung im System zweifelsfrei nachvollziehen. Von Vorteil ist die Identifikationsmöglichkeit von Diamanten: Jeder Diamant ist auf Grund seines optischen Verhalten eindeutig identifizierbar, vergleichbar mit einem Fingerabdruck. Wenn ein Diamant untersucht wird, kann auf Basis des Fingerabdrucks geprüft werden, ob er in der Blockchain bekannt ist und es können damit die Eigentumsverhältnisse geklärt werden. Interessant ist dieser Service für vielfältige Geschäftspartner wie Banken, Versicherungen, Diamantenhändler aber auch Polizei und Gerichte. Everledger baut auf die eindeutige Identifizierbarkeit und die Wertigkeit des Produktes auf.

Vergleichbare Herkunftsnachweise werden aber auch für andere Industriesektoren und Produktarten benötigt. Zum einen ist bei Produktzulassungen nachzuweisen, dass bestimmte Konflikt-Mineralien wie Zinn, Wolfram oder Tantal nicht im Produktionsprozess verwendet wurden. Zum anderen ist die Verwendung herstellertestifizierter Ersatzteile von Interesse um sicher zu stellen, dass aus Sicherheitsgründen keine gefälschten Bauteile verwendet werden. Beides kann auf einer eindeutigen Kennung der Produkte oder einer revisionssicheren Duplizierung der Buchführung aufbauen. Im Kern ist immer sicher zu stellen, dass die Herkunft der Produkte und Rohstoffe eindeutig rückverfolgbar ist.

Beispielsweise sind beim Transport von Gefahrgut jedem Fahrzeug umfangreiche Dokumentationen von Transportbehältern, Fahrzeugeigenschaften, Schulungen, etc. beizulegen. Mit Smart Contracts lassen sich die Regularien und Vorschriften im Sinne eines elektronischen Kontraktmanagement abbilden, d.h. Regeln und Prozesse werden formal beschrieben und automatisch überwacht. Da gemäß neu etablierter Richtlinien der Aufsichtsbehörden die Transportpapiere nun in digitaler Form zu verwalten und von verschiedenen Stakeholdern lesbar sind, erhält man ein geschlossenes System der Informationen und Prozesse zum Gefahrguttransport und kann jederzeit zeigen, dass die gesetzlichen Bestimmungen für jeden Transport eingehalten wurden. Zudem lassen sich bei internationalen Transportketten die national jeweils gültigen Bestimmungen prüfen und gleichzeitig die Sicherungsmaßnahmen normalisieren, um in jedem Land die Mindestbestimmungen einzuhalten.

3.4 Supply Chain Management und Einkauf

Die Blockchain steht für eine sichere, verteilte, insbesondere fehlerresistente Technologie, die darüber hinaus das Potenzial besitzt, das Vertrauensproblem zwischen Wertschöpfungspartnern hinsichtlich Transaktionen monetärer Werte, Vertragsabwicklungen und den Austausch von Daten zu lösen.

Das Supply Chain Management beschreibt in diesem Zusammenhang ein interessantes Anwendungsfeld für unterschiedliche Implementierungen dieser Technologie. Die Vielzahl an Wertschöpfungspartnern bestehend aus Lieferanten, Herstellern, Händlern, Logistik- und Finanzdienstleistern, zwischen denen verschiedene Leistungsvereinbarungen existieren, benötigen insbesondere vor dem Hintergrund der zunehmenden Digitalisierung, Technologien, die einen sicheren Datenaustausch unterstützen. Die Digitalisierungsbestrebungen im Kontext des Internets der Dinge (IoT) führen darüber hinaus zu vielen neuen Möglichkeiten der smarten Prozesssteuerung im Supply Chain Management und insbesondere im Financial Supply Chain Management.

Während wir heute im Bereich der physischen Leistungserbringung von logistischen Prozessen in der Supply Chain die Grenze des Möglichen, durch Automatisierung, neueste Hard- und Software und intelligente Planungskonzepte sowie smarte Prozesse erreicht zu scheinen haben, sind Finanzprozesse in der Supply Chain immer noch zu langsam und damit entkoppelt vom eigentlichen Leistungserstellungsprozess. Die Gründe dafür lassen sich in der Regel auf manuelle und fehleranfällige Prozesse zurückführen. So werden heute immer noch mehr als 60 Prozent der B2B-Transaktionen basierend auf Papierrechnungen abgewickelt. Durch den Einsatz von Blockchains können Transaktionen unabhängig von Rechnungen über Smart Contracts abgewickelt werden. Diese Technologie erlaubt zudem eine einfache Integration und sichere Vernetzung von verschiedenen Supply Chain Partnern. In der folgenden Abbildung ist ein Blockchain-basiertes Supply Chain Netzwerk aus verschiedenen Partnern vereinfacht dargestellt.

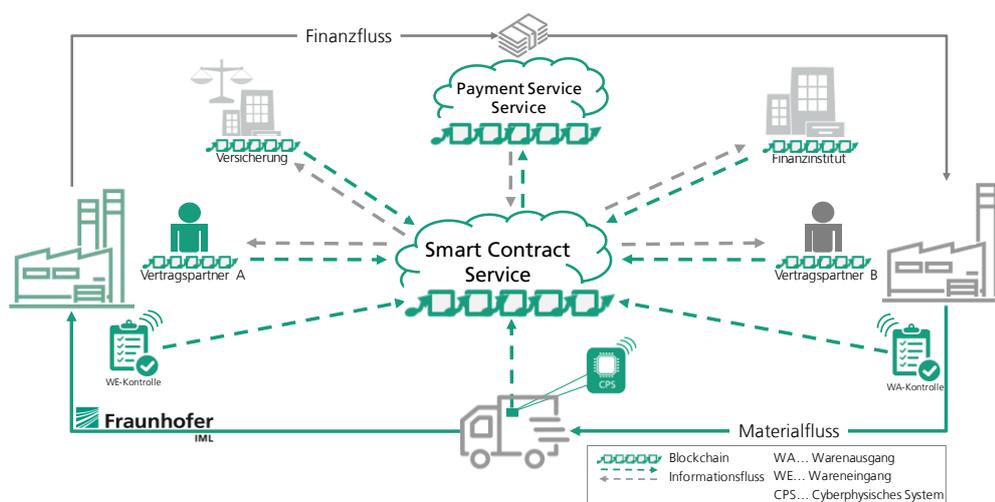


Abbildung 1: Blockchain-basiertes Supply Chain Netzwerk

Die Blockchain fungiert dabei als verteilter Datenspeicher und sichert öffentlich sowie unwiderruflich alle relevanten Informationen für den Smart Contract. Der Smart Contract als ausführendes Computerprogramm überprüft basierend auf diesen Informationen die Einhaltung der darin enthaltenen Vertragsinhalte und legitimiert selbständig Finanztransaktionen bei Erfüllung von bestimmten Vertragsbedingungen. In Kombination mit dem Einsatz von dezentralen Steuereinheiten (siehe www.sofia-projekt.de) können logistische Objekte im Supply Chain Netzwerk Dispositionsentscheidungen autonom treffen und Aufträge selbständig erteilen.

Neben autonomen Dispositionsentscheidungen und der selbständigen Abwicklung von Transaktionen bieten Smart Contracts ein großes Potential zur Effizienzsteigerung von Prozessen insbesondere im operativen und strategischen Einkauf. So können Bestellungen autonom ausgeführt werden, und Wertschöpfungsstammbäume über mehrere Stufen im Lieferantennetzwerk (Tier 1-n) zur Qualitätssicherung und Lieferantenentwicklung über die Blockchain angelegt werden. Der Transparenzgewinn für Herstellerunternehmen wäre enorm. Es existieren bereits Beispiele wie mit Hilfe dieser Smart Contracts Leasingverträge überwacht werden können. So kann bei nicht fristgerechter Entrichtung der Leasinggebühr durch den Leasingnehmer das Fahrzeug blockiert bzw. die Weiterfahrt systemseitig verhindert werden.

3.5 Medizintechnik

Im Bereich der Medizintechnik sind verschiedenartige Anwendungen von Blockchain- und Smart-Contract-Technologien denkbar. Wenngleich noch keine konkreten Einsatzszenarien implementiert und publiziert sind, so ist das Forschungsinteresse bereits geweckt, angetrieben von dem Wertversprechen, in einem Umfeld hochsensibler Daten grundsätzliche Probleme auf dem Weg zu datengetriebener, personalisierter Medizin zu lösen. Im Zeitalter digitaler Medizin liegen mehr und mehr gesundheitsbezogene Daten in verschiedenen Systemen vor. Das umfasst longitudinale Sensordaten (z.B. von Wearables) genauso wie radiologische Bilder, klinische Informationen aus elektronischen Patientenakten, aber auch hoch schützenswerte Daten wie die Ergebnisse genetischer Tests.

Andererseits ist es ein Erfordernis moderner präventiver Medizin, solche Daten populationsweit auszuwerten, zum Beispiel mit modernen Methoden modellfreier Statistik (deep learning). Der klassische Weg der Modellbildung kann in diesem Umfeld

nicht beschränkt werden, da Daten dieser Art nicht zentralisiert gesammelt und bereit gestellt werden dürfen, und – selbst wenn dies kein Problem wäre – weil es keine gesellschaftlich akzeptierten Methoden der sicheren Datenspeicherung und sicheren Nutzungsüberwachung gibt. Ein Ausweg könnten Mechanismen sein, die dem Besitzer der Daten transaktionelle, auditierbare Kontrolle über ihre Verwendung erlauben. Genau das ist das Wertversprechen von Blockchain-Technologie.

Im Umfeld der Medizin werden nicht alle Blockchain-Charakteristika benötigt, zum Beispiel ist es nicht unbedingt notwendig, die Verifizierung zu dezentralisieren. Nach herrschender Meinung sind dennoch mindestens drei große technische Herausforderungen zu meistern:

1. Lückenlose Datennutzungs-Überwachung. Es muss nachweisbar ausgeschlossen sein, dass Datennutzung am System vorbei geschieht. Das kann auch die Zertifizierung sicherer Hardware notwendig machen.
2. Gruppen- und personenspezifische Nutzungserlaubnis. Es muss möglich sein, die Datennutzung auf bestimmte Personen oder Institutionen zu beschränken, oder auch auf spezifische Teile der Daten.
3. Lückenlose dezentrale Daten und Logs. In einem Szenario, in dem Daten dezentral gespeichert werden (in Krankenhäusern, Versicherungen, Mobilgeräten, ...) müssen Daten zwischen Systemen übertragen werden. Die Sicherung der Übertragung gegen Missbrauch ist eine große Herausforderung.

In allen drei Bereichen existieren Projekte und Ansätze, die eine Grundlage sein könnten, einen neuartigen Zutritt zum Bereich des personalisierten datengetriebenen Gesundheitsmanagements zu eröffnen.

3.6 Finanzbranche

Die Finanzbranche bildet derzeit den Sektor mit den größten Aktivitäten im Bereich Blockchain. Dennoch beginnen viele etablierte Institutionen der Finanzbranche gerade erst damit, das Potenzial der Blockchain für sich nutzbar zu machen. Während nicht selten betont wird, dass die Blockchain Finanzintermediäre theoretisch komplett ersetzen könnte, wird derzeit gerade von diesen viel Energie in die Verbesserung bereits existierender Finanzsysteme und -dienstleistungen durch die Blockchain-Technologie gesteckt. Um eine Einschätzung über den Einfluss der Blockchain auf die Branche zu ermöglichen, werden im Folgenden exemplarisch ausgewählte Anwendungsbeispiele der Blockchain im Finanzsektor analysiert.

3.6.1 Zahlungsverkehr

Heutige Zahlungsprozesse involvieren mehrere Intermediäre, wie Banken, Clearing-Stellen und Zentralbanken, und sind dabei sehr ressourcenintensiv. Zudem finden Abwicklungsprozesse aufgrund der vielen Intermediären und unterschiedlichen Systeme aus Koordinations- und Kostengründen nicht kontinuierlich, sondern nur einige Male pro Tag statt, wodurch spürbare Zeitverzögerungen entstehen. Blockchains haben theoretisch das Potenzial, diese Zeit- und Kostennachteile zu beseitigen. Die Finanzbranche fokussiert sich dabei vor allem auf internationale Überweisungen, bei denen derzeit besonders hohe Gebühren anfallen. Zudem würde durch eine kürzere Abwicklungszeit das Wechselkursrisiko bei internationalen Transaktionen reduziert. Zusätzlich können Blockchain-basierte Zahlungssysteme Sicherheit und Privatsphäre erhöhen, da Zahlungen auf dem Push-Prinzip beruhen: Kunden können Transaktionen

aktiv initiieren ohne dabei Details wie beispielsweise Bankdaten bereitzustellen. Vorteile für Händler können darin bestehen, dass Betrug durch Ausgleichsbuchungen (wegen der in Blockchain-Systemen inhärenten Transaktionsirreversibilität) verhindert werden kann. Des Weiteren entstehen geringe Bearbeitungsgebühren und eine Kosten- und Risikominimierung, da Zahlungsinformationen von Kunden nicht gespeichert werden müssen.

3.6.2 Kapitalmarkthandel

Da Transaktionsprozesse im Kapitalmarkthandel eine große Anzahl an Akteuren involvieren, müssen kontinuierlich Daten abgeglichen und im Rahmen von Validierungsprozessen wiederholt werden, weshalb hohe Kosten, lange Transaktionszeiten sowie operationale Risiken auftreten. Entsprechend wird vor allem in der Abwicklung von Wertpapiertransaktionen ein vielversprechendes Anwendungsfeld von Blockchain gesehen. Durch die Verwendung einer Blockchain-Lösung könnten die Kosten und die Komplexität in der Transaktionsabwicklung signifikant reduziert und die Abwicklungszeit auf Minuten bzw. Sekunden verringert werden, da die Parteien direkt miteinander handeln. Durch die Verkürzung der Zeitspanne werden sowohl das operationale als auch das Kontrahentenrisiko reduziert, wodurch sich potenziell auch die Eigenkapitalanforderungen für Banken verringern könnten. Das Kredit- und Liquiditätsrisiko könnte effektiv eliminiert werden, da in Blockchain-Systemen aufgrund ihrer Funktionsweise der Besitz entsprechender Mittel vor dem Handel vorausgesetzt wird.

Die Blockchain Technologie ermöglicht darüber hinaus in Verbindung mit dem Einsatz von Smart Contracts rechnungslose Transaktionen. Während heute im B2B-Bereich immer noch mehrheitlich Papierrechnungen versendet werden, die in langwierigen und manuellen Prozessen geprüft, bestätigt und weitergeleitet werden müssen, sichern Blockchains die Vertragsinhalte (Service Level Agreements) und Smart Contracts überwachen die Vertragsausführung. Die zur Leistungsverrichtung gehörende Transaktion kann dann automatisch angestoßen werden. Die Transaktionsbestätigung wird ebenfalls in der Blockchain gespeichert werden. Diese vom Rechnungsprozess entkoppelten und automatischen Transaktionen werden als Smart Payment zusammengefasst.

3.6.3 Compliance

Insbesondere in der Finanzwirtschaft wird für Blockchain auch großes Potenzial im Bereich der Compliance gesehen. In diesem Rahmen werden vor allem zwei Einsatzmöglichkeiten der Blockchain diskutiert: zum einen als zentrales Register zur konsolidierten Buchführung und zum anderen als „Konsortiums-Blockchain“ für Kundendaten. Banken unterhalten aktuell eine Vielzahl unterschiedlicher Kontenbücher für verschiedene Zwecke und implementieren diverse Maßnahmen, um Fehlverhalten in der Buchhaltung zu verhindern. Dies umfasst typischerweise die Durchführung verschiedener Datenintegritätsprozesse und die Verteilung der Verantwortung für die Aufnahme finanzieller Daten in die Bücher. Durch die Verwendung von Blockchain-Konzepten können diese Prozesse weitgehend automatisiert werden, da Blockchain die vertrauenswürdige Konsolidierung einzelner Kontenbücher in ein Datenmodell ermöglicht. Nützlich erscheint hierbei besonders die Umgehung des Double-Spending-Problems in Blockchain-Systemen. Manipulationen in der Buchhaltung wie das Zurückdatieren von Verträgen auf andere Perioden können durch die Irreversibilität und zuverlässigen Zeitstempel von Transaktionen verhindert werden. Die Erfüllung diverser Gesetze und Regelungen zur Geldwäscheprevention wie beispielsweise „Know Your Customer“ (KYC) birgt für Finanzinstitute hohe Kosten und verzögert Transaktionen teilweise maßgeblich. Zudem werden KYC-Prozesse in unterschiedlichen Finanzinstituten

jeweils individuell durchgeführt. Ein branchenweites Kundenregister basierend auf einem Blockchain-System könnte den mehrfachen Aufwand hinsichtlich der KYC-Überprüfungen eliminieren sowie die verschlüsselte Übertragung von Kundendaten erleichtern. In Kombination mit der Verwendung von Smart Contracts könnten außerdem diverse Aspekte automatisiert werden.

3.7 Medienindustrie

Kryptowährungen wie Bitcoin oder Ether bieten Ansätze zu alternativen Vergütungsmodellen und heizen die Fantasie an. Vor allem das omniprésente Metadatenchaos in der Musikindustrie mit ihren fragmentierten Rechten inklusive deren lokaler Ausprägungen scheint in Zeiten transparenter Datenströme Ausgangspunkt für die Fokussierung auf die Blockchain zu sein. Angesichts aller bisher gescheiterten Versuche innerhalb der Branche einheitliche Registrierungs- und Lizenzstandards einzuführen, setzen die unterschiedlichen Stakeholder vor allem nach dem Ende der Aktivitäten zur Global Repertoire Database (Juli 2014)¹ auf die Verheißungen dieser Technologie.

Anders als in der klassischen Herkunftshistorien sind bereits kleinste Teile der im Markt distribuierten Medien (Songs, Filme etc.) mit IPs von vielen individuellen Berechtigten versehen, wodurch die Nachvollziehbarkeit und Authentizitätsprüfungen für die Berechtigten selbst nahezu unmöglich ist.

Bei allen Überlegungen der Marktteilnehmer für einen ersten Einsatz von Blockchain spielen vor allem die intransparenten Lizenzströme in den digitalen Geschäftsmodellen eine große Rolle. Auf Grund von nicht identifizierten Rechteinhabern verbleiben ca. 20 - 50% der nicht zuzuordnenden Lizenzen² aus den sogenannten „black boxes“ bei den großen Marktteilnehmern mit ihren Vermittlerrollen zwischen Konsument und Kreativen. Dies steht im Gegensatz zur Finanzindustrie, wo solche Zahlungen in Regierungsfonds gehen und damit ein Druck zur korrekten Abrechnung schon immer aufrechterhalten wird.

Um die Blockchain Technologie für alle Akteure und vor allem für eine globale, transparente und zeitnahe Vergütung der Kreativen als alternative Lösung einzusetzen, bedarf es einer intensiven Diskussion und Abgleichs aller Hauptteilnehmer und Interessenvertreter („stakeholder alignment focus“). Ziele dieses Austauschs sind Kostenanalysen, die Erstellung einer Roadmap zur Zusammenarbeit der Beteiligten an Standards und die Führung von Diskussionen zu sozialen Auswirkungen, um die Technologie zu stützen sowie eventuelle Regulatoren und Rechtsrahmen zu verstehen. Dabei kann die Fraunhofer-Gesellschaft den Akteuren helfen, immer das wichtigste Transformationspotential der Blockchain im Auge zu behalten: die Reduktion des Bedarfes für Vermittler zur autonomen Ausführung von Transaktionen. Das bedeutet u.a.:

- Festlegung von Übereinkünften in einer geteilten Plattform mit einer Garantie zu deren Ausführung, basierend auf gegenseitig vereinbarten Konditionen und bei einer begrenzten Anzahl von nötigen Aktionen der Gegenseite

¹ <http://www.musikmarkt.de/Aktuell/News/Aus-fuer-die-Global-Repertoire-Database-PRS-will-Alternative>

² Fair Music: Transparency and payment flows in the music industry (Rethink Music, a project of Berklee Institute of Creative Entrepreneurship 2015)

- Eliminierung von erforderlicher Unterstützung bei der Ausführung von Lizenztransaktionen
- Reduzierung von Risiken auf Grund von Misstrauen gegenüber dem Vermögen oder der Verpflichtung der Parteien
- Abschaffung von Vermittlerrollen und deren Konfliktpotential bei der Lösung der aktuellen und kommenden digitalen Geschäftsmodelle

An erster Stelle muss eine Studie zur Identifizierung der erfolgversprechendsten Use Cases stehen, die einen Überblick zu den Playern und deren Zahlen gibt, den aktuellen Stand der relevanten Prozesse und die Analyse der Probleme („pain points“) wiedergibt und eine Beschreibung des zukünftigen Systems und dessen Nutzen abbildet. Nur so kann der Hauptnutzen herausgearbeitet werden, welcher durch neue Infrastruktur sowie Services erreicht werden soll, und die Aufklärung der Community über die entscheidenden Vorteile der Blockchain gelingen.

Wir sehen einen erfolgreichen Einsatz der Blockchain vor allem in der Schaffung geteilter, transparenter Aufbewahrungsorte („shared repository“) für Informationen (Metadaten, digitale Inhalte, Lizenzinformationen), die von mehreren Partnern genutzt werden. Dies erfolgt auf Basis der Definition aller Beziehungen der Schreibberechtigten zu allen Beteiligten und deren geteilten Transaktionen (Lizenzierung, Bearbeitung), für ein Lizenzsystem, welches von einer kleinen Anzahl von berechtigten Marktteilnehmern kontrolliert und völlig transparent betrieben wird.

Fraunhofer ist durch die Neutralität und Technologieführerschaft ideal positioniert, das hierfür nötige Vertrauen zwischen den Partnern, die gemeinsam an den Transaktionen beteiligt sind, zu schaffen. Alle innerhalb der Verwertungskette einzeln oder im Verbund operierende Vermittler profitieren von der Nachvollziehbarkeit und der Automatisierung der gegenseitigen Abhängigkeit bei Transaktionen in einem Blockchain-basierten System und werden somit in die Lage versetzt, sich mit neuen Geschäftsmodellen der z.T. gefährdeten Vermittlerrolle und der Disruption entgegen zu stellen.

3.8 Öffentlicher Sektor

Für den öffentlichen Sektor ist die Blockchain-Technologie sowohl Angriff, als auch Chance zugleich. Die Digitalisierung der Verwaltung zeichnete sich bislang dadurch aus, bestehende Prozesse zu beschleunigen oder effizienter zu gestalten. Mit der Blockchain-Technologie kommt eine neue Dimension hinzu, indem bisher staatlich organisierte Funktionen durch privat organisierte ersetzt werden können. Gleichzeitig bietet der Einsatz der Blockchain-Technologie das Potenzial Transparenz und Vertrauenswürdigkeit in Verwaltungsprozesse zu stärken. Für die verwaltungsinterne Kommunikation bietet die Blockchain zudem die Chance, Abläufe zu vereinfachen insbesondere bei Verwaltungsebenen übergreifenden Prozessen.

In vielen Fällen treten Akteure des öffentlichen Sektors heute als Intermediär auf. Die öffentliche Verwaltung führt Register um Eigentumsverhältnisse zu dokumentieren und Notare sichern durch ihre besondere Vertrauensstellung Eigentumsübertragungen ab. Darüber hinaus tritt der Staat an vielen Punkten als vertrauenswürdige Dritte Instanz (Trusted Third Party) auf, etwa wenn es darum geht Identitäten von Personen oder Dingen zu bestätigen oder die Echtheit von Dokumenten zu belegen.

Entsprechend vielfältig werden potenziellen Einsatzmöglichkeiten im öffentlichen Sektor diskutiert. Das Spektrum der aktuellen Diskussion reicht von E-Payment über Transparenz

& Offenheit, öffentlich geführte Register und Verwaltung von Eigentumsverhältnissen, Herkunftsnachweise, Verifikations- und Bestätigungsdienste, Abbildung digitaler Identitäten bis hin zur Absicherung elektronischer Wahlen. Oftmals handelt es sich dabei um konzeptionelle Überlegungen oder Prototypen. Es lassen sich jedoch auch Beispiele finden, wo die Technologie bereits seit einigen Jahren produktiv im Einsatz ist. Exemplarisch sei hier Estland genannt, das seit einigen Jahren mit einer Blockchain-ähnlichen Technologie¹ die Integrität medizinischer Dokumente absichert. Seit 2015 bietet das Land zudem mit seinem E-Residency-Programm einen Blockchain-basierten Notardienst an. Neben Estland befassen sich viele weitere Staaten intensiv mit der Technologie und entwickeln Strategien zum Einsatz der Blockchain in der Verwaltung, unter anderem Großbritannien, Dubai oder die USA. Eine Vielzahl von Einsatzszenarien wird dabei diskutiert.

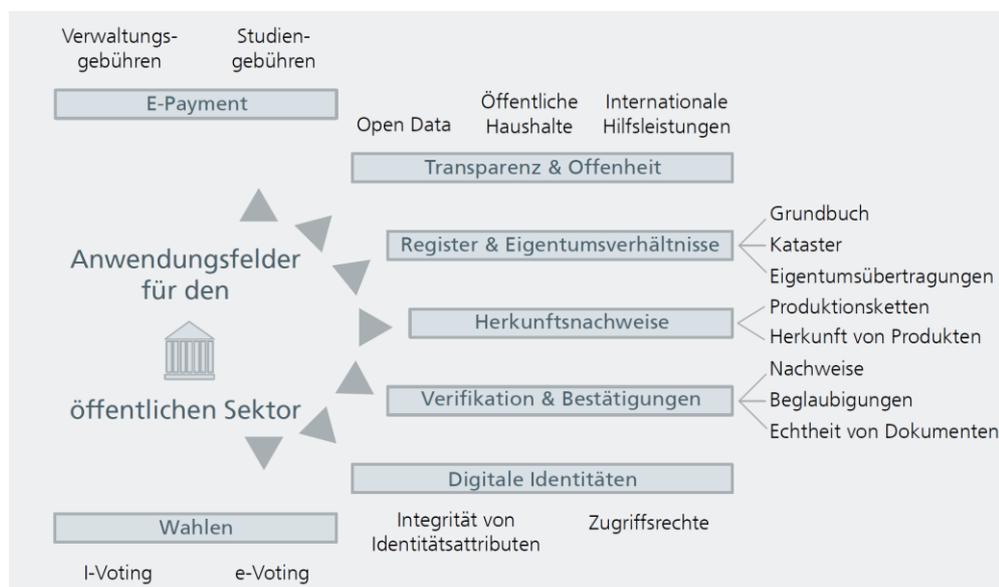


Abbildung 2: International häufig diskutierte Anwendungsfelder der Blockchain-Technologie. [17]

Der offensichtliche Anwendungsfall des E-Payment ist dabei ebenso trivial wie einfach realisierbar. Ein Beispiel findet sich etwa in der schweizerischen Stadt Zug, hier werden Bitcoin als Zahlungsmittel für Verwaltungsgebühren akzeptiert. Ein Dienstleister, der die Bitcoin noch am selben Tag in Schweizer Franken umtauscht verringert für die Verwaltung das Risiko allzu großer Kursschwankungen.

Die weiteren Anwendungsgebiete sind visionärer, gehen jedoch auch mit aufwendigeren Prozessanpassungen einher. Besonders häufig wird die Blockchain im Kontext von Registern und der Eigentumsübertragung genannt. Ihre Eigenschaft Transaktionen nachweisbar, transparent und unveränderbar zu dokumentieren kommt den Anforderungen klassischer Registerführung sehr nahe. Die Gründe für den Einsatz der Blockchain-Technologie können dabei variieren. Interessant ist sie sowohl für jene Regionen, in denen klassische staatliche Strukturen zur Registerführung oder das Vertrauen in eben diese fehlen. Dort wo staatliche Strukturen bereits etabliert sind, kann

¹ Konkret Keyless Signature Infrastructure (KSI)

mit Hilfe der Technologie der Prozess der Eigentumsübertragung selbst transparenter und ggf. schneller abgewickelt werden.

Darüber hinaus kann die Technologie auch zur verwaltungsinternen Zusammenarbeit eingesetzt werden, bspw. zur Prüfung ob bestimmte Daten oder Dokumente in einer Verwaltung vorliegen oder nicht. Des Weiteren ist es möglich über eine Blockchain die Integrität von Daten und Dokumenten abzusichern, was zumindest aus Nutzerperspektive eine leichtgewichtige Alternative zu digitalen Signaturen darstellen kann (siehe auch 3.3).

Weniger relevant für die deutsche Perspektive sind Lösungen aus dem Bereich des E-Voting (elektronische Wahlen) oder gar I-Voting (Wahlen über das Internet). Hierzu erhält in der Regel jeder Stimmberechtigte ein Coin oder Token, das seine Stimme repräsentiert. Jeder Kandidat erhält eine Empfangsadresse (vgl. mit einem Wallet). Die Wahl selbst wird durch eine Transaktion des Token auf die Empfangsadresse des Kandidaten repräsentiert. Zumindest für den Bereich parlamentarischer Wahlen wird der Einsatz technologischer Hilfsmittel in Deutschland sehr kontrovers diskutiert, sodass der Einsatz der Blockchain hier eher unrealistisch erscheint. Für Abstimmungsprozesse mit geringeren Anforderungen (bspw. Vereinswahlen), kann der Ansatz über eine Blockchain durchaus interessant sein, muss sich jedoch mit bereits etablierten Lösungen messen.

In der deutschen Verwaltungslandschaft ist die Blockchain-Technologie bislang nur in Fachkreisen angekommen. Die öffentliche Verwaltung in Deutschland befindet sich seit einigen Jahren in einem tiefgreifenden Wandel, bedingt durch zunehmende Aufgabenfelder, verbunden mit gestiegenen Anforderungen bei gleichzeitig immer knapperen Budgets. Seit Langem wird in der Digitalisierung ein Ausweg aus diesem Dilemma gesehen. Doch zumindest in Deutschland wird das Potenzial bei weitem noch nicht ausgeschöpft wie diverse Studien zeigen. Durch ihren dezentralen Charakter bietet die Blockchain-Technologie eine interessante Perspektive für die föderale Struktur der deutschen Verwaltungslandschaft.

Viele der international diskutierten Anwendungsszenarien im öffentlichen Sektor gehen mit einer Reihe neuer Herausforderungen einher. Aufbau und Betrieb einer Blockchain sind nicht trivial und fordern erfahrene Fachkräfte, unter anderem Kryptologen und Informatiker. Neben einer Vielzahl offener technischer Punkte, stellen sich jedoch auch grundsätzliche Fragen. Klassische Intermediäre schaffen Vertrauen durch organisatorische Maßnahmen. An Intermediäre aus dem öffentlichen Sektor werden dabei besondere Anforderungen hinsichtlich Korrektheit und Vertrauenswürdigkeit gestellt. Mit der Blockchain-Technologie wird dieses organisatorische Vertrauen durch Vertrauen in eine Technologie und deren kryptografische Verfahren ersetzt. Hier gilt es im Einzelfall abzuwägen, ob der Einsatz einer Blockchain sinnvoll und langfristig tragfähig ist.

3.9 Juristischer Sektor

Blockchain kann einerseits den Geltungsanspruch von Recht auf fundamentale Weise herausfordern und andererseits neue Wegen der Rechtsdurchsetzung eröffnen. Die dezentrale und meist pseudonyme Architektur der Netzwerke spielt hierbei die entscheidende Rolle.

Der überwiegende Teil der Rechtsordnung ist technologieneutral ausgestaltet. Der Umstand, dass ein bestimmtes Geschäft mit Hilfe von Blockchain Technologie abgewickelt wird, hat damit im Regelfall keinen Einfluss auf die rechtliche Einordnung des Geschäfts. Von diesem Grundsatz gibt es aber natürlich Ausnahmen.

Offene Blockchain Netzwerke operieren meist global und ermöglichen ohne weiteres grenzüberschreitende Transaktionen. Gepaart mit pseudonymen Strukturen wird der traditionelle Ansatz zur Rechtsdurchsetzung dadurch oftmals faktisch unmöglich gemacht. Blockchain basierte Netzwerke sind damit in sehr geringerem Umfang an regionale Rechtsordnungen gebunden.

Klassisches Regulierungsrecht basiert auf der Annahme, einen konkreten Adressaten definieren und diesem, wenn erforderlich, auch habhaft werden zu können. Diese Annahme wird sowohl durch die Dezentralität als auch die Pseudonymität von Blockchain umfassend in Frage gestellt. Es gilt daher neue Ansätze zur effektiven Rechtsdurchsetzung zu definieren.

Anders verhält es sich freilich bei geschlossenen Systeme, sogenannten Permissioned Ledgers. Die Durchsetzung von Rechtsgrundsätzen und Standards fällt hier leichter. Die entsprechenden Gatekeeper sind taugliche Regulierungsadressaten. Klassische Ansätze des Regulierungsrechts können insoweit ohne weiteres zum Einsatz gebracht werden.

Blockchain kann insgesamt einen wichtigen Beitrag zur automatisierten Abwicklung von Recht leisten. Denkbar wäre zum Beispiel der Einsatz im Bereich EGovernment, etwa bei öffentlichen Katastern vom Grundbuchamt bis hin zur Steuerverwaltung. Auch das Stromnetz könnte über Blockchain sich dezentral selbst verwalten. Inzwischen denken auch viele Kreditinstitute und Versicherungen über den Einsatz solcher Instrumente nach.

Die Automatisierung der Vertragsabwicklung wird bereits seit Mitte der 1990er Jahre unter dem Stichwort Smart Contracts diskutiert. Bei Smart Contracts handelt es sich dabei entgegen der Begrifflichkeit nicht um Verträge im rechtlichen Sinne, sondern um die Verknüpfung von Verträgen mit der Realität. Bestimmte Eigenschaften der Blockchain Technologie können sich bei der Automatisierung der Ausführung nun als sehr nützlich erweisen:

1. Die dezentrale Validierung von Transaktionen erlaubt eine Automatisierung der Vertragsabwicklung auch auf Peer-to-Peer Basis.
2. Blockchain Technologie ermöglicht es, Werte in der Form von Tokens, direkt in einen Vertrag einzubetten und damit dessen Ausführung auch jenseits von Kreditrisiken zu garantieren.
3. Mithilfe von Blockchain Technologie kann die Ausführung von Verträgen so automatisiert werden, dass eine einseitige Veränderung des Prozesses im Nachhinein nicht mehr möglich ist.

Blockchain wird das Potential zugeschrieben, Transaktionskosten dramatisch zu senken, insbesondere durch die Ausschaltung von Intermediären. Dadurch ergibt sich Potential für neue Verträge und Vertragstypen, deren Abwicklung bislang nicht rentabel gewesen wäre, insbesondere im Zusammenhang mit Mikrozahlungen. Bei alledem ist aber zu beachten, dass die Automatisierung von Recht Grenzen hat und auch haben muss. Wertentscheidungen können nicht ersetzt werden durch Technik und Schutzrechte dürfen nicht umgangen werden. Die staatliche Gerichtsbarkeit muss zugänglich und auch praktisch effektiv bleiben.

Neben einzelnen Vertragsverhältnissen können auch Teile gesellschaftsrechtlicher Verhältnisse auf der Grundlage von Blockchain abgewickelt werden. Sogenannte Decentralized Autonomous Organizations (DAOs) basieren auf dieser Idee. Tokens werden insoweit als Stimmrechte innerhalb der „Gesellschaft“ eingesetzt. Innovative Organisationsformen und Finanzierungsgrundlagen können ökonomisch stimulierend

wirken. Die daraus resultierenden gesellschaftlichen und schuldrechtlichen Fragestellungen sind aber bislang weitgehend ungeklärt.

Chance und Herausforderung gleichermaßen bedeutet Blockchain für den Datenschutz. Mit Blick auf offene Systeme wird dies besonders deutlich: Einerseits basiert die Datenbank und das Vertrauen in diese gerade auf der Transparenz aller Transaktionen. Andererseits basiert die Technologie auf der Nutzung von Pseudonymen und inkorporiert insbesondere damit letztlich Privacy by Design Gedanken. Konflikte zwischen dem Blockchain-Ansatz und der Datenschutzgrundverordnung können sich insbesondere hinsichtlich der Verantwortlichkeit für die Datenverarbeitung und das Recht auf „vergessen werden“ ergeben.

Um Innovationen zu fördern, können regulatorische Sandkästen definiert werden, in denen der allgemeine regulatorische Rahmen zu hohe Marktzugangshürden bilden würde, ohne dabei unverantwortliche Gefahren einzugehen. Insoweit muss aber sichergestellt werden, dass angemessene Sorgfaltsmaßnahmen Anwendung finden, sobald vordefinierte Schwellenwerte überschritten werden.

Auf mittlere Sicht wird ein regulatorischer laissez-faire Ansatz allerdings nicht genug sein. Änderungen der Rechtsordnung werden erforderlich werden, sowohl um Gefahren vorzubeugen, als auch um weitere Innovationen zu ermöglichen.

Einerseits können sich nämlich aus dem möglicherweise rasanten Wachstum einzelner Anwendungen neue systemische Herausforderungen ergeben, auch für die Rechtsordnung. Der für die Entwicklung der Technologie erforderliche Freiraum muss deshalb einhergehen mit Investitionen in Monitoring und der Entwicklung von Stress-Tests. Dies gilt auch und vor allem im Zusammenhang mit Smart Contracts.

Andererseits sind Anpassungen des regulatorischen Rahmens erforderlich, um Innovationen zu ermöglichen. Ein offensichtliches Beispiel sind Formvorschriften: Blockchain hat Potential im Bereich der Verifizierung von Transaktionen. Das Recht ist insoweit aber gerade nicht technologieneutral. Das Potential ist damit bedingt durch die Anerkennung der Technologie als geeignete Form des jeweiligen Geschäfts. Regulatorische Zurückhaltung ist insoweit nicht genug zur Beförderung von Innovation.

3.10 Darknet

Das Darknet als Anwendungsfeld von Blockchain und der durch sie ermöglichten Kryptowährungen steht im gesellschaftlichen Interessensausgleich zwischen freiem und unbeobachteten Informations- und Gütertausch und den Interessen der Strafverfolgung.

Neben dem öffentlich leicht zugänglichen sowie von Google und anderen Suchmaschinen indexierten WWW sind heute weitere Ausprägungen des Internets bekannt. Einige davon sind gezielt darauf ausgelegt, eine nicht oder nur schwer nachvollziehbare Kommunikation, Datenaustausch und Handel zu ermöglichen. Sie werden heute oft unter dem Begriff "Darknet" zusammengefasst. Es handelt sich um Kanäle im Internet, die auch für illegale Zwecke genutzt werden. Hierzu gehören Marktplätze wie Silk Road und zahlreiche Foren im Verbindungsdaten anonymisierenden Tor-Netz sowie Tauschbörsen für Software und Medien.

Dieses "Darknet" hat zunehmend an Relevanz gewonnen, da es einen scheinbar rechtsfreien Raum bietet, der vom restlichen Internet aus nicht unmittelbar zugänglich ist und Raum für extremistische Botschaften, kriminelles Gedankengut und kriminellen

Handel sowie als Kommunikations- und Interaktionsform dient. So ist im Darknet eine Umgebung entstanden, die durch das Versprechen von Anonymität und Nichtverfolgbarkeit sehr attraktiv für Radikale und Kriminelle ist. Dabei darf nicht übersehen werden, dass natürlich auch zahlreiche völlig legale und nachvollziehbare Nutzungsformen im Darknet vorhanden sind, die ausschließlich den Aspekt des freien und unbeobachteten Informationsaustauschs verfolgen.

Die meisten heute in Gebrauch befindlichen Kryptowährungen (wie Bitcoin, im Folgenden pars pro toto für Kryptowährung verwendet) nutzen als Datenbasis Blockchains. Diese Blockchain ist für jeden Handelspartner stets einsehbar. Entitäten, zwischen denen Bitcoins transferiert werden, sind sogenannte Bitcoin-Wallets. Diese sind per se nicht an die Identität einer Person geknüpft und können in beliebiger Anzahl erzeugt werden, sodass Partner einer Bitcoin-Transaktion in der Regel anonym bleiben können. Entsprechend wird Bitcoin auch als Währung für die Durchführung illegaler Handelsgeschäfte im Darknet verwendet, z.B. bezüglich Drogen, Waffen und Kinderpornografie.

Strafverfolgungsbehörden haben ein Interesse daran illegale Handlungen im Darknet aufzuspüren. Es geht darum herauszufinden, inwieweit das gesetzekonforme Beobachten von Bitcoin-Transaktionen bekannter Handelspartner (beispielsweise bekannte Wallets, gegebenenfalls zugehörige Identitäten) sowie das gesetzekonforme Erheben zusätzlicher Daten auf Handelsplätzen im Darknet (beispielsweise angebotene Waren, Zuordnungen von Nicknames zu Wallets) weitere Rückschlüsse auf die Art der Transaktion, der gehandelten Ware sowie zusätzliche Informationen über die Identitäten der jeweiligen Handelspartner zulassen.

3.11 Kriterien für einen Blockchain-Einsatz

Die in diesem Kapitel erfolgte Beschreibung unterschiedlicher Anwendungsfelder zeigt, dass der Einsatz einer Blockchain-Lösung unter bestimmten Rahmenbedingungen ein großes Potenzial hat. Zusammengefasst ist dies der Fall, wenn ein oder mehrere der folgenden Kriterien erfüllt sind.

1. **Intermediäre:** Im betroffenen Anwendungsfall können oder sollen Intermediäre im Prozess umgangen werden. Unternehmen sollten daher ihre Prozesse und Geschäftsmodelle daraufhin prüfen, ob sie entweder selbst die Rolle eines Intermediärs erfüllen oder Prozesse optimieren können, bei denen sie auf einen Intermediär angewiesen sind. Der Einsatz einer Blockchain ist sinnvoll, wenn der Intermediär
 - a. Kosten für die Prozessschritte verursacht, die durch Funktionen der Blockchain ebenfalls erbracht werden können
 - b. einen Prozess verzögert und eine Blockchain Anwendung dies beschleunigen kann
 - c. politische Gründe dafür sprechen von einer zentralen Intermediär-gesteuerten Prozessführung auf eine dezentrale zu wechseln
2. **Daten- und Prozessintegrität:** Für den Anwendungsfall ist eine rückwirkende Unveränderbarkeit der Transaktionen sowie eine exakt vorgegebene Durchführung erforderlich.

3. **Dezentrales Netzwerk:** Der Einsatz eines Netzwerks an validierenden bzw. passiv nutzenden Knoten, die Prozesse autonom durchführen, ist sinnvoll und/oder möglich. Dies ist für alle Prozesse relevant die flexible neue und flüchtige Kooperationspartnern ohne stabile und sichere Transaktions- und Vertrauensbasis involvieren. Eine Blockchain kann in einem solchen Fall eine vernetzte Integrität garantieren
4. **Übermittlung von Werten und Wahrung von Rechten:** Blockchains ermöglichen die Übertragung von Werten und Rechten, daher sind alle Prozesse relevant, in denen Originale, Herkunftsnachweise oder Rechte transportiert oder übertragen werden müssen.

Ergänzend zu diesen Kriterien gilt, dass der Fokus nicht auf der Anwendung einer Kryptowährung liegen sollte und keine Prozesse ausgewählt werden sollten, die einer strengen Regulierung unterliegen.

4 Beitrag und Kompetenzen der Fraunhofer-Gesellschaft

4.1 Blockchain Lab - Konzeption, Entwicklung und Evaluation

Die Technologie der Blockchain hat somit nicht nur vielfältige Auswirkungen auf die Prozesse, sondern auch auf Strukturen der Governance, welche die Aufgabenverteilung zwischen Prozessbeteiligten signifikant ändern kann. Durch die neue Aufgabenverteilung und Änderung der Governance ergibt sich auch die Frage nach neuen Geschäftsmodellen für die *neue Value Chain* nach Re-Engineering des Prozesses.

Die verschiedenen Dimensionen des Konzepts einer Blockchain erfordern demzufolge einen multidisziplinären Ansatz zur Erschließung des Potentials verteilten Transaktionsmanagements mit innovativen Ansätzen der Konsensfindung. Diesen Aspekt greift das Blockchain-Labor des Fraunhofer FIT als ein Experience Lab für technologische Komponenten, Implementierungsplattformen, prototypische Anwendungen und Blaupausen für innovative Governance und Geschäftsmodelle auf. Es ist eine multidisziplinäre Einrichtung zur Konzeption, Entwicklung und Evaluation von Blockchain-Lösungen und hat seine Wurzeln in drei Forschungsbereichen des Instituts: computer-gestützte Gruppenarbeit für die Konsensfindung, Entscheidungsunterstützung für neue Governance mit Geschäftsmodellen, Wirtschaftsinformatik für Anwendungsinnovationen, sowie juristische Aspekte in Kooperation mit der Universität Münster. Ziel des Labors ist es, die aktuellen wissenschaftlichen Erkenntnisse auf dem noch jungen Forschungsfeld mit praxistauglichen, integrativen Anwendungen zu demonstrieren.

Dabei wird großer Wert auf kurze Entwicklungszyklen gelegt, um in kurzer Zeit und enger Abstimmung mit den Partnerunternehmen funktionierende Anwendungen zu entwickeln, die anschließend sukzessive in marktfähige Lösungen überführt werden. Die Entwicklung dieser individuellen und bedarfsgerechten Lösungen erfolgt in Ein- oder Mehrtagesworkshops, in angewandten Forschungsprojekten (von der Potenzialanalyse bis zur Implementierung) sowie in branchenweiten und -übergreifenden Konsortien.



Abbildung 3: Der multidisziplinäre Ansatz des Blockchain Labors

Die integrativen Lösungsangebote basieren auf der Trias aus Geschäftsmodell, Technologie und Recht. Die **Geschäftsmodell-Entwicklung** erfolgt kunden- und branchenspezifisch und umfasst die Potentialanalyse, Einordnung und Entwicklung von disruptiven Lösungen. Im Fokus der **Technologie-Implementierung** stehen die Bereitstellung einer Entwicklungsplattform mit unterschiedlichen Blockchain-Systemen (P2P-Netzwerk, Validierungsserver, etc.), die Implementierung von Blockchain-Lösungen sowie die Evaluation von Blockchain-Konzepten. Die **Rechtliche Betrachtung** umfasst die Beratung hinsichtlich zu berücksichtigender rechtlicher Aspekte sowie die Evaluation von Blockchain-Systemen und Geschäftsmodellen unter Berücksichtigung gültiger regulatorischer Vorschriften.

Ergebnis der Aktivitäten des Fraunhofer-Labors sind individuelle Lösungen in vielschichtigen Anwendungsgebieten auf Grundlage der Blockchain-Konzepte: Smart Contracts und dezentrale autonome Organisation für effizientere Governance und Prozesse. Beispielhafte Anwendungsgebiete sind Internet of Things, (Intellectual) Property Management, Börsenhandel, Vermögensverwaltung und Clearing-Prozesse.

4.2 Blockchain Security Lab - Sicherheit

Das Blockchain Security Labor dient dem Aufbau von Know-How, der Erforschung von Angriffen und der Entwicklung von Sicherheitstechnologien für Blockchain-basierte Anwendungen.

In der Praxis existiert nicht eine einzelne Blockchain-Technologie, sondern es werden ganze Stacks aus mehreren Technologie-Blöcken zusammengesetzt, auf deren Basis Blockchain-Anwendungen implementiert und ausgeführt werden können. Diese Stacks umfassen die eigentliche Peer-Software, Peer-to-Peer-Overlay-Protokolle, Consensus-Protokolle, BC-APIs und die eigentlichen Anwendungen. Durch die große Variantenvielfalt von Permissioned/Permissionless Ledgers mit verschiedenen Mining-Strategien bzw. Trust-Modellen ergibt sich eine ganze Landschaft von BC-basierten Anwendungen mit jeweils unterschiedlichen Eigenschaften.

Um deren Verhalten in verschiedenen Grenzsituationen zu evaluieren, bzw. ihre Korrektheit zu validieren, können mit dem Blockchain Security Labor entsprechende Infrastrukturen realistischer Größe aufgesetzt und typische Angriffe ausgeführt werden. Hierzu zählen u.a.

- 51%-Angriffe auf Blockchains mit PoW (Proof-of-Work)--basierten Consensus-Protokollen, bei denen ein Angreifer mit ausreichend Ressourcen selbst einen Konsens herbeiführen und damit Inhalte der Blockchain gezielt modifizieren kann
- Andere strukturelle Mehrheits-Attacken wie etwa „Selfish Mining“ wo eine Gruppe von Angreifern ihren Fund erstmals zurückhalten und ohne das Wissen der anderen Miner bereits anfangen den nächsten Block zu errechnen um sich somit einen Zeitlichen Vorteil zu verschaffen und einen höheren Gewinn zu erzielen bzw. Transaktionen zu manipulieren
- Bekannte Angriffe auf Peer-to-Peer-Netze, wie etwa die gezielte Manipulationen einzelner Knoten und Herbeiführen eines Fehlverhaltens der Mehrheit der validierenden Peers (Eclipse-Angriff)
- Untersuchung von Fehlern in Smart-Contract-Implementierungen oder den entsprechenden Ausführungsumgebungen
- Validieren der Korrektheit von Smart-Contract-Implementierungen

Das vorrangige Ziel des Blockchain Security Labors ist es, Kompetenz in Bezug auf Blockchain-Security aufzubauen, die zum einen in Dienstleistungen eingesetzt werden kann und zum anderen Grundlage für die Entwicklung von Sicherheitstechnologien für derzeit ungelöste Probleme der Blockchain-Technologie ist. Das Blockchain Security Labor umfasst daher drei Komponenten:

- Aufbau einer technischen Infrastruktur und Erprobung bekannter Angriffe
- Entwicklung sicherer Smart Contracts, Anwendung von Methoden formaler Verifikation auf Smart Contracts
- Erarbeitung Schulungsangebot für Industriekunden

Das Vorgehen sieht hier folgendermaßen aus: In einem ersten Schritt werden praktische Erfahrungen mit verschiedenen Blockchain-Technologien gesammelt und in der Theorie bekannte Angriffe in der Praxis nachvollzogen werden. Hierzu wird eine technische Infrastruktur aufgebaut werden, auf der im Anschluss Experimente und Angriffe nachgestellt werden, ohne dass der Aufwand für Aufbau und Konfiguration der Infrastruktur wiederholt anfällt. Die Infrastruktur erlaubt das einfache Aufsetzen und Deployment von Peers auf unterschiedlichen Blockchain-Stacks. Hierbei ist es wichtig, dass einzelne oder mehrere Peers im Blockchain-Netz mit modifizierter Software ausgestattet werden können, um nicht-kooperative Peers zu simulieren. Hierzu zählt auch Funktionalität zum Instrumentieren einzelner Peers und der gezielten Ressourcenverteilung. Weiter muss die Netzwerkkonfiguration dynamisch konfigurierbar sein, so dass Effekte von Angriffen oder ungleich verteilten Bandbreiten nachgestellt werden können, die Einfluss auf die Konsensfindung in der Blockchain haben.

4.3 Cybersicherheitsberatung

Fraunhofer SIT unterstützt Unternehmen und Einrichtungen dabei, Blockchain-Konzepte, -Projekte und -Systeme hinsichtlich IT-Sicherheit und Privatsphäre zu bewerten. Eine Sicherheitsanalyse des Fraunhofer SIT liefert frühzeitig, z. B. bereits in der Konzeptionsphase, wichtige Informationen über die Erreichbarkeit von Schutzziele der IT-Sicherheit und die Wirksamkeit von Maßnahmen zum Privatsphärenschutz. Zur

Verbesserung der Sicherheit von Software, IT-Diensten und IT-Systemen ist es dringend erforderlich, dass Sicherheit und Privatsphärenschutz von Beginn an bei der Entwicklung, also bereits in der Designphase, berücksichtigt wird und dann über dem kompletten Lebenszyklus der Designphase betrachtet wird. Die nachträgliche Absicherung von Schwachstellen ist schwierig und teuer, insbesondere wenn die Ursache tief in der Architektur des Systems liegt.

4.3.1 Dezentralität

Die Vorteile von Dezentralität und der Abwesenheit einer zu vertrauenden dritten Partei können durch das Blockchain-basierte Konsensus Verfahren aber beispielsweise auch durch byzantinische Protokolle erreicht werden. Eine Sicherheitsevaluation unterstützt die Entscheidung für das zu wählende Protokoll.

4.3.2 Transparenz aller Transaktionen

Bezüglich der Offenlegung von Information gilt es ebenfalls eine Abwägung zu machen: Dass alle Akteure Kenntnis über das Buchhaltungssystem der Blockchain erhalten, kann sowohl einen Gewinn als auch einen Verlust an Sicherheit und/oder Privatsphäre bedeuten - je nach betrachtetem Schutzziel und Anwendung. Herausragendes Schutzziel ist die Integrität bzw. Fälschungssicherheit.

4.3.3 Spezifische Angriffe auf Blockchains

In der Regel sind bei Blockchains mehrere Parameter für das erreichte Sicherheitsniveau je nach Schutzziel ausschlaggebend. So spielt beispielsweise die Anzahl der Akteure eine große Rolle, wenn evaluiert wird, wie leicht oder schwer Blockchain-spezifische Angriffe, wie der 51%-Angriff durchzuführen sind. Bezüglich Kryptowährungen zeigen Simulationen des Fraunhofer SIT auf, ab wann Performanz und erreichtes Sicherheitsniveau auseinanderlaufen, z. B. hinsichtlich der Angriffe double spending und selfish mining.

4.3.4 Code = Code?

Das Dogma (Program) Code = (Legal) Code, d.h. der Programmiercode setzt unumstößlich die Regeln für eine Blockchain auch für Konfliktfälle fest und kann nicht mehr korrigiert werden, muss kritisch betrachtet werden. Allein aus dem Grund, dass es unwahrscheinlich ist, dass Programme ab einer gewissen Anzahl von Zeilen keine Fehler enthalten. Wegen des Konsensusprinzips (mindestens die Hälfte der Akteure müssen eventuellen Änderungen zustimmen), ist es sehr empfehlenswert Regelwerke bereits bei der Einführung von Blockchains abzustimmen bzw. bekannt zu geben und sie agil änderbar über den gesamten Lebenszyklus zu konzipieren. Die Frage, was es bedeutet, wenn eine Minderheit sich nicht an die Beschlüsse der Mehrheit halten möchte, ist dabei höchst relevant (siehe bisherige Beispiele von hard-forks).

4.3.5 Kryptographie

Die in der Blockchain verwendeten Verfahren müssen hinsichtlich ihres aktuellen Sicherheitsniveaus (inklusive potenzieller Implementierungsschwächen), ihrer Änderungsfreundlichkeit und ihrer voraussichtlichen Zukunftssicherheit bewertet werden.

4.3.6 Klassische Angriffsvektoren auf IT-Systeme

Blockchains und die auf ihnen beruhenden Kryptowährungssysteme sind selbstverständlich den üblichen Angriffsvektoren auf Software und IT-Systeme unterworfen, beispielsweise Hackingangriffe auf Wallets (wo sind privaten Schlüssel gespeichert: "hot storage" vs. "cold storage"?) und Angriffe auf Tauschbörsen (z. B. Mt Gox, Cryptsy, Bitfinex-Hack).

4.4 Forensikberatung

Die proaktive Forensikberatung des Fraunhofer SIT folgt dem Grundsatz der "Forensic Readiness" – dies gilt selbstverständlich auch für Anwendungen der Blockchain. Die reaktive Forensikberatung im Blockchaintext richtet sich überwiegend an Strafverfolgungsbehörden.

Forensic Readiness bezeichnet die Vorbereitung auf die IT-forensische Aufklärung von Vorfällen und ermöglicht damit eine effektive und effiziente Reaktion bei zukünftigen Angriffen. Gerade bei einer recht jungen Technologie wie der Blockchain mit potenziell unbekanntem und je nach Anwendung sehr unterschiedlichen Angriffsvektoren ist eine Forensic Readiness von besonders hoher Wichtigkeit. Wiederholt liest man in Meldungen bezüglich Vorfällen und Angriffen, dass die Betroffenen "hiermit nicht gerechnet haben" und entsprechende Mechanismen, die eine Aufklärung erleichtern oder überhaupt ermöglichen würden, nicht eingesetzt wurden. Wenn auch viele zukünftige Angriffe nicht konkret vorhersehbar sind, so ist dennoch das Schadpotenzial – auch bisher unbekannter Angriffe – grundsätzlich abschätz- und kategorisierbar. Technische und nicht-technische Maßnahmen wie Versicherungen oder alternativer Risikotransfer können somit greifen. Das Fraunhofer SIT bietet hier seine langjährige Erfahrung in der IT-Forensik für eine effektive und effiziente Prävention und Risikobewertung an – insbesondere Unternehmen, deren Geschäftsmodelle auf der Blockchain-Technologie aufbauen und Anwender missionskritischer Informationstechnologie (z. B. Banken, Versicherungen, Energieversorger), die beabsichtigen neu in diese Technologie einzusteigen.

Ein weiterer Schwerpunkt liegt bei den Strafverfolgungsbehörden: Begründet durch Anzahl und Schweregrad der Vorfälle liegt das Interesse von Strafverfolgungsbehörden bezüglich Forensik für Blockchain-Systeme in Kryptowährungen und speziell in der damit verbundenen Aufklärung von Straftaten wie Erpressungen mittels Ransomware oder illegalen Handelsgeschäften im Darknet. Zwar erschwert die Pseudonymität von Transaktionen mit Kryptowährungen die Ermittlungen, allerdings steht den Behörden ein großes Portfolio an IT-forensischen Methoden nach dem Stand der Technik und Forschung zur Verfügung, um illegale Handlungen aufzuspüren. Die jeweiligen Methoden gilt es hinsichtlich ihrer Wirksamkeit einzuordnen, weiterzuentwickeln und zu bewerten.

Fraunhofer SIT steht den Behörden hier als bewährter Partner für die grundrechts- und gesetzeskonforme Aufklärung zur Verfügung. Das Fraunhofer SIT kann bei der Aufklärung von Straftaten Blockchain-Datenspuren im Darknet zugänglich machen und auswerten. Selbst wenn die Täter Mechanismen zur Forensikabwehr einsetzen, können Ermittler mit Unterstützung von Fraunhofer SIT oft an die gewünschten Daten gelangen. Bei einem solchen Vorgehen ist stets besonders darauf zu achten, dass der Beweiswert der Daten erhalten bleibt.

4.5 Wirtschaftlichkeit

Sicherlich ist eine der zentralen Fragen hinsichtlich der Implementierung von Blockchains auch die Frage nach ihrer Wirtschaftlichkeit. Eine Antwort auf diese Frage lässt sich pauschal nicht geben. Eine konzeptionell-architektonischen Betrachtung der Blockchain-Technologie lässt grundsätzlich die Frage offen, ob eine public Blockchain überhaupt unter wirtschaftlichen Aspekten dauerhaft funktionieren kann. Die Bitcoin Blockchain z.B. benötigt auf Grund der kommunikationsintensiven Proof-Verfahren und dem rechenintensiven Mining sehr viel Energie, um das System aufrechtzuhalten. Ein weiterer negativer Aspekt ist die redundante Datenhaltung, die sehr viel Speicherkapazität benötigt, der ebenfalls zu erheblichen Kosten führen kann. Darüber hinaus fallen in öffentlichen Projekten für Transaktionen (Datenspeicherungen) i. d. R. geringe Gebühren an, die durch Skalierungseffekte nicht zu vernachlässigen sind.

Sie ist u.a. vom Öffentlichkeitscharakter (public/private) der Blockchain und dem jeweiligen konkreten Anwendungsfall abhängig. Grundsätzlich bleibt festzuhalten, dass viele der privaten Blockchain-Lösungen Open Source Projekte sind und damit nicht an komplizierte Lizenzmodelle geknüpft. Zudem können durch Administrationen aufwändige Proof-Verfahren reduziert werden. Die Komplexität in heutigen Wertschöpfungsketten und -netzwerken erfordert zudem einen multidimensionalen Ansatz. Das Fraunhofer IML entwickelt hierzu eine Demonstrator-basierte Lösung, mit der eine End-to-End-Betrachtung entlang der Supply Chain für den spezifischen Anwendungsfall simuliert und berechnet werden kann. Dabei setzt Fraunhofer bei der Bewertung von nichtöffentlichen Systemen im Supply Chain Management und im Einkauf unterschiedliche Methoden ein.

Eine weitere Herausforderung der wirtschaftlichen Bewertung besteht in der Quantifizierung von Vertrauen. Wie bereits beschrieben, steht die Blockchain für eine Technologie, die das Vertrauensproblem lösen kann, welches heute in verschiedenen Wirtschaftszweigen durch gebührenpflichtige Dienstleistungen von Drittanbietern (Zahlungsdienstleister, Kreditkartenunternehmer) gewährleistet wird.

Somit bleibt festzuhalten, dass eine Business-Case-Aussage nur durch eine Betrachtung des konkreten Anwendungsfalls möglich ist. Die bereits genannten Aufwände, die bei der Implementierung und im Betrieb der Blockchain Technologie entstehen, sowie die direkten monetären Nutzenaspekte, die beispielsweise auf die Prozessoptimierung (u. a. durch Aufwandsreduktion, Beschleunigung manueller Prozesse) zurückzuführen sind, bilden die Grundlage für eine umfassende Business Case Bewertung.

Da die Vorhersage monetärer Größen in einem bestimmten Prognosezeitraum allerdings mit hoher Unsicherheit verbunden ist, ist es sinnvoll neben der reinen monetären Bewertung auch die (indirekten) qualitativen Nutzenpotenziale zur ganzheitlichen Betrachtung eines Business Case heranzuziehen. Diese könnten u.a. sein, Unternehmenswertsteigerung durch horizontale Vernetzung mit Wertschöpfungspartnern, Komplexitätsreduktion administrativer Prozesse, sicherere Transaktionsabwicklung, Schutz vor Manipulationen, engere Orientierung an regulatorischen Vorschriften etc.

Erweitert um den Einbezug potenzieller Risiken (u. a. aktueller Technologiestand, Folgen eines Systemausfalls, Hackerangriffe) kann der Einsatz einer Blockchain Technologie somit umfassend bewertet werden.

Das Fraunhofer IML entwickelt hierzu im eigenen Labor und im Dialog mit Industriepartnern den **Blockchain Business Case Kalkulator**. Dieser soll eine multidimensionale und interdisziplinäre Betrachtung der wirtschaftlichen Tragfähigkeit des Einsatzes der Blockchain-Technologie entlang der Wertschöpfungskette ermöglichen

und somit einen essentiellen Beitrag für die Absicherung der Investitionsentscheidung im Unternehmen leisten.

4.6 Industrial Data Space IDS

Die Industrial-Data-Space-Initiative verfolgt das Ziel eines internationalen Standards für Datensouveränität. Datensouveränität ist die Fähigkeit einer natürlichen oder juristischen Person zur ausschließlichen Selbstbestimmung über ihre Datengüter. Diese Fähigkeit ist eine Schlüsselvoraussetzung für Unternehmen in der digitalen Wirtschaft, weil sämtliche Smart-Service-Szenarien sowie viele innovative, digitale Geschäftsmodelle darauf beruhen, dass Eigentümer bzw. Besitzer von Daten ihre Daten in Geschäftsökosystemen austauschen können, aber gleichzeitig die Kontrolle über diese Daten nicht verlieren möchten.

Die Industrial-Data-Space-Initiative ist zurzeit als Forschungsprojekt und als Anwenderverein institutionalisiert. In dem Forschungsprojekt entwirft die Fraunhofer-Gesellschaft das Referenzarchitekturmodell und pilotiert es in verschiedenen Use-Cases. Das Projekt arbeitet eng mit dem Anwenderverein zusammen, der die Interessen der Industrie bündelt, Anforderungen einbringt und die Standardisierungen verantwortet. Das Referenzarchitekturmodell ermöglicht die informationstechnische Unterstützung der Datensouveränität. Es basiert auf Entwurfsprinzipien, welche die Umsetzung spezifischer Implementierungen leiten. Hierzu gehören u.a.:

Dezentrale Datenhaltung: Der Industrial Data Space ist ein dezentraler Datenraum ohne zwingende zentrale Datenhaltung, wie sie beispielsweise bei IoT-Cloud-Lösungen oder „Data Lakes“ zu finden ist.

Nutzungsbedingungen: Dateneigentümer und -besitzer müssen in der Lage sein, ihren Daten Nutzungsbedingungen mitzugeben, bevor sie austauscht werden. Im Sinne sogenannter „Sticky Policies“ müssen die Daten also selbst Information darüber mitführen, unter welchen Umständen sie von wem gelesen bzw. verwendet werden dürfen.

Vertrauensschutz: Alle Teilnehmer müssen vertrauenswürdig sein, d.h. sowohl Software, die den Zugang zum Industrial Data Space gewährt, also auch Unternehmen, die solche Software betreiben, sind zu zertifizieren. Die Kriterien der Zertifizierung definiert der Anwenderverein.

Geschäftsökosystem: Der Industrial Data Space manifestiert sich als virtueller Raum von Endpunkten. Die Endpunkte bilden verschiedene Rollen, etwa Datengeber, Datennutzer, Broker zur Vermittlung von Datenangebot und -nachfrage, eine Clearing-Stelle sowie Anbieter von „Data Apps“ und Identity Services.

Der Industrial Data Space ist also ein dezentraler Architekturentwurf zur Förderung der Datensouveränität in der digitalen Wirtschaft. Daten sind dabei ein eigenes Wirtschaftsgut, das in Geschäftsökosystemen ausgetauscht wird, das einen Wert hat und für dessen Austausch Zahlungsströme anfallen. Zahlungen basieren auf Datentransaktionen zwischen Datengebern und Datennutzern bzw. multilateral im Datennetzwerk. Damit Zahlungen für Daten abwickelt werden können, bedarf es einer Erfassung und Speicherung der entsprechenden Datentransaktionen.

Im Sinne des dezentralen Architekturparadigmas des Industrial Data Space stellt die Blockchain-Technologie als Konzept zur Dezentralisierung von Zahlungsverkehren grundsätzlich eine Variante zur Implementierung des Datentransaktionsmanagements

dar, das in den Aufgabenbereich der Clearing-Stelle im Industrial Data Space fällt. Der Einsatz von Blockchain-Technologie im Industrial Data Space ist zudem auch deswegen vielversprechend, weil insbesondere Anforderungen hinsichtlich Data Provenance und Data Traceability in Datennetzwerken gut zu den Blockchain-Eigenschaften passen.

Derzeit evaluiert die-Industrial-Data-Space-Initiative den Einsatz von Blockchains in Use-Cases für Datennetzwerke.

5 Zusammenfassung

Dieses Positionspapier untersucht die Blockchain-Technologie aus Sicht der Fraunhofer-Gesellschaft. Dazu wurden zunächst die relevanten Technikaspekte und die damit verbundenen Forschungsfragen untersucht. Dabei zeigt sich, dass die noch junge Technik in allen Bereichen noch grundlegende Forschungs- und Entwicklungs-Herausforderungen aufweist. Eine große Herausforderung wird die Modularisierung einzelner Blockchain-Konzepte und deren Kombination und Integration für eine anwendungsspezifische Blockchain-Lösung sein.



Abbildung 4: Technik, Anwendungen und Kompetenzen aus Sicht der Fraunhofer-Gesellschaft

Die Untersuchung von Anwendungsfeldern und Branchen, die von der neuen Technik am ehesten profitieren können zeigt, dass jeweils unterschiedlichen Eigenschaften der Blockchain für ein Anwendungsfeld relevant sind. Während für das Internet der Dinge vor allem die mit Smart Contracts verbundenen Automatisierungspotentiale wesentlich sind, ist es für Anwendungen aus den Bereichen Supply-Chain oder für Herkunftsnachweise die Irreversibilität der verwalteten Transaktionen. Zentral ist jedoch der Aspekt, dass die Blockchain eine große Relevanz für viele verschiedene Anwendungsbereiche außerhalb der Finanzbranche und vor allem auch unabhängig von Kryptowährungen hat. Zur Identifikation von Anwendungen, die für die Nutzung einer Blockchain geeignet sind liefert das Papier eine Kriterienliste.

Die Breite der Blockchain-Technologien als auch ihrer Anwendungen erfordert einen multidisziplinären Ansatz sowohl bei der Entwicklung der Basistechnologien als auch bei der Anwendungsentwicklung, der Wirtschaftlichkeitsberechnung und der Konzeption neuer Governance-Modelle. Die vielfältigen Kompetenzen der Fraunhofer-Institute

ermöglichen der Fraunhofer-Gesellschaft einen wesentlichen Beitrag bei der Weiterentwicklung und Anwendung der Blockchain-Technologie zu leisten.

6 Literatur

1. Martin Abadi, Mike Burrows, Mark Manasse, and Ted Wobber. 2005. Moderately Hard, Memory-bound Functions. *ACM Trans. Internet Technol.* 5, 2: 299–327. <https://doi.org/10.1145/1064340.1064341>
2. Adam Back. 2002. *Hashcash - A Denial of Service Counter-Measure*. Retrieved from <http://www.hashcash.org/papers/hashcash.pdf>
3. P. Baran. 1964. On Distributed Communications Networks. *IEEE Transactions on Communications Systems* 12, 1: 1–9. <https://doi.org/10.1109/TCOM.1964.1088883>
4. Neil Daswani, Hector Garcia-Molina, and Beverly Yang. 2003. Open Problems in Data-Sharing Peer-to-Peer Systems. In *Database Theory — ICDT 2003*, 1–15. https://doi.org/10.1007/3-540-36285-1_1
5. Dwork, Cynthia and Naor, Moni. 1993. Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology. In *CRYPTO'92: Lecture Notes in Computer Science*. 139–147. Retrieved from <http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.ps>
6. Ilias Giechaskiel, Cas Cremers, and Kasper Bonne Rasmussen. 2016. On Bitcoin Security in the Presence of Broken Crypto Primitives. *IACR Cryptology ePrint Archive 2016*: 167. Retrieved March 19, 2017 from <http://ai2-s2-pdfs.s3.amazonaws.com/2377/2e1eb97b39865aee0a3b3e83b0d87d0798ab.pdf>
7. Michael Hammer and James Champy. 1993. *Reengineering the Corporation: A Manifesto for Business Revolution*. Harper Business.
8. Hudson Jameson. Hard Fork No. 4: Spurious Dragon - Ethereum Blog. Retrieved March 16, 2017 from <https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/>
9. Sunny King and Scott Nadal. 2012. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper*, August 19. Retrieved March 19, 2017 from <http://peerco.in/assets/paper/peercoin-paper.pdf>
10. Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.* 4, 3: 382–401. <https://doi.org/10.1145/357172.357176>
11. Diego Ongaro and John Ousterhout. 2014. In Search of an Understandable Consensus Algorithm. In *Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference (USENIX ATC'14)*, 305–320. Retrieved March 16, 2017 from <http://dl.acm.org/citation.cfm?id=2643634.2643666>
12. M. Pease, R. Shostak, and L. Lamport. 1980. Reaching Agreement in the Presence of Faults. *J. ACM* 27, 2: 228–234. <https://doi.org/10.1145/322186.322188>
13. Johan Pouwelse, Paweł Garbacki, Dick Epema, and Henk Sips. 2005. The bittorrent p2p file-sharing system: Measurements and analysis. In *International Workshop on Peer-to-Peer Systems*, 205–216. Retrieved March 16, 2017 from http://link.springer.com/10.1007/11558989_19
14. Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved March 16, 2017 from <https://bitcoin.org/bitcoin.pdf>
15. Don Tapscott and Alex Tapscott. 2016. *Die Blockchain-Revolution: Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert*. Plassen Verlag.
16. Vincent Schlatt, André Schweizer, Nils Urbach, Gilbert Fridgen. 2016. *Blockchain White Paper: Grundlagen, Anwendungen und Potentiale*. Fraunhofer FIT. Retrieved from <https://www.fit.fraunhofer.de/blockchain>

17. Welzel C., Eckert K.-P., Kirstein F., Jacumeit V. 2017. *Mythos Blockchain: Herausforderung für den Öffentlichen Sektor*. Kompetenzzentrum Öffentliche IT. Berlin. Retrieved from www.oeffentliche-it.de/publikationen
18. Taieb Znati and Mehmod Abliz. 2009. A Guided Tour Puzzle for Denial of Service Prevention. In *Computer Security Applications Conference, Annual*, 279–288. <https://doi.org/10.1109/ACSAC.2009.33>
19. Whitepaper:Nxt. Retrieved from <https://nxtwiki.org/wiki/Whitepaper:Nxt>