Fraunhofer
FIT

FRAUNHOFER INSTITUTE FOR APPLIED INFORMATION TECHNOLOGY FIT

BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE

White Paper

BLOCKCHAIN: GRUNDLAGEN, ANWENDUNGEN UND POTENZIALE

WHITE PAPER

Autoren
Vincent Schlatt, André Schweizer, Prof. Dr. Nils Urbach, Prof. Dr. Gilbert Fridgen
Fraunhofer-Institut für
Angewandte Informationstechnik FIT
Projektgruppe Wirtschaftsinformatik
Wittelsbacherring 10
95444 Bayreuth

Empfohlene Zitierweise:
Schlatt, V., Schweizer, A., Urbach, N., and Fridgen, G. 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT

Bildquellen
Titelseite: © arrow/fotolia.de
Alle übrigen Abbildungen: © Fraunhofer FIT

Management Summary

Längst ist die Blockchain mehr als nur die Technologie hinter der Kryptowährung Bitcoin. Vielmehr wird die Technologie mittlerweile als die eigentliche Innovation erachtet, die Experten zufolge das Potenzial hat, etliche Bereiche der Gesellschaft, die weit über das Gebiet digitaler Währungen hinausgehen, zu verändern. Nicht zuletzt aufgrund der vielfältigen Einsatzmöglichkeiten rückt sie zunehmend in den Fokus der Öffentlichkeit.

Grundsätzlich ist die Blockchain ein elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die durch die Teilnehmer eines verteilten Rechnernetzes verwaltet werden. Im Rahmen der vorliegenden Studie werden Status Quo der Forschung aufgearbeitet, eine theoretische Einordung der Technologie vorgenommen, Blockchain-Anwendungen untersucht sowie die aktuellen Entwicklungen in der Praxis analysiert. Dazu hat das Fraunhofer FIT und seine Projektgruppe Wirtschaftsinformatik unter anderem eine Marktanalyse von Blockchain-Startups durchgeführt. Die Studie zeigt, dass die meisten aktuellen Anwendungen auf der Blockchain als manipulationssichere Datenstruktur und System zum Werttransfer aufbauen und hauptsächlich im Finanzsektor eingesetzt werden. Weitere Anwendungsbereiche sind aber auch in der Industrie, dem öffentlichen und juristischen Sektor sowie im Internet der Dinge zu finden.

Zusätzlich zur Vorstellung der Blockchain-Grundkonzepte, der unterschiedlichen Blockchain-Einsatzgebiete und der detaillierten Erläuterung verschiedener Blockchain-Anwendungen wurden Potentiale und Risiken der Blockchain sowie Hindernisse und Empfehlungen bei der Implementierung untersucht. Potentiale sieht die Forschung insbesondere in der hohen Datenintegrität, der großen Transparenz und der Programmierbarkeit von Transaktionen das Potential von Blockchain-Lösungen. Unter anderem werden die aktuellen Probleme hinsichtlich Skalierbarkeit, mangelnder Interoperabilität von Blockchain-Systemen und der hohe Energiekonsum einiger Konsensmechanismen als Risiken und Hindernisse bei der Einführung angeführt. Als Empfehlungen hinsichtlich Blockchain-Implementierungen ist der Literatur und aktuellen Praxisstudien zu entnehmen, dass die Kollaboration zwischen Unternehmen bzw. sogar branchenweite Konsortien als zielführend erachtet wird. Des Weiteren wird empfohlen bei Blockchain-Projekten auf spezifische Anwendungsbereiche zu fokussieren, um die Charakteristika und Vorteile und Nachteile der Technologie je Geschäftsfeld evaluieren zu können.

Insgesamt fällt die Bewertung der Blockchain in Wissenschaft und Praxis sehr positiv aus – der endgültige Einfluss der Technologie bleibt dennoch abzuwarten. Festzuhalten ist allerdings, dass die Blockchain viele neue und spannende Fragen in unterschiedlichsten Branchen und Bereichen der Wissenschaft aufwirft. Das Fraunhofer FIT und seine Projektgruppe Wirtschaftsinformatik werden weiterhin gemeinsam umfassende und wissenschaftlich fundierte Untersuchungen sowie die Erarbeitung von praxistauglichen Lösungen im Blockchain-Umfeld vorantreiben.

CONTENT

1. MOTIVATION

Fortschritte in der Entwicklung von Informations- und Kommunikationstechnologien sowie des Internets haben in den vergangenen Jahrzehnten eine Reihe an Innovationen ermöglicht, die einen großen Einfluss auf nahezu jeden Bereich der Gesellschaft haben (Loader und Dutton 2012). Besonders das 21. Jahrhundert hat eine Vielzahl disruptiver Innovationen hervorgebracht (Peters und Panayi 2015). Wie Christensen (1997) dargelegt hat, haben disruptive Innovationen das Potenzial, traditionelle Geschäftsfelder grundlegend in Frage zu stellen. Beispiele umfassen Social-Media-Innovationen (Peters und Panayi 2015), Crowdfunding-Plattformen (Haas et al. 2015) oder die digitale Währung Bitcoin (Vora 2015), die in den vergangenen Jahren in unterschiedlichen Kontexten Aufmerksamkeit in der Öffentlichkeit erregt hat (vgl. Kiviat 2015).

Mittlerweile weist das Bitcoin-Netzwerk eine Marktkapitalisierung von knapp 9 Milliarden US-Dollar auf (Blockchain.info 2016) und wird vielerorts als Zahlungsmittel akzeptiert (Eikmanns und Sandner 2015). Das Besondere an der Bitcoin ist, dass Transaktionen sowie die generelle Verwaltung der Währung durch ein verteiltes Computernetz und ohne den Einfluss einer zentralen Institution sicher durchgeführt werden können (vgl. Nakamoto 2008). Intermediäre, wie beispielsweise Banken, sind dabei somit überflüssig (Jacob et al. 2015).

Deshalb wird die zu Grunde liegende Technologie inzwischen häufig als der eigentliche innovative Durchbruch hinter Bitcoin erachtet: die Blockchain (Glaser und Bezzenberger 2015). Aufgrund ihrer Eigenschaften hat die Blockchain Experten zufolge das Potenzial, etliche Bereiche der Gesellschaft, die weit über das Gebiet digitaler Währungen hinausgehen, zu verändern (vgl. Giaglis und Kypriotaki 2014; Swan 2015; Tasca 2015; Wright und De Filippi 2015) und die nächste disruptive Innovation darzustellen (Peters und Panayi 2015).

Zahlreiche Unternehmen haben in den vergangenen Monaten damit begonnen, sich mit der Blockchain auseinanderzusetzen (Glaser und Bezzenberger 2015), und auch Risikokapitalgeber zeigen eine hohe Aktivität in dem Bereich (Bogart und Rice 2015). Eine Studie des World Economic Forum (2015) prognostiziert gar, dass in elf Jahren Transaktionen im Umfang von 10% des globalen Bruttoinlandsprodukts über die Blockchain gespeichert werden.

Bisher gibt es jedoch trotz der Vielzahl an Ansätzen und Initiativen in der Praxis sowie einer zunehmenden medialen Aufmerksamkeit vergleichsweise wenig wissenschaftliche Beiträge zu diesem Thema (Atzori 2015). Obwohl die Blockchain bereits im Umfeld der Finanzbranche (Lee 2016; Peters und Panayi 2015), betreffend ihrer technischen Aspekte (Becker et al. 2013; Croman et al. 2016) oder unter rechtlichen Perspektiven (Fairfield 2015; Kiviat 2015; Wright und De Filippi 2015) untersucht wurde, sind umfassende Untersuchungen über generelle Anwendungsbereiche der Technologie selten. In den wenigen vorhandenen Publikationen gehen die Autoren dabei stark exemplarisch vor und verzichten zudem auf eine übergeordnete Kategorisierung (vgl. Forte et al. 2015; Mattila 2016; Pilkington 2016; Tsilidou und Foroglou 2015).

Die vorliegende Studie setzt an diesem Punkt an und hat das Ziel, *die bestehende Literatur* aufzuarbeiten und zu analysieren, um *aktuelle sowie zukünftige Anwendungsbereiche der Blockchain* vorzustellen. Im Zuge dessen wurde auch *eine umfangreiche Marktanalyse über Startups mit Fokus auf die Blockchain* durchgeführt.

Die Studie ist dabei wie folgt gegliedert: Zunächst erfolgt im zweiten Kapitel eine grundlegende technische Erklärung der Blockchain. Im Rahmen dessen werden verschiedene Modelle vorgestellt sowie die Funktionsweise der Bitcoin-Blockchain detailliert beschrieben. Zudem wird eine Einordnung der Blockchain als Informationsinfrastruktur vorgenommen. Auf dieser Grundlage folgen im dritten Kapitel eine systematische Einordnung von Blockchain-Applikationen sowie eine Analyse des aktuellen Blockchain-Startup-Markts. Im darauffolgenden vierten Kapitel werden konkrete Anwendungsbereiche der Blockchain analysiert. Im fünften Kapitel werden die strukturellen Chancen und Risiken der Blockchain sowie Hindernisse und Empfehlungen hinsichtlich der Blockchain-Implementierung diskutiert. Den Abschluss des Papiers bilden eine Zusammenfassung sowie ein Ausblick auf weitere Einwirkungsmöglichkeiten und Forschungsfelder der Blockchain im sechsten Kapitel.

2. GRUNDLAGEN DER BLOCKCHAIN

Das folgende Kapitel stellt einen Überblick über wesentliche konzeptionelle und technische Grundlagen der Blockchain dar. Nach einer allgemeinen Definition der Blockchain erfolgt zunächst eine grundlegende Erklärung der technischen Funktionsweise. Anschließend werden verschiedene Ausprägungen aufgezeigt sowie eine Einordnung der Blockchain als Informationsinfrastruktur vorgenommen.

2.1 Wesentliche Bestandteile der Blockchain

Da die Blockchain erst am Anfang ihrer Entwicklung befindet, haben sich bisher keine einheitlichen Definitionen durchgesetzt (Mattila 2016; Swan 2015).

Condos et al. (2016) definieren eine Blockchain als ein elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die durch die Teilnehmer eines verteilten Rechnernetzes verwaltet werden. Aus dieser Definition wird deutlich, dass zwischen der Blockchain als Datenstruktur und dem zugehörigen Verwaltungssystem unterschieden werden muss.

Walport (2015) definiert eine Blockchain als eine Art Datenbank, in der Einträge in Blöcken gruppiert werden. Diese Blöcke sind in chronologischer Reihenfolge über eine kryptographische Signatur miteinander verknüpft (Bogart und Rice 2015; Walport 2015). Jeder Block enthält Aufzeichnungen valider Netzwerkaktivität seit dem Hinzufügen des letzten Blocks (Bogart und Rice 2015). Im Falle von Bitcoin umfasst dies beispielsweise die durchgeführten Transaktionen. Dabei grenzt Walport (2015) Blockchains von Distributed Ledgers ab, in denen Aufzeichnungen kontinuierlich, anstatt in Blöcken geordnet, gespeichert werden. In dieser Studie erfolgt aufgrund des anwendungsorientierten Fokus keine Differenzierung zwischen den Begriffen Blockchain und Distributed Ledger.

Die zugehörigen Verwaltungssysteme werden von Glaser und Bezzenberger (2015) als verteilte Konsenssysteme bezeichnet. Laut den Autoren beruhen derartige Systeme auf Kryptographie und Peer-to-Peer (P2P) Prinzipien, statt einer zentralen Autorität, um per Konsens eine netzwerkweite Verifikation des Status des Systems zu erreichen (Glaser und Bezzenberger 2015). In der vorliegenden Studie werden vergleichbare Systeme als Blockchain-Systeme bezeichnet.

Aus den obenstehenden Definitionen geht hervor, dass Blockchain-Systeme verteilte Systeme sind. Mullender (1990) schreibt, dass verteilte Systeme nicht exakt definiert, sondern vielmehr durch mehrere Eigenschaften charakterisiert werden können. Zunächst weisen sie mehrere unabhängige Rechner (Netzknoten) auf, die miteinander kommunizieren und sich synchronisieren. Der Ausfall einzelner Rechner beeinflusst andere Rechner dabei nicht. Zudem speichert jeder Netzknoten einen gemeinsamen Status des Systems, sodass der Ausfall einzelner Rechner nicht den (teilweisen) Verlust des Systemstatus impliziert. In Blockchain-Systemen werden die Daten der Blockchain in jedem Knoten (redundant) gespeichert.

Unter den von Glaser und Bezzenberger (2015) erwähnten Peer-to-Peer-Prinzipien können zudem die folgenden Eigenschaften zusammengefasst werden. Die Netzteilnehmer stellen Hardware-Ressourcen zur Verfügung, um Inhalte bzw. Leistungen des Netzwerks bereitzustellen (Schollmeier 2001). Zudem findet ein direkter Austausch zwischen den Knoten statt, d.h. es gibt keine zentrale Instanz zur Koordination der Kommunikation zwischen den einzelnen Netzknoten (Schoder und Fischbach 2002).

Ferner geht aus den zuvor genannten Definitionen hervor, dass Blockchain-Systeme Kryptographie anwenden. Diese, sowie der ebenfalls angesprochene Konsensmechanismus, mittels dessen die Netzknoten den Systemstatus koordinieren und der als die grundlegende Innovation hinter Blockchain-Systemen angesehen werden kann (vgl. Bogart und Rice 2015), werden im folgenden Abschnitt am Beispiel Bitcoin näher betrachtet.

2.2 Funktionsweise eines Blockchain-Systems am Beispiel Bitcoin

Zur Erklärung der grundsätzlichen Funktionsweise von Blockchain-Systemen wird in dieser Studie die Bitcoin-Blockchain herangezogen. Bitcoin ist als P2P-basiertes digitales Währungssystem zu verstehen, in dem Transaktionen ohne einen Intermediär vollzogen werden (Nakamoto 2008). Die Blockchain dient dabei als chronologisches Register aller vergangenen Transaktionen innerhalb des Bitcoin-Netzwerks (Badev und Chen 2014). Sie ist dezentral bei allen Teilnehmern des Netzwerks (Netzknoten) gespeichert und wird durch diese verwaltet (Franco 2015). Sogenannte Bitcoins (BTC) fungieren dabei als Rechnungseinheit (Badev und Chen 2014). Sichere Transaktionen und eine dezentrale Verwaltung der Blockchain werden über kryptographische Algorithmen ermöglicht (Badev und Chen 2014).

2.2.1 Kryptographische Grundlagen

Bitcoin baut auf zwei fundamentalen Konzepten der Kryptographie auf: Public-Key-Kryptographie bzw. digitalen Signaturen und kryptographischen Hash-Funktionen (Badev und Chen 2014; Böhme et al. 2015).

Das Konzept der Public-Key-Kryptographie wurde bereits 1976 von Diffie und Hellman (1976) eingeführt. Dabei wird durch einen Algorithmus ein mathematisch miteinander verbundenes Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel, generiert (Franco 2015). Dieses Schlüsselpaar kann zur Erstellung einer digitalen Signatur verwendet werden (Stallings 2003). Dazu unterschreibt bzw. kombiniert der Absender eine Nachricht mit seinem privaten Schlüssel, der nur ihm bekannt ist, und sendet die so entstandene signierte Nachricht an den Empfänger. Dieser kann die signierte Nachricht nun mit dem öffentlichen Schlüssel des Absenders prüfen und somit die Authentizität der Nachricht (falls die beiden Schlüssel korrespondieren) verifizieren (Badev und Chen 2014). Insgesamt lassen sich durch eine digitale Signatur drei Ziele erreichen. Da nur der Absender den privaten Schlüssel kennt, kann die Authentizität der Nachricht nachgewiesen werden. Außerdem kann der Absender nicht leugnen, die Nachricht signiert zu haben (Franco 2015). Ferner kann die Nachricht durch die asymmetrische Verschlüsselung nicht unbemerkt verändert werden, wodurch ihre inhaltliche Integrität gewährleistet wird (vgl. Stallings 2003).

Ferner nutzt Bitcoin eine kryptographische Hashfunktion. Eine Hashfunktion ist ein Algorithmus, der eine Zeichenfolge von beliebiger Länge in eine Zeichenfolge fixer Länge umwandelt; diese wird Hashwert genannt (Franco 2015). Eine Hashfunktion ist deterministisch, d.h. dieselben Eingangsdaten ergeben immer denselben Hashwert (Badev und Chen 2014). Zudem führt jede Veränderung der Eingangsdaten zu einem stark veränderten Hashwert (Condos et al. 2016).

Kryptographische Hashfunktionen besitzen zudem folgende drei Eigenschaften. Ausgehend vom Hashwert kann der ursprüngliche Dateninput nicht mit vertretbarem Aufwand bestimmt werden (Franco 2015). Es ist nicht möglich, mit vertretbarem Aufwand einen zweiten Dateninput zu finden, der denselben Hashwert ergibt. Gleichermaßen ist es nicht mit vertretbarem Aufwand möglich, zwei verschiedene Dateninputs zu finden, die denselben Hashwert ergeben (Schäfer 2003).

2.2.2 Transaktionen im Bitcoin-Netzwerk

Die Funktionsweise von Transaktionen im Bitcoin-Netzwerk soll an einem Beispiel verdeutlicht werden. Angenommen Alice möchte an Bob zwei Bitcoins (BTC) transferieren. Zu diesem Zweck nutzt sie ein so genanntes Wallet, eine Software mittels derer Alice ihre Bitcoins verwalten kann (Franco 2015). Zunächst wird darüber eine Nachricht mit den Transaktionsdetails erstellt – also zum Beispiel »Alice möchte zwei BTC an Bob überweisen«.

Im Bitcoin-Netzwerk existieren jedoch keine Konten bzw. Kontostände (Antonopoulos 2014). Es besteht lediglich eine öffentliche Liste aller bisher getätigten Bitcoin-Transaktionen (Bonneau et al. 2015) – die Bitcoin-Blockchain. Deshalb stellen auch Bitcoins selbst nur Referenzen früherer Transaktionen dar (Böhme et al. 2015). Da keine Konten existieren, werden Bitcoins an Adressen transferiert, die den Hashwert eines öffentlichen Schlüssels repräsentieren (Bonneau et al. 2015). Nur der Besitzer des zugehörigen privaten Schlüssels kann den Mittelbestand folglich verwenden (Franco 2015).

Die Nachricht, die Alice für die Transaktion erstellt, enthält also Transaktionsoutputs, die sich aus einem Betrag und der Adresse des Empfängers (Bob) zusammensetzen, und Transaktionsinputs, welche Outputs früherer Transaktionen an Alice (und somit ihre Bitcoins) referenzieren (vgl. Franco 2015). Um zwei Bitcoins an Bob zu überweisen muss Alice nun die Inputs mit den zugehörigen privaten Schlüsseln digital signieren, um ihre Kontrolle über die Mittelbestände nachzuweisen (vgl. Franco 2015). Die signierte Transaktion wird dann an das Netzwerk versandt (Antonopoulos 2014). Dieser Vorgang wird in Abbildung 1 als *Transaktionsdefinition* veranschaulicht.

Jeder Netzknoten innerhalb dieses Netzwerks enthält neben einer kompletten Kopie der Blockchain außerdem einen Cachespeicher (UTXO), der Transaktionsoutputs der Blockchain enthält, die noch nicht für neue Transaktionen weiterverwendet wurden, und eine Datenbank mit unbestätigten Transaktionen (also solchen, die noch nicht in die Blockchain aufgenommen wurden) (Franco 2015).

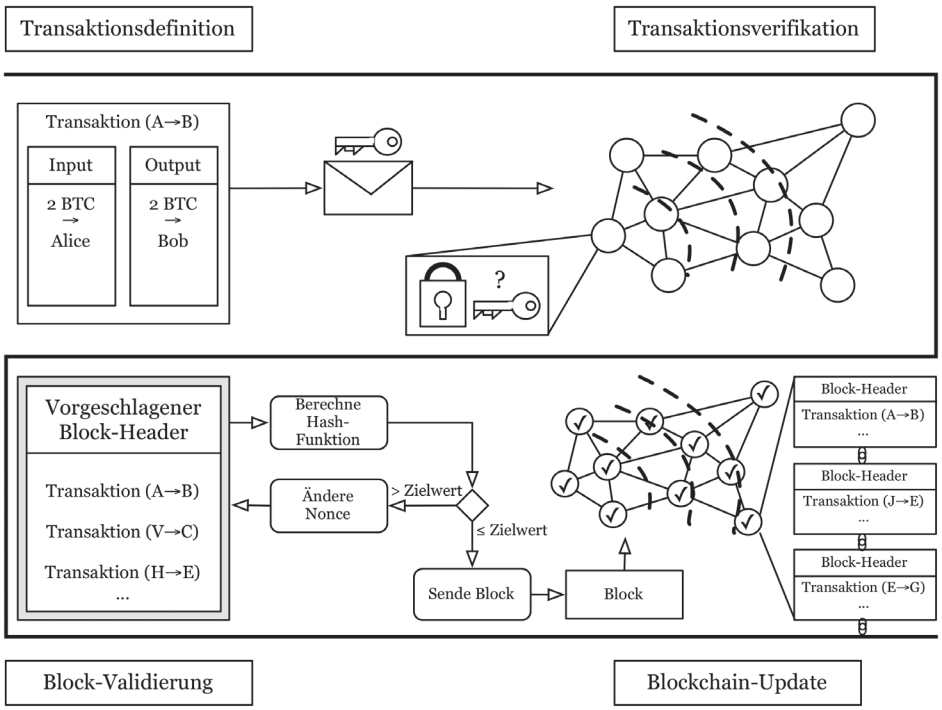

Abbildung 1:
Der Transaktionsprozess im Bitcoin-System (in Anlehnung an Burelli et al. 2015)

Der erste Netzknoten, den die Transaktion erreicht, prüft nun über den UTXO, ob die in der Transaktion referenzierten Inputs noch nicht für andere Transaktionen verwendet wurden (Franco 2015). Zudem wird überprüft, ob die Summe der Inputs größer oder gleich der Summe der Outputs ist und ob die digitalen Signaturen gültig sind (Franco 2015). Treffen diese drei Kriterien zu, leitet der Netzknoten die Transaktion an möglichst viele andere Knoten weiter, von denen die Transaktion dann jeweils überprüft und in die Datenbank mit unbestätigten Transaktionen aufgenommen wird (Franco 2015). In obenstehender Abbildung wird dieser Vorgang als *Transaktionsverifikation* dargestellt.

2.2.3 Aktualisierung der Blockchain

Im Bitcoin-Netzwerk gibt es zwei Arten von Netzknoten, so genannte Mining-Netzknoten und passive Netzknoten (Franco 2015). Während beide Typen jeweils Transaktionen annehmen, überprüfen und weiterleiten, können nur die Mining-Netzknoten dafür sorgen, dass eine Transaktion in die Blockchain aufgenommen wird (Franco 2015). Zu diesem Zweck fassen sie zunächst unbestätigte Transaktionen in einem Block zusammen, der neben den Transaktionen zusätzlich einen sogenannten Block-Header enthält (Antonopoulos 2014).

Bis zu diesem Punkt ergeben sich allerdings mehrere Probleme. Ein bösartiger Absender könnte widersprüchliche Transaktionen versenden, welche dieselben Transaktionsinputs an unterschiedliche Adressen transferieren; dies ist als das Double Spending Problem bekannt (Zohar 2015). Zudem ist es aufgrund von Unvollkommenheiten im Netzwerk möglich, dass Verzögerungen bei der Weiterleitung von Transaktionen auftreten oder Netzknoten abstürzen (Narayanan et al. 2016). Folglich können unterschiedliche Transaktionen in den jeweiligen Blöcken der Netzknoten enthalten sein.

Die Methode, mittels derer die Teilnehmer des Bitcoin-Netzwerks abstimmen, welcher Block als gültig angesehen und in die Blockchain aufgenommen werden kann, wird oft als die größte Innovation hinter Bitcoin angesehen (vgl. Bonneau et al. 2015; Zohar 2015). Durch einen Konsensmechanismus wurde eine Variante des in der Informatik lange bekannten Problems der byzantinischen Generäle, das durch Lamport et al. (1982) beschrieben wurde, gelöst (Zohar 2015). Das Problem beschreibt eine Situation, in der sich Generäle mittels Boten über einen gemeinsamen Schlachtplan einigen müssen, wobei einige Generäle bösartig sein könnten (Tschorsch und Scheuermann 2015). Somit ist es mit der Herausforderung im Bitcoin-Netzwerk vergleichbar (Tschorsch und Scheuermann 2015).

Das Bitcoin-Netzwerk löst das Problem der byzantinischen Generäle und erreicht den Konsens über ein sogenanntes Proof-of-Work (PoW) Schema (Zohar 2015). Dieser Vorgang wird in Abbildung 1 als *Block-Validierung* veranschaulicht. Generell soll das Proof-of-Work die übermäßige bzw. missbräuchliche Verwendung eines Dienstes verhindern. Das Erbringen eines PoW erfordert einen gewissen Aufwand, eine Art Benutzungsentgelt (Franco 2015); im Falle von Bitcoin muss dabei ein rechenintensives Problem gelöst werden (Bonneau et al. 2015). Der speziell in Bitcoin verwendete PoW stellt eine partielle Hashinversion dar, die auf dem Hashcash-Prinzip von Adam Back (2002) aufbaut (Franco 2015). Dabei muss ein Hashwert solange verändert werden, bis er mit einem bestimmten Muster übereinstimmt (Franco 2015).

Ein Mining-Netzknoten muss den Hashwert des Block-Headers so manipulieren, dass er kleiner als ein festgelegter Zielwert ist; vereinfacht gesprochen muss dieser mit einer gewissen Anzahl an Nullen beginnen (Narayanan et al. 2016). Der Block-Header enthält eine Referenz zum vorherigen Block in der Blockchain, den vorgegebenen Zielwert des Hash-Rätsels, einen Zeitstempel und eine Nonce, sowie die Wurzel eines Merkle-Baumes, der eine Datenstruktur darstellt, die alle in dem Block enthaltenen Transaktionen über Hashes effizient zusammenfasst (Antonopoulos 2014). Die Nonce, eine Zeichenfolge, die beliebig gewählt werden kann, muss nun so oft verändert werden, bis der Hash-Wert des Block-Headers unter dem vordefinierten Zielwert liegt (Zohar 2015). Der Mining-Netzknoten, der den entsprechenden Hash-Wert zuerst findet, sendet seinen Block an das Netzwerk; die Netzknoten berechnen nun ebenfalls den Hash-Wert und nehmen den Block, falls die Lö-

sung valide ist, in ihre Blockchain auf (Badev und Chen 2014). Folglich gilt eine Transaktion erst dann als vollzogen, wenn sie in die Blockchain aufgenommen wurde (Böhme et al. 2015). Dieser Vorgang wird in Abbildung 1 als *Blockchain-Update* veranschaulicht.

Da jedoch jeder Mining-Netzknoten individuell an der partiellen Hashinversion arbeitet, kann es vorkommen, dass zwei Knoten ihre Lösung beinahe simultan finden und versenden, wodurch kurzzeitig mehrere Versionen einer validen Blockchain im Netzwerk bestehen; dieses Phänomen wird als Gabelung bezeichnet (Tschorsch und Scheuermann 2015) und tritt bei ca. 1,69% aller Blöcke auf (Decker und Wattenhofer 2013). Um dieses Problem zu umgehen, arbeiten die Mining-Netzknoten so lange auf Basis ihrer jeweiligen Blockchain weiter, bis sie über eine längere Blockchain benachrichtigt werden (Zohar 2015). Die jeweils »längste« bekannte Blockchain[1] wird vom Netzwerk als richtig erachtet (Zohar 2015). Transaktionen, die nun möglicherweise nicht mehr in der aktuellen Blockchain enthalten sind, werden wieder in den Pool mit unbestätigten Transaktionen zurückgespeist (Antonopoulos 2014). Es besteht also die Gefahr, dass der Block mit Alice's Transaktion an Bob aufgrund einer Gabelung vernachlässigt und wieder in den Pool der unbestätigten Transaktionen verschoben wird, weshalb etwa sechs Blöcke ab der Transaktionsvollendung als angemessene Bestätigungszeit angesehen werden (Böhme et al. 2015).

Damit die Blöcke in einem relativ gleichmäßigen zeitlichen Abstand (derzeit ca. zehn Minuten) in die Blockchain aufgenommen werden, wird die Schwierigkeit des PoW regelmäßig automatisch entsprechend angepasst (Tschorsch und Scheuermann 2015). Als Anreiz, den PoW durchzuführen, erhalten die Mining-Netzknoten neben evtl. in den Transaktionen inkludierten Transaktionsgebühren für jeden gefundenen Block, der in die Blockchain aufgenommen wird, eine gewisse Anzahl an Bitcoins. Durch diesen Mechanismus werden zudem neue Bitcoins erzeugt und somit die Geldmenge erhöht (Zohar 2015).

[1]Tatsächlich adoptieren die Netzknoten die Blockchain, für die die höchste aggregierte Rechenleistung in Form des PoW aufgewendet wurde (Zohar 2015).

2.3 Alternative Ausprägungen von Blockchain-Systemen

Nachfolgend werden verschiedene technisch-konzeptionelle Modelle von Blockchain-Systemen vorgestellt. Zunächst lassen sich Blockchain-Systeme darin unterscheiden, ob sie *privat* oder *öffentlich* sind (Peters und Panayi 2015). Hierbei ist ausschlaggebend, durch wen sich die Systeme verwenden lassen, das heißt, wer Zugriff auf die Daten hat bzw. neue Dateninputs vorschlagen darf. Ist diese Verwendung jedermann gestattet, handelt es sich um ein öffentliches System; ist sie jedoch auf eine Organisation oder ein Konsortium beschränkt, ist das Blockchain-System als privat anzusehen (Peters und Panayi 2015).

Eine weitere mögliche Differenzierung unterschiedlicher Systeme besteht darin, ob zur Teilnahme am Verwaltungsprozess der Blockchain eine Genehmigung erforderlich ist (Walport 2015). Im Bitcoin-System umfasst dieser Prozess das Erbringen des PoW und ist jedermann *genehmigungsfrei* gestattet (Walport 2015). Sind die Netzknoten, die eine entsprechende Validierung durchführen, jedoch durch ein Konsortium oder eine zentrale Autorität vorher ausgewählt, so handelt es sich um ein *genehmigungsbasiertes* Blockchain-System (Peters und Panayi 2015). In diesem Fall sind ökonomische Barrieren, wie ein energieaufwendiger und folglich kostenintensiver PoW als Anreiz für korrektes Verhalten bei der Validierung hinfällig, weshalb effizientere Mechanismen zur Konsensfindung implementiert werden können (vgl. Mattila 2016). Das Ripple-Netzwerk beispielsweise weist eine erhöhte Effizienz auf, indem ausgewählte Netzknoten über den aktuellen Status des Systems abstimmen (Swanson 2014).
Aus diesen Unterscheidungskriterien lässt sich der Grad der Zentralisierung des jeweiligen Systems ableiten, wie in der nachfolgenden Graphik aufgezeigt wird.

Laut Peters und Panayi (2015) sind genehmigungsfreie Systeme in der Regel öffentlich, genehmigungsbasierte Systeme

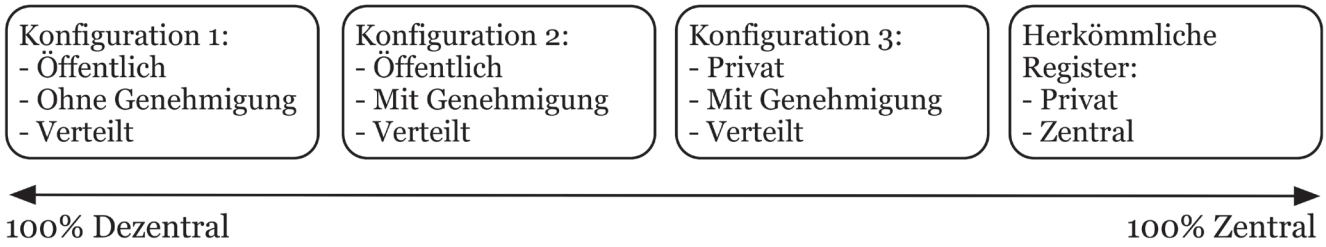

Abbildung 2: Der Grad der Zentralisierung verschiedener Blockchain-Systeme (in Anlehnung an Walport 2015, S. 35)

dahingegen in der Regel privat. Gemäß der BitFury Group (2016) funktionieren private Systeme ausschließlich genehmigungsbasiert.

Zudem können Systeme darin unterschieden werden, auf welche Weise ein Konsens über den Systemstatus erreicht wird. Neben dem im Bitcoin-System verwendeten Proof-of-Work existiert eine Vielzahl an Methoden. Eine Option ist beispielsweise die Verwendung eines Proof-of-Stake (PoS). Die Grundidee hierbei ist es, sicherzustellen, dass die Blockchain vornehmlich durch solche Netzknoten aktualisiert wird, die einen großen Anteil an der Währung (Narayanan et al. 2016) bzw. generell Werten in der Blockchain hält, wodurch ein Anreiz für eine korrekte Aufrechterhaltung des Systems bestehen soll. Weitere Alternativen umfassen unter anderem die Verwendung eines Proof-of-Activity, bei dem die Konzepte des PoW und PoS kombiniert werden und zudem ein Beweis für Aktivität innerhalb des Netzwerks von den Netzknoten erbracht werden muss (Bentov et al. 2014), eines Proof-of-Publication (Tschorsch und Scheuermann 2015) oder eines Proof-of-Storage (Narayanan et al. 2016).

In Swanson (2015) wird zudem eine Unterscheidung von Blockchain-Systemen nach ihrer Verwendung von Tokens aufgegriffen. Tokens dienen laut Pilkington (2016) als Wertbehälter; beispielsweise repräsentiert ein Bitcoin einen Token (Mainelli und Smith 2015). Diese Tokens stellen allgemein einen Anreiz zur Validierung der Blockchain dar. In genehmigungsbasierten Blockchain-Systemen sind deshalb keine Tokens notwendig, da die validierenden Netzknoten anderweitig vergütet werden (BitFury Group und Garzik 2015). Swanson (2015) argumentiert dahingegen, dass Tokens auch lediglich als Beleg für Netzwerkaktivitäten ohne Wertrepräsentation dienen können. Insgesamt wird die Notwendigkeit von Tokens in Blockchain-Systemen kontrovers diskutiert (vgl. Pilkington 2016). Es ist jedoch darauf hinzuweisen, dass auch Blockchain-Systeme ohne jegliche Tokens existieren (Swanson 2015).

Zudem existieren Methoden, um bestehende Blockchain-Systeme für andere Zwecke als die ihnen jeweils ursprünglich zugedachten zu nutzen. Ein Beispiel hierfür sind sogenannte Colored Coins. Diese sind als markierte Bitcoins zu verstehen, die allerdings andere Werte (z.B. den Goldpreis, definiert durch den Emittenten) als die ihnen zugrunde liegenden Bitcoins repräsentieren (Rosenfeld 2012).

2.4 Die Blockchain als Informationsinfrastruktur

Ølnes (2015) bemerkt, dass eine theoretische Einordnung der Blockchain als Informationsinfrastruktur (II) nach Hanseth und Lyytinen (2010) vorgenommen werden kann. IIs können sich laut den Autoren theoretisch ad infinitum weiterentwickeln, wodurch auch neue Anwendungsmöglichkeiten entstehen können (Hanseth & Lyytinen 2010). Folglich können sich in Anbetracht dessen auch derzeit unvorhersehbare Entwicklungen der Blockchain ergeben. Hanseth & Lyytinen (2010) definieren eine II als »a shared, open (and unbounded), heterogeneous and evolving socio-technical system [...] consisting of a set of IT capabilities and their user, operations and design communities.« (Hanseth und Lyytinen 2010, S.4). Tabelle 1 zeigt eine Einordnung der Blockchain als Informationsinfrastruktur.

Eigenschaft	II allgemein	Blockchain als II
Shared	Universally and across multiple IT capabilities (Star und Ruhleder 1996; Porra 1999).	Die Blockchain wird von allen Knoten, die mit dem Netzwerk verbunden sind, geteilt (Mainelli und Smith 2015). Die Nutzung des Systems ist dabei unabhängig von der Verwendung spezifischer Hardware (Bogart und Rice 2015)
Open	Yes, allowing unlimited connections to user communities and new capabilities (Weill und Broadbent, 1998; Kayworth und Sambamurthy 2000; Freeman 2007).	In öffentlichen, genehmigungsfreien Blockchain-Systemen (vgl. Punkt 2.3) ist die Teilnahme am Netzwerk jedem möglich (Peters und Panayi 2015). Somit kann jedermann über das offene Netzwerk neue Produkte und Anwendungen implementieren (Bogart und Rice 2015).
Heterogeneous	Increasingly heterogeneous both technically and socially (Kling und Scacchi 1982; Hughes 1987; Kling 1992; Edwards et al., 2007).	Seit der Implementierung im Rahmen von Bitcoin wurde die Blockchain für Anwendungen in diversen Bereichen verwendet (Peters und Panayi 2015). Zudem bestehen mittlerweile verschiedene technische Blockchain-Strukturen für unterschiedliche Zwecke (Peters und Panayi 2015).
Evolving	Yes, unlimited by time or user community (Star und Ruhleder 1996; Freeman 2007; Zimmerman 2007).	Bogart und Rice (2015) erwarten, dass sich durch die Blockchain ein weitreichendes Umfeld mit einer Vielzahl verschiedener Anwendungen entwickelt. Ølnes (2015) prognostiziert, dass sich die Blockchain unabhängig von Bitcoin weiterentwickeln wird.
Organizing Principles	Recursive composition of IT capabilities, platforms and infrastructures over time (Star und Ruhleder 1996; Edwards et al. 2007).	Im Umfeld der Blockchain haben sich bereits rekursive Beziehungen, wie Sidechains, die an andere Blockchains gekoppelt sind (vgl. Bogart und Rice 2015) oder die Verwendung von Kryptowährungen als Plattformen für andere Zwecke (vgl. Rosenfeld 2012) herausgebildet. Plattformen zur Entwicklung vielfältiger Applikationen sind entstanden (vgl. EBA 2015).
Control	Distributed and dynamically negotiated (Weill und Broadbent 1998).	Blockchain-Systeme sind per Definition verteilte Systeme (vgl. Glaser und Bezzenberger 2015). Somit gibt es in Blockchain-Systemen keine zentrale Autorität (Bogart und Rice 2015) und der aktuelle Status des Systems wird per Konsensmechanismus von den Netzteilnehmern ermittelt (Bogart und Rice 2015).

Tabelle 1: Die Blockchain als Informationsinfrastruktur (in Anlehnung an Hanseth und Lyytinen 2010 sowie Olnes 2015)

3. EINORDUNG VON BLOCKCHAIN-APPLIKATIONEN

Als Ausgangsbasis für die Analyse aktueller Anwendungen sollen zunächst verbreitete Kategorisierungen diskutiert sowie kritisch evaluiert werden. Die danach folgende Analyse aktueller Anwendungsbereiche wird durch die Ergebnisse einer ausführlichen Marktrecherche ergänzt und der Status Quo des aktuellen Blockchain-Startup-Markts umfangreich dargelegt.

3.1 Diskussion verschiedener Einordnungsansätzen

Jüngst entstanden Anwendungen der Blockchain, die weit über ihre erste Funktion im Rahmen von virtuelle Währungen wie Bitcoin hinausgehen (vgl. Peters und Panayi 2015). Da sich diese Anwendungsbereiche jedoch erst am Anfang ihrer Entwicklung befinden, bilden sich konsistente Klassifizierungen momentan noch heraus (Swan 2015) und fehlen in bisherigen Publikationen (vgl. Glaser und Bezzenberger 2015).

In einigen Kategorisierungen wird die Entwicklung von der ersten Implementierung im Rahmen digitaler Währungen wie Bitcoin hin zu anderen Anwendungsbereichen der Technologie systematisiert. Dabei wird zur Einordnung häufig zwischen den Phasen 1.0, 2.0 und 3.0 unterschieden (vgl. Duivestein et al. 2015; Burelli et al. 2015; Swan 2015). Während Phase 1.0 Währungen und damit verbundene Anwendungen im Bereich der Finanzdienstleistungen umfasst (Duivestein et al. 2015), werden in Phase 2.0 darüberhinausgehende Anwendungen in der Wirtschaft bzw. im Umfeld von Märkten und Finanzen eingeordnet (Swan 2015), wie beispielsweise Smart Contracts, die nachfolgend erläutert werden (Duivestein et al. 2015; Swan 2015). Phase 3.0 umfasst laut Swan (2015) Anwendungen über Finanzen und Märkte hinaus, beispielsweise im öffentlichen Sektor. Duivestein et al. (2015) sehen Phase 3.0 dahingegen in der Zukunft und nennen Dezentrale Autonome Organisationen (DAOs, siehe Kapitel 4.1.3) als beispielhafte Anwendung. Insgesamt erscheinen die Kategorien in dieser Einordnung nicht trennscharf und klare Abgrenzungskriterien werden durch die Autoren nicht definiert. Während Duivestein et al. (2015) für die dritte Phase nur zukünftige Anwendungen berücksichtigen, zitiert Swan (2015) auch bereits umgesetzte Beispiele. Aufgrund der fehlenden Trennschärfe und da mögliche zukünftige Anwendungen Gegenstand der Diskussion in Kapitel 4 sind, wird diese Kategorisierung nachfolgend nicht weiter berücksichtigt.

Eine weitere Kategorisierung wird von der Euro Banking Association (EBA) (2015) vorgeschlagen und zum Beispiel von Peters et al. (2015) aufgegriffen. Dabei umfasst die erste Kategorie ebenfalls Kryptowährungen. Die zweite Kategorie wird als »Asset Registration« bezeichnet und beschreibt die Verwendung öffentlicher Blockchain-Systeme, um diverse andere Positionen als die ursprünglichen Tokens zu repräsentieren (EBA 2015). Unter die nächste Kategorie fallen so genannte »Application Stacks«, die laut der EBA (2015) Plattformen zur Entwicklung und Implementierung von Blockchain-Anwendungen darstellen. Die letzte Kategorie bilden »Asset-Centric Technologies«, die gemäß der EBA (2015) den Austausch digitaler Repräsentationen diverser Objekte mittels privater Blockchains ermöglichen. An dieser Kategorisierung ist jedoch zu kritisieren, dass zur Einordnung nur inkonsistent technisch-konzeptionelle Aspekte

berücksichtigt werden; beispielsweise werden die Kategorien »Asset Registration« und »Asset-Centric Technologies« gemäß der EBA (2015) durch die Verwendung öffentlicher respektive privater Blockchains definiert, wobei die technisch-konzeptionelle Implementierung von Währungen nicht angesprochen wird. Insgesamt erscheinen die Kriterien zur Einordnung unklar. Während Währungen bereits eine konkrete Anwendung der Blockchain darstellen, so sind die übrigen Kategorien von konkreten Anwendungen abstrakt.

3.2 Einordnung nach William Mougayar

Die nachfolgende Untersuchung der Fintechs im Blockchain-Umfeld basiert auf der Kategorisierung von William Mougayar (2015). Dieser unterteilt das gesamte momentane Anwendungsumfeld der Blockchain in die Kategorien Infrastruktur und Plattformen, Middleware Services, Applikationen und Nebenleistungen. Diese Oberkategorien lassen sich wiederum granular in verschiedene Einzelbereiche unterteilen. Somit wird das gesamte aktuelle Umfeld der Blockchain in trennscharfen Kategorien abgebildet. Dabei wird weder eine zeitliche noch technische Einordnung, sondern lediglich eine funktionale Kategorisierung verwendet. Es ist zudem zu bemerken, dass die Oberkategorien aufeinander aufbauen bzw. sich gegenseitig bedingen.

3.2.1 Infrastruktur und Plattformen

Eine IT-Infrastruktur wird durch Duncan (1995) als eine Zusammenstellung mehrfach genutzter, konkreter IT-Ressourcen definiert, welche die Grundlage für Anwendungen bilden. Die genannten IT-Ressourcen umfassen dabei sowohl Hardware, als auch Betriebssysteme, Netzwerke und Telekommunikationstechnologie sowie grundlegende Daten und Anwendungen zur Datenverarbeitung (Duncan 1995). In Bezug auf die Blockchain fallen unter diese Kategorie unter anderem diverse Blockchain-Systeme selbst, Multi-Plattformen für die Entwicklung und Implementierung unterschiedlicher Anwendungen, die auf Blockchain-Systemen basieren, spezialisierte Hardware zur Durchführung des PoW sowie Kryptowährungen (Mougayar 2015).

Die zuvor erwähnte Programmierbarkeit der Transaktionen bestimmter Kryptowährungen, wie zum Beispiel Bitcoin (Barber et al. 2012), ermöglicht es, diese als infrastrukturelle Grundlage für Anwendungen wie beispielsweise Treuhandverträge zu verwenden (Barber et al. 2012). Zudem können einige Währungen, wie zuvor beschrieben, durch den Colored-Coins-Ansatz als Repräsentation diverser Objekte verwendet werden (vgl. Rosenfeld 2012) und somit wiederum als infrastrukturelle Grundlage dienen.

Eine weitere Kategorie, die unter dem Oberbegriff Infrastruktur und Plattformen einzuordnen ist, stellen Multiplattformen dar (Mougayar 2015). Aufbauend auf Kazan et al. (2014) kann eine digitale Plattform als proprietäre oder frei verfügbare, modular geschichtete, technologische Architektur definiert werden. Sie ermöglicht die Entwicklung innovativer Derivate, die in einem wirtschaftlichen oder gesellschaftlichen Kontext eingebettet werden (Kazan et al. 2014). Im Kontext der Blockchain können solche Plattformen unter die Kategorie der »Application Stacks« der EBA (2015) eingeordnet werden und sind somit als Plattformen für die Entwicklung und Implementierung dezentraler Blockchain-Applikationen anzusehen (Tasca 2015).

Ein Beispiel, das häufig in der Literatur genannt (vgl. EBA 2015; Forte et al. 2015; Koblitz und Menezes 2015; Pilkington 2016) und als das wichtigste Projekt seiner Art bezeichnet wird (Koblitz und Menezes 2015), ist Ethereum. Vereinfacht gesagt kann Ethereum als Generalisierung von Bitcoin angesehen werden (Jacob et al. 2015). Ethereum bietet eine universelle Blockchain in Verbindung mit einer Turing-vollständigen Programmiersprache mit dem Zweck, die Entwicklung und Implementierung von Applikationen zu ermöglichen, die von der Blockchain Gebrauch machen (Buterin 2014). Turing-Vollständigkeit bezeichnet in diesem Zusammenhang die Flexibilität

der Programmiersprache, jeden kryptographisch durchsetzbaren Vertrag zu entwerfen (Koblitz und Menezes 2015). Zur Verifikation von Transaktionen innerhalb des Netzwerkes verwendet Ethereum eigene Tokens, die ether genannt werden, sowie ein eigenes PoW-Schema (Buterin 2014).

3.2.2 Middleware Services

In diesem Kontext erscheint es sinnvoll, auf die Kategorie der Middleware Services überzuleiten. Middleware Services sind gemäß Bernstein (1996) universelle Services, die als Bindeglied zwischen Plattformen und Applikationen dienen. Sie erfüllen die Anforderungen einer Vielzahl von Applikationen in mehreren Bereichen (Bernstein 1996). Beispielsweise zählt das Konzept der Smart Contracts, die basierend auf Multiplattformen wie Ethereum implementiert werden können (Tasca 2015), gemäß Mougayar (2015) zu den Middleware Services. Eine detaillierte Beschreibung des Konzepts von Smart Contracts ist in Kapitel 4.1.2 einzusehen. Weitere Bereiche, die unter die Kategorie der Middleware Services fallen, umfassen beispielsweise Entwickler-Tools, wie Programmierschnittstellen zur Implementierung von Anwendungen basierend auf Blockchain-Systemen (vgl. Mougayar 2015).

3.2.3 Applikationen

Auf Basis der infrastrukturellen Grundlage sowie gegebenenfalls vorhandener Middleware Services lassen sich schließlich konkrete Applikationen umsetzen. Während das Konzept der Smart Contracts den Middleware Services zugeordnet wird, zählt die fallspezifische Implementierung der Smart Contracts zum Bereich der Applikationen.

Ein Anwendungsbeispiel ist die Registrierung digitaler und analoger Objekte in einer Blockchain. Am Beispiel des Unternehmens Everledger soll die Idee hinter dieser Art von Applikation illustriert werden. Everledger erstellt digitale Dokumente, die Informationen zur eindeutigen Identifizierung und über die Besitzverhältnisse von Diamanten enthalten und sichert diese in einem Blockchain-System ab. Die Blockchain stellt dabei für diverse Stakeholder eine verifizierbare Quelle dar, die Transparenz über die Historie der Diamanten bietet (Walport 2015). Organisationen können mittels der Blockchain nahezu jedes Objekt in der Blockchain abbilden und damit verbundene Informationen sichern (Walport 2015). Die Regierungen von Honduras und Georgien zeigen beispielsweise Interesse an einem Konzept zur Registrierung von Grundbucheinträgen in einer Blockchain, um Korruption zu verhindern (Bogart und Rice 2015). Hierbei ist anzumerken, dass lediglich die Hashes der Dokumente anstatt der Dokumente selbst in Blockchain-Systemen gespeichert werden. Die Dokumente müssen separat abgespeichert werden und können mittels der Blockchain lediglich auf ihre inhaltliche Integrität überprüft werden (Condos et al. 2016).

Der Hauptgrund, für diesen Zweck ein Blockchain-System zu verwenden, ist die Unveränderbarkeit der Daten in der Blockchain (Bogart und Rice 2015). Zudem kann der Transfer von Eigentum effizienter als bisher gestaltet werden, da die Blockchain eine schnelle, sichere und transparente Übertragung von Eigentum erlaubt, ohne auf die Hilfe eines Intermediäres angewiesen zu sein (Burelli et al. 2015; Wan und Hoblitzell 2014).

Ein Problem, das sich negativ auf die Umsetzung solcher Anwendungen auswirken könnte, ist dabei gemäß Peters et al. (2015) die Skalierbarkeit öffentlicher Blockchain-Systeme, wodurch die Anwendung in Bereichen mit einer hohen Anzahl an zu registrierenden Objekten limitiert ist. Mizrahi (2015) merkt zudem an, dass die eindeutige Identifizierung eines Objektes ein möglicher Schwachpunkt ist und eine vertrauenswürdige Partei für die Aufnahme des Objektes in die Blockchain notwendig ist.

Zusammenfassend lässt sich die Blockchain allgemein in jedem Bereich einsetzen, der die Erfassung, den Nachweis oder Transfer jeglicher Art von Kontrakt oder Objekt zum Gegenstand hat (vgl. Forte et al. 2015).

3.2.4 Nebenleistungen

In Ergänzung zu den zuvor erläuterten Kategorien werden zudem Nebenleistungen als vierte Kategorie im Anwendungsumfeld der Blockchain genannt. Diese Kategorie umfasst beispielsweise Dienstleister für die Bereitstellung von Marktdaten, Fachmedien oder branchenspezifische Kapitalgeber (Mougayar 2015). Zu den Nebenleistungen gehört beispielsweise die Internetseite CoinGecko, die einen Überblick über verschiedene Kryptowährungen liefert. Darüber hinaus ermöglicht die Webseite umfangreiche Vergleiche von Kryptowährungen (CoinGecko 2016). Neben Informationen über die Marktkapitalisierung und aktuelle Marktwertentwicklungen werden dort auch Messungen der Entwickleraktivitäten sowie Analysen des öffentlichen Interesses aufbereitet (CoinGecko 2016).

3.3 Status Quo des Blockchain-Startup-Markts

Um die exemplarische Darstellung der aktuellen Anwendungsbereiche in der Breite zu ergänzen, wurde eine Analyse von 222 Unternehmen aus dem Umfeld der Blockchain durchgeführt. Als Primärquelle diente die Plattform AngelList (2016b), die der Investorensuche für junge Unternehmen dient. Im Datensatz wurden Firmen berücksichtigt, die bis einschließlich April 2016 in die Plattform aufgenommen wurden. 25 weitere Firmen wurden durch eine individuelle Recherche ergänzt. Die Einordnung wurde auf Basis der Unternehmensbeschreibungen auf der Plattform bzw. den Internetauftritten der Unternehmen vorgenommen. Sofern keine ausreichenden Informationen zur Einordnung verfügbar waren, wurde ein entsprechender Hinweis gegeben. Unternehmen, deren Geschäftsmodelle einen reinen Bezug zu Bitcoin haben, wurden aus dem Datensatz entfernt. Dies hat den Hintergrund, dass ein breiter Überblick über das aktuelle Umfeld der Blockchain über Bitcoin hinaus gegeben werden soll. Aus demselben Grund wurden auch sonstige Kryptowährungen nicht beachtet. AngelList (2016a) listet zum Zeitpunkt der Abfassung dieser Studie 874 Unternehmen mit Fokus auf Bitcoin. Dieser Unterschied verdeutlicht, dass der Schwerpunkt bisher deutlich auf Bitcoin-bezogenen Innovationen lag, was vermutlich auf Netzwerkeffekte der Kryptowährung (Bogart und Rice 2015) zurückzuführen ist.

Der in der Abbildung 3 dargestellte Datensatz enthält 245 Datenreihen, da einige der 222 Unternehmen mehrere Produkte anbieten. Das linke Diagramm zeigt eine Einordnung der analysierten Produkte gemäß den adressierten Branchen. Wie daraus ersichtlich wird, stellen IT-Services nahezu ein Viertel aller Produkte dar. Die hierin am häufigsten vertretene Produktkategorie sind Entwicklertools. In diesem Zusammenhang ist auffällig, dass auch IT-Infrastruktur mit 8% aller Produkte stark als Branche vertreten ist. Eine mögliche Erklärung für diese Häufungen wird durch Bogart und Rice (2015) gegeben. Die Autoren beobachten, dass momentan noch die infrastrukturellen Grundlagen geschaffen werden, die zunächst notwendig sind, um ein vielfältiges Umfeld an Blockchain-Applikationen zu ermöglichen. Die ebenfalls auffallend häufig vertretenen Finanzprodukte werden nachfolgend ausführlich analysiert. Das rechte Diagramm in Abbildung 3 stellt eine Einordnung der Produkte in die unter Kapitel 3.2 verwendete Kategorisierung von Mougayar (2015) dar. Die Mehrheit bilden dabei Applikationen. Hierbei ist zu beachten, dass Kryptowährungen, welche die Zahl nochmals deutlich erhöhen würden, in der Analyse nicht berücksichtigt wurden. Weiterhin fällt auf, dass Nebenleistungen ein Viertel aller Produkte ausmachen. Dabei hat die Produktkategorie »Consulting & Services« mit 51% den größten Anteil. Dieses Angebot ist möglicherweise als Antwort auf eine große Unsicherheit über das Anwendungspotenzial der Blockchain (Bogart und Rice 2015) bzw. die geringe Vertrautheit von Entscheidungsträgern mit dem Konzept beispielsweise in der Finanzbranche (PwC 2016) zu erklären.

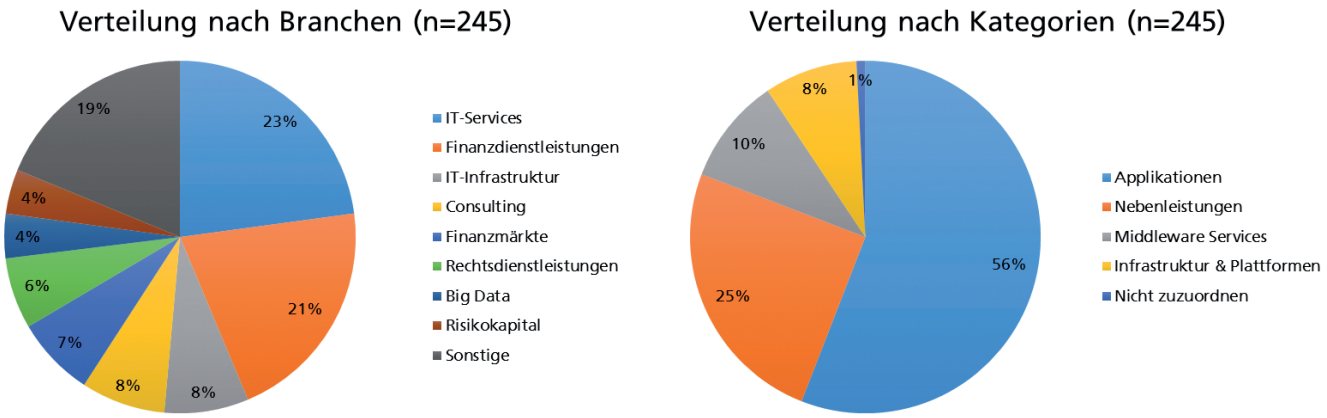

Abbildung 3: Verteilung der Unternehmen nach Branchen und Kategorien

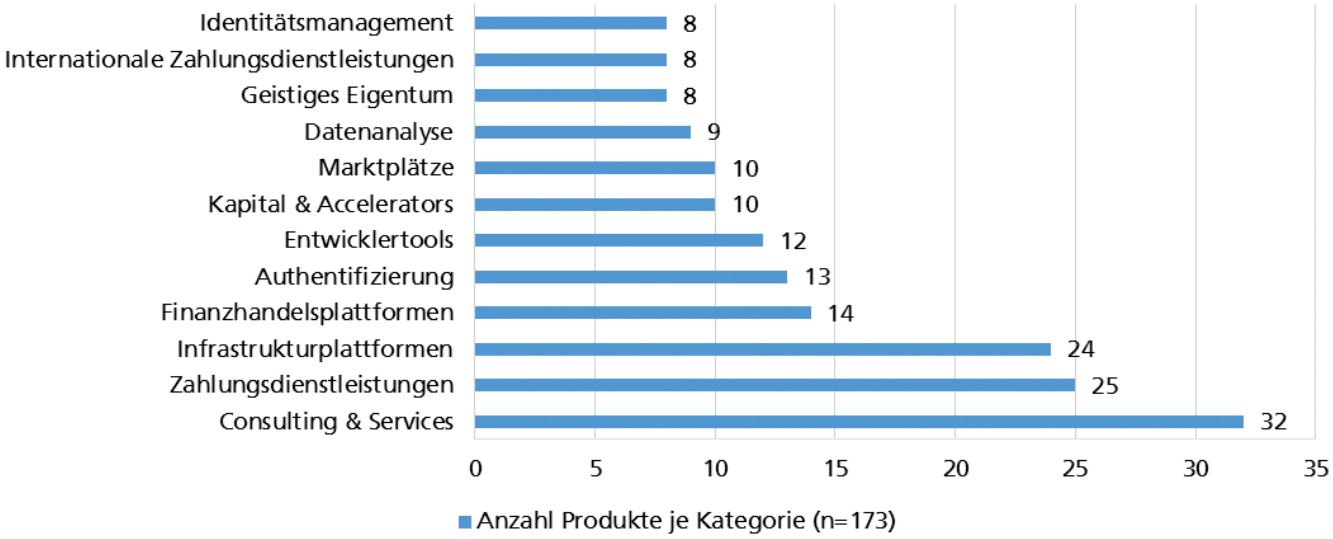

Abbildung 4: Die 12 häufigsten Produktkategorien

Obige Abbildung zeigt die zwölf am häufigsten vertretenen Produktkategorien. Insgesamt umfassen diese 173 Produkte, während sich die restlichen 72 Produkte auf 23 weitere Kategorien verteilen. Neben Beratungsleistungen und finanziellen Anwendungen fällt wiederum auf, dass Infrastrukturprodukte stark vertreten sind. Die Produktkategorie »Authentifizierung«, die auf Platz 5 rangiert, stellt eine Anwendung dar und baut auf der Eigenschaft von Blockchain-Systemen als unveränderbares Register auf. Ein exemplarisches Produkt ist die Authentifizierung von Diamanten durch Everledger, die in

Kapitel 3.2.3 vorgestellt wurde. Auffällig ist, dass die Mehrzahl der Anwendungen auf zwei Eigenschaften der Blockchain aufbauen: erstens auf ihrer Funktion als unveränderbares Register und zweitens als System zum Transfer von Informationen.

Von den analysierten Unternehmen haben 54% angegeben, ihren Standort in den USA zu haben, während 15% im Vereinigten Königreich ansässig sind. Die übrigen Firmen verteilen sich auf 27 Länder, während zu 7 Unternehmen entsprechende Daten fehlten.

Abbildung 3 zeigt bereits, dass die Finanzbranche, die in Finanzdienstleistungen und Finanzmärkte untergliedert ist, mit insgesamt 28% sehr stark vertreten ist. Wie aus Abbildung 5 hervorgeht, stellen Zahlungsanwendungen und Handelsplattformen die häufigsten Produktkategorien dar. Im Vergleich mit dem gesamten Datensatz fällt der Anteil an Nebenleistungen zu Gunsten von Applikationen deutlich niedriger aus. Eine mögliche Erklärung für diesen Unterschied ist, dass viele Beratungen und sonstige unterstützende Dienstleister zwar Dienste für die Finanzbranche anbieten, methodisch jedoch als eigene Branche eingestuft wurden. Aufgrund ihrer hohen Relevanz werden die Anwendungen der Blockchain in der Finanzbranche in Kapitel 4.2.1 umfangreicher als Anwendungen anderer Branchen analysiert.

Abbildung 5: Detailübersicht der Unternehmen im Bereich der Finanzwirtschaft

4. BLOCKCHAIN-APPLIKATIONEN

In Kapitel 4 werden zunächst drei Grundbausteine von Blockchain-Anwendungen vorgestellt. Diese Bausteine dienen dann als Grundlage für die detaillierte Beschreibung einzelner Anwendungen der Finanzbranche, des öffentlichen und juristischen Sektors sowie im Internet der Dinge. Es ist hierbei anzumerken, dass der Reifegrad einzelner Anwendung sehr stark schwanken kann und von einer ausschließlich konzeptionellen Überlegung bis hin zu marktreifen Produkten reicht.

4.1 Grundbausteine von Blockchain-Applikationen

In den nachfolgenden Abschnitten werden drei Bausteine (Kryptowährungen, Smart Contracts und DAO) vorgestellt, die häufig Bestandteile konkreter Blockchain-Applikationen darstellen. Zudem werden die Vor- und Nachteile von Kryptowährungen und Smart Contracts diskutiert.

4.1.1 Kryptowährungen

Währungen stellen die erste praktische Anwendung der Blockchain dar (Peters und Panayi 2015). Kryptowährungen existierten bereits 20 Jahre vor der Einführung von Bitcoin. Ihre Abhängigkeit von einer dritten Partei, die einen einzelnen Angriffspunkt bot, führte jedoch jeweils zu ihrem Scheitern (Forte et al. 2015). Durch die Verwendung der Blockchain wurde diese Schwachstelle im Bitcoin-System umgangen (Forte et al. 2015). So können Kryptowährungen auf der Basis der Blockchain, aufbauend auf Ahamad et al. (2013), als eine digitale Währung definiert werden, für die kryptographische Prinzipien, in der Regel gepaart mit einem PoW-Schema, verwendet werden, um die Währung zu erschaffen und zu verwalten. Ein dezentrales P2P-Rechnernetz erstellt und verifiziert dabei Transaktionen der Währung innerhalb des Netzwerks (Ahamad et al. 2013). Sie sind dabei in ihrem Wert nicht von einer Regierung oder Organisation gestützt (Ametrano 2014). Obwohl Bitcoin als die wichtigste Kryptowährung angesehen wird (vgl. Koblitz und Menezes 2015) und mit Abstand am weitesten verbreitet ist (Baur et al. 2015), existiert inzwischen eine Vielzahl an alternativen Kryptowährungen (Baur et al. 2015). Die Website coinmarketcap.com listet zum Zeitpunkt der Abfassung dieser Studie 751 Kryptowährungen mit einer kombinierten Marktkapitalisierung von annähernd $12 Mrd. auf (CoinMarketCap 2016). Die EBA (2015) nennt drei primäre Verwendungszwecke von Kryptowährungen: Spekulation, Online- bzw. Point-of-Sale-Transaktionen sowie Wertaufbewahrung. Obwohl die Frage, ob Kryptowährungen tatsächlich als Währungen anzusehen sind, kontrovers diskutiert wird (vgl. Peters et al. 2015), argumentiert Blundell-Wignall (2014), dass Kryptowährungen alle Bedingungen (Werterhaltung, Verrechnungseinheit und Zahlungsmittel) erfüllen, um als Währung anerkannt zu werden.

In der Forschung waren Kryptowährungen bisher vornehmlich Gegenstand der Untersuchung nach technischen, ökonomischen, regulatorischen und sozialwissenschaftlichen Aspekten (Baur et al. 2015). Im Umfeld von Kryptowährungen haben sich zudem diverse Geschäftsfelder entwickelt; die bedeutendsten werden exemplarisch anhand des Bitcoin-Systems in Böhme et al. (2015) aufgezeigt und umfassen z.B. Devisen-Händler. Ferner weisen die Autoren darauf hin,

Vorteile	Nachteile
Teilbarkeit in sehr kleine Einheiten (vgl. Godsiff 2015)	Hohe Fluktuation der Wechselrate von Kryptowährungen (Morabito 2016); Markt für digitale Währungen wird jedoch laut Tasca (2015) insgesamt effizienter, zum Beispiel stetige Abnahme der Volatilität von Bitcoin seit dem Jahr 2011
Geringe Transaktionskosten (Godsiff 2015) und -zeiten (Morabito 2016) durch die Umgehung von Intermediären	Probleme hinsichtlich des Konsumentenschutzes, beispielsweise da Transaktionen irreversibel sind (Morabito 2016).
Teilweise erhöhte Privatsphäre, da keine Bindung an Bankkonten, die einen Nachweis der Identität benötigen (vgl. Morabito 2016)	Instrumentalisierung des hohen Grads an Anonymität für kriminelle Aktivitäten (Morabito 2016): insbesondere Geldwäsche, die Bezahlung illegaler Güter oder Dienstleistungen und Terrorfinanzierung (HM Treasury 2014) sowie potenziell als Mittel zur Steuerhinterziehung (vgl. Marian 2013)
Unmöglichkeit der Fälschung von Kryptowährungen aufgrund der Eigenschaften der Blockchain (Morabito 2016)	Hackerangriffe möglich, sofern die Währungen online in sog. E-Wallets gespeichert werden (vgl. Morabito 2016)
Erhöhte Sicherheit aufgrund der Umgehung von Intermediären (Morabito 2016)	

Tabelle 2: Vor- und Nachteile von Kryptowährungen

dass damit involvierte Akteure als Intermediäre agieren und somit die Dezentralität innerhalb des Systems kompromittieren. Kryptowährungen bieten wesentliche Vor-, allerdings auch Nachteile gegenüber regulären, staatlichen Währungen, die in der folgenden Tabelle zusammengefasst aufgezeigt werden.

Die Regulierung von Kryptowährungen variiert von Land zu Land – Tasca (2015) verzeichnet drei generelle Haltungen bezüglich weltweiter Regulierung: ablehnend (z.B. Bangladesch oder Island), umstritten (z.B. China oder Thailand) und tolerant (z.B. USA oder Japan). Für eine ausführliche Übersicht verschiedener Regulierung weltweit (im direkten Bezug auf Bitcoin) ist auf den Report des Global Legal Research Center (2014) zu verweisen.

4.1.2 Smart Contracts

Bereits 1997 wurde das Konzept der Smart Contracts von Nick Szabo eingeführt (Wright und De Filippi 2015) und als computerbasiertes Transaktionsprotokoll definiert, das die Bedingungen eines Vertrages implementiert (Szabo 1997). Aufgrund ihrer Eigenschaften bietet die Blockchain erstmals ein geeignetes Medium zur Implementierung solcher Kontrakte (DeRose 2016; Wright und De Filippi 2015). Smart Contracts sind als Computerprogramme zu verstehen, die Entscheidungen treffen können, wenn bestimmte Konditionen erfüllt werden (Kõlvart et al. 2016). Dazu können durch den Smart Contract externe Informationen als Input verwendet werden, die dann über die festgelegten Regeln des Vertrages eine bestimmte Aktion hervorrufen (Tuesta et al. 2015). Die entsprechenden Skripte mit den Vertragsdetails werden zu

diesem Zweck in einer bestimmten Adresse der Blockchain gespeichert. Tritt das festgelegte externe Ereignis ein, wird eine Transaktion an die Adresse gesendet, worauf die Bedingungen des Vertrages entsprechend ausgeführt werden (Tuesta et al. 2015). Laut Swanson (2014) sind Smart Contracts folglich Hilfsmittel, mit denen menschliche Interaktionen automatisiert werden, indem Kontrakte durch Algorithmen ausgeführt, durchgesetzt, verifiziert und gehemmt werden können. Somit sind die Anwendungsmöglichkeiten sehr breit gefächert (Tsilidou und Foroglou 2015). Beispielsweise könnten Besitztümer wie Autos, Fahrräder oder Wohnungen über ein smartes Schloss und ein Blockchain-System ohne physische Schlüsselübergabe vermietet werden. Dazu legt der Besitzer die Kaution und Miete im Smart Contract fest. Darüber hinaus werden im Smart Contract Regeln für die Zugangs-/Nutzungsberechtigung hinterlegt (bspw. der Nutzer kann erst nach

Chancen	**Risiken**
Autonome Ausführung des Vertrages (Wright und De Filippi 2015); störende Eingriffe dritter Parteien in die Ausführung folglich nicht möglich (Juels et al. 2015)	Exakte und garantierte Ausführung eines Smart Contracts nach seiner Implementierung (Wright und De Filippi 2015); Unmöglichkeit des Rückzugs einzelner Vertragsparteien kann jedoch auch als Vorteil gesehen werden (vgl. Juels et al. 2015)
Vertragsausführung in Echtzeit (Wright und De Filippi 2015)	Hohe Abhängigkeit von dem jeweils ausführenden System (Walport 2015)
Geringe Vertrags-, Durchsetzungs- und Compliance-Kosten im Vergleich zu regulären Verträgen (Walport 2015); allgemein niedrigere Kosten der Ausführung, da Smart Contracts aufgrund ihrer Implementierung via Quellcode leicht zu standardisieren sind (Wright und De Filippi 2015)	Rechtliche Probleme, wie beispielsweise die Relation von Smart Contracts zu konventionellem Vertragsrecht oder dem Verbraucherschutz (Wright und De Filippi 2015); generell Frage der rechtlichen Verantwortung, da Verträge durch ein Computerprogramm anstelle einer rechtlichen Entität ausgeführt werden (Tuesta et al. 2015)
Möglichkeit, die Ausführung eines Smart Contracts von externen Ereignissen abhängig zu machen (Juels et al. 2015)	Einschränkung des Umfangs von Smart Contracts durch die Notwendigkeit, die jeweiligen Interaktionen durch Daten ausdrücken zu können (Peters et al. 2015; Tuesta et al. 2015)
Fairer Austausch zwischen zwei Vertragsparteien ohne intermediäre Partei möglich, selbst wenn sich die Vertragsparteien nicht gegenseitig vertrauen (Juels et al. 2015)	Maximale Vorteile von Smart Contracts bei der Verwendung durch viele Unternehmen, wobei jedoch zunächst ein Fachkräftemangel für die Implementierung auftreten könnte (Tuesta et al. 2015)
Minimierung der Interaktion zwischen den Vertragsparteien (Juels et al. 2015)	

Tabelle 3: Chancen und Risiken von Smart Contracts

Zahlung der Kaution und Miete das Schloss öffnen). Sämtliche Interaktionen mit dem Blockchain-System, wie das Ausführen von Zahlungen, der Austausch des digitalen Schlüssels oder das Öffnen und Schließen des smarten Schlosses, können vom Mieter und Nutzer mittels Smartphone ausgeführt werden. Die Zahlungseingänge, Berechtigungsverteilung und -verwaltung sowie die Kautionsrückzahlungen erfolgen transparent, sicher und unveränderbar über die Blockchain. Allgemeine Chancen und Risiken, die sich durch die Implementierung von Smart Contracts ergeben, sind in Tabelle 3 zusammengestellt.

4.1.3 Dezentrale Autonome Organisation

Im Hinblick auf zukünftige Anwendungsbereiche scheint es unerlässlich, das Konzept der Dezentralen Autonomen Organisation (DAO) einzuführen. Bisher hat sich noch keine einheitliche Definition einer DAO durchgesetzt (Swanson 2014). Duivestein et al. (2015) definieren eine DAO sehr generisch als ein dezentrales Netzwerk autonomer Subjekte, denen eine leistungsmaximierende Produktionsfunktion zugrunde liegt. In solchen DAOs können sowohl Menschen als auch Geräte miteinander kooperieren (Forte et al. 2015). Eine DAO ist folglich als eine neuartige Organisationsform anzusehen. Wird durch sie ein Profitziel verfolgt, so wird von einer DAC (Decentralised Autonomous Corporation) gesprochen (Van Valkenburgh et al. 2015). DAOs agieren dabei ohne menschlichen Einfluss; Handlungen der DAO beruhen vielmehr auf Geschäftsregeln und Prozessen, die durch Smart Contracts vorgegeben sind, sowie Besitzverhältnissen, die in einer Blockchain registriert sind (Duivestein et al. 2015; Forte et al. 2015). Sobald eine DAO über eine Blockchain implementiert worden ist, kann sie unter der Bedingung, ausreichende Ressourcen zu erhalten, unabhängig agieren und beispielsweise von Nutzern Kompensation für ihre Leistungen einfordern oder selbst für notwendige Ressourcen bezahlen (Forte et al. 2015). Schlüsselhalter, die als Anteilseigner verstanden werden können, können dabei über digitale Signaturen darüber abstimmen, ob Mittel der DAO verwendet werden oder der Quellcode verändert wird (Swanson 2014). Im Gegensatz zu herkömmlichen Organisationen liegt die Autorität, Entscheidungen treffen zu können, somit direkt bei den Anteilseignern (Swanson 2014). Durch die Eigenschaften von Blockchain-Systemen weisen DAOs laut Swanson (2014) Vorteile gegenüber Schwächen und Missbrauchsmöglichkeiten regulärer Organisationen auf. Jede Entscheidung kann transparent nachvollzogen werden und das Vertrauen liegt nicht bei einer zentralen Organisation, sondern vielmehr in dem der DAO zugrundeliegenden Quellcode, der offen überprüft werden kann (Wright und De Filippi 2015). Aufgrund ihrer Struktur werfen DAOs jedoch diverse Fragen hinsichtlich der Haftung und Verantwortlichkeit auf (Mainelli und von Gunten 2014). Die Diskussionen um DAOs haben in den letzten Monaten und Wochen nicht zuletzt durch den DAO-Hack und des anschließenden Ethereum-Hard Forks stark zugenommen. Beim DAO-Hack war es Unbekannten gelungen, eine Schwachstelle im DAO-Programmcode zu nutzen, um mehr als 3,6 Millionen ether auf das Konto einer Tochterorganisation der DAO zu transferieren (Siegel 2016). Durch einen Hard Fork der Ethereum Blockchain wurden tiefgehende Veränderung des Blockchain Protokolls vorgenommen und die Ausnutzung der DAO-Schwachstelle rückgängig gemacht (Siegel 2016). Ein konkretes DAO Anwendungsbeispiel wird durch Zhang und Wen (2015) beschrieben und in Kapitel 4.5 erläutert.

4.2 Die Blockchain in der Finanzbranche

Wie aus der Marktrecherche hervorgeht, bildet die Finanzbranche den Sektor mit der größten Aktivität unter den analysierten Unternehmen und Produkten. Dennoch bemerken Glaser und Bezzenberger (2015), dass etablierte Institutionen der Branche erst damit beginnen, das Potenzial der Blockchain für sich nutzbar zu machen. Während Condos et al. (2016) betonen, dass die Blockchain Finanzintermediäre theoretisch komplett ersetzen könnte, argumentiert die EBA (2015), dass sie auch existierende Finanzdienstleistungen signifikant verbessern kann. Eine Analyse der Santander Innoventures et al. (2015) stellt beispielsweise heraus, dass die Blockchain die Infrastruktur-Kosten von Banken in bestimmten Bereichen bis zum Jahr 2022 um $15-20 Milliarden pro Jahr verringern könnte.

In Anbetracht dieser Einschätzungen erscheint es sinnvoll, dass sich Marktteilnehmer intensiv mit der Blockchain auseinan-

dersetzen. Dennoch zeigt eine Studie von PwC (2016), für die weltweit 544 Top-Manager aus der Finanzbranche befragt wurden, dass 83% der Befragten höchstens moderat mit der Technologie vertraut sind. Um eine Einschätzung über den Einfluss der Blockchain auf die Branche zu ermöglichen, werden im Folgenden exemplarisch verschiedene Anwendungsbeispiele der Blockchain im Finanzsektor dargelegt.

4.2.1 Ausgewählte Anwendungsbeispiele

Die ausgewählten Anwendungsfälle orientieren sich dabei an den Ergebnissen einer Studie der Cofinpro AG und dem IT Finanzmagazin (2016), im Rahmen derer die Meinungen von 86 Akteuren der Finanzbranche hinsichtlich der Blockchain eingeholt wurden. Die Teilnehmer sehen die möglichen Vorteile vor allem in Bezug auf Schnelligkeit, Kosten und Transparenz. Eine Einschätzung der Befragten darüber, in welchen Bereichen die Blockchain die größten Potenziale hat, ist in der folgenden Abbildung illustriert.

Nachdem das Potenzial von Kryptowährungen, die auf Platz 2 der Einschätzungen rangieren, bereits zuvor ausführlich behandelt wurde, werden nachfolgend zunächst Anwendungen im Zahlungsverkehr betrachtet. Dieser Bereich wird mit einer Zustimmung von 74% der Befragten als der Vielversprechendste im Finanzsektor angesehen, was aber natürlich nicht zuletzt dem Erfolg der Bitcoin geschuldet sein dürfte.

4.2.1.1 Zahlungsverkehr

Momentane Zahlungsprozesse involvieren eine Vielzahl an Intermediären, wie Banken, Clearing-Stellen und Zentralbanken, und sind dabei sehr ressourcenintensiv (EvryLabs 2015). Zudem finden Abwicklungsprozesse aufgrund der vielen Intermediäre und unterschiedlichen Systeme aus Koordinations- und Kostengründen nicht kontinuierlich, sondern mehrmals pro Tag statt, wodurch zeitliche Verzögerungen entstehen (EBA 2015; EvryLabs 2015). Kiviat (2015) argumentiert, dass bisherige Probleme des digitalen Zahlungsverkehrs, wie hohe Kosten und lange Transaktionszeiten, durch die Blockchain gelöst werden können. Dies sei dabei für jegliche Währung möglich und nicht auf Kryptowährungen beschränkt. Der

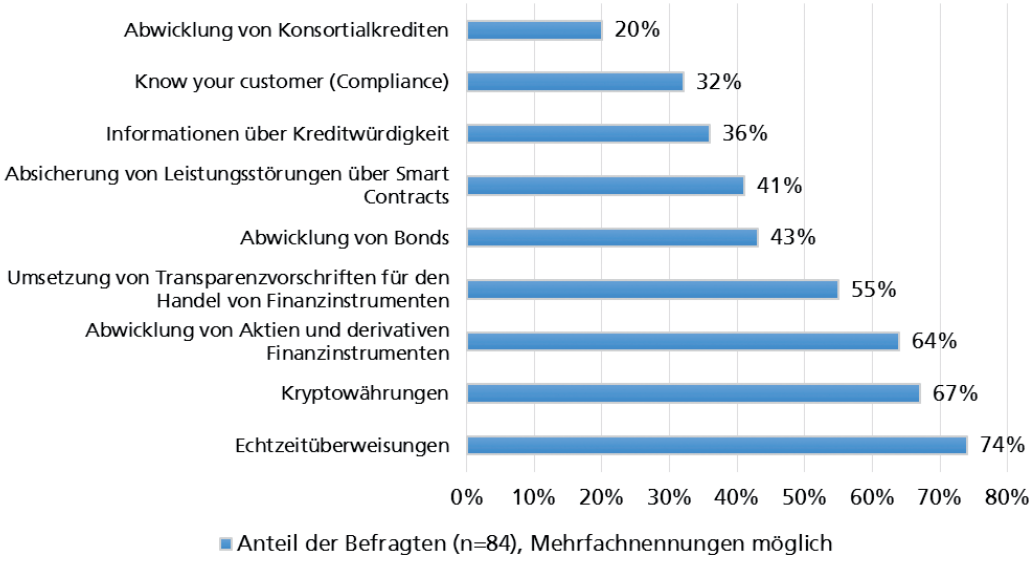

Abbildung 6: Potenzial der Blockchain in Anwendungsbereichen der Finanzbranche (Cofinpro AG und IT Finanzmagazin 2016)

größte Vorteil eines Blockchain-Systems scheint dabei zu sein, dass die Finanzpositionen einzelner Marktteilnehmer verlässlich in Echtzeit aktualisiert werden (vgl. EBA 2015).

Die Finanzbranche fokussiert sich dabei vor allem auf internationale Überweisungen (Geiling 2016). Hierbei fallen besonders hohe Gebühren an; Kiviat (2015) kalkuliert, dass die durchschnittliche Gebühr von 6% für internationale Überweisungen durch eine Blockchain-basierte Lösung auf 2% gesenkt werden kann. Zudem wird durch die kurze Abwicklungszeit das Wechselkursrisiko bei internationalen Transaktionen minimiert (Bogart und Rice 2015). Die Rolle der Blockchain als Zahlungssystem wird nachfolgend durch ein konkretes Beispiel illustriert.

Das Unternehmen Ripple bietet eine Zahlungsplattform an, die einen schnellen und nahezu kostenfreien Währungsumtausch sowie (internationale) Überweisungen ermöglicht (Pilkington 2016). Banken interagieren über das Netzwerk ohne eine zentrale Gegenpartei direkt miteinander (RippleLabs 2016). Durch ausgewählte Validierungsknoten wird der Konsensmechanismus und somit die gesamte Transaktionsabwicklung auf 5 bis 15 Sekunden reduziert (Swanson 2014). Über das Ripple-Netzwerk kann jegliche Währung transferiert werden; zu diesem Zweck wird ein nativer Token verwendet, der die entsprechende Währung repräsentiert. Dieser Token wird innerhalb des Systems transferiert und kann schließlich in Bitcoin und danach in beliebige Währungen umgetauscht werden (Swanson 2014). Ein weiterer Vorteil dieser Methode ist, dass lediglich Liquidität zwischen der jeweiligen Währung und dem Token, jedoch nicht zwischen den beiden gehandelten Währungen vorliegen muss, was insbesondere bei selten gehandelten Währungspaarungen vorteilhaft ist (EBA 2015). Gegenläufig zu der Grundidee der Dezentralisierung wird in einem Report von EvryLabs (2015) argumentiert, dass zur Realisierung internationaler Zahlungen über Blockchain-Systeme beispielsweise Devisen-Marktmacher involviert werden müssen. Über Partnerschaften mit Zahlungsdienstleistern, die als Schnittstellen fungieren und die gehandelten Währungen als Sicherheit halten, werden im Ripple-Netzwerk internationale Transaktionen ermöglicht (EvryLabs 2015). Dabei wird jeweils der Devisen-Marktmacher mit dem günstigsten Wechselkurs gewählt (EvryLabs 2015).

Während Ripple lediglich institutionelle Kunden bedient, existieren auch Lösungen für Konsumenten. Das Unternehmen Circle beispielsweise bietet eine App an, mittels derer Konsumenten kostengünstige und schnelle Zahlungen vornehmen können, wobei Bitcoins als intermediäre Tokens dienen (Silverberg et al. 2015).

Zusätzlich zu niedrigeren Gebühren können Blockchain-basierte Zahlungssysteme für Nutzer laut Bogart und Rice (2015) Sicherheit und Privatsphäre erhöhen, da Zahlungen auf dem Push-Prinzip beruhen: Kunden können Transaktionen aktiv initiieren ohne dabei Details wie beispielsweise Bankdaten bereitzustellen. Als Vorteile für Händler nennen Bogart und Rice (2015), dass Betrug durch Ausgleichsbuchungen (wegen der in Blockchain-Systemen inhärenten Transaktionsirreversibilität) verhindert wird sowie geringe Bearbeitungsgebühren und eine Kosten- und Risikominimierung, da Zahlungsinformationen von Kunden nicht gespeichert werden müssen.

4.2.1.2 Kapitalmarkthandel

Da Transaktionsprozesse im Kapitalmarkthandel eine große Anzahl an Akteuren involvieren (EvryLabs 2015), müssen kontinuierlich Daten abgeglichen und im Rahmen dessen Prozesse wiederholt werden (Van de Velde et al. 2016), weshalb hohe Kosten, lange Transaktionszeiten sowie operationale Risiken auftreten (McKinsey & Company 2015). Abbildung 6 zeigt, dass die Befragten mit einer Zustimmung von 64% vor allem in der Abwicklung von Wertpapiertransaktionen ein vielversprechendes Anwendungsfeld sehen.

Die Abwicklung von Wertpapiertransaktionen dauert in der Regel zwei bis drei Tage (Condos et al. 2016; Peters und Panayi 2015) und involviert mehrere Intermediäre (Bliss und Steigerwald 2006). Die lange Abwicklungszeit kann Kredit- und Liquiditätsrisiken hervorrufen (Condos et al. 2016) und erhöht des Weiteren das Kontrahentenrisiko (Peters und Panayi

2015). Peters und Panayi (2015) diskutieren in diesem Kontext den Einsatz einer zentralen Blockchain für ein Konsortium aus Finanzinstituten. Durch die Verwendung einer »Konsortiums-Blockchain« können die Kosten und die Komplexität in der Transaktionsabwicklung signifikant reduziert (Walport 2015) und die Abwicklungszeit auf Minuten bzw. Sekunden verringert werden (Peters und Panayi 2015), 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 (Condos et al. 2016; EvryLabs 2015). Das Kredit- und Liquiditätsrisiko wird laut McKinsey & Company (2015) effektiv eliminiert, da in Blockchain-Systemen aufgrund ihrer Funktionsweise der Besitz entsprechender Mittel vor dem Handel vorausgesetzt wird. Insgesamt besteht der Vorteil also darin, dass Abläufe effizienter gestaltet werden, da die Aufgaben von Intermediären, wie zum Beispiel die Absicherung des Kontrahentenrisikos, durch die Blockchain übernommen werden.

Aktuell wird in mehreren branchenweiten Initiativen an der Umsetzung einer solchen Lösung gearbeitet (Peters und Panayi 2015), wobei exemplarisch das Unternehmen SETL vorgestellt werden soll. SETL arbeitet an einer spezialisierten Blockchain-Infrastruktur, die es Marktteilnehmern erlaubt, Wertpapiertransaktionen direkt abzuwickeln (Walport 2015). Zu diesem Zweck bildet die SETL-Blockchain ein Register mit den Wertpapier- und Geldbeständen der Teilnehmer ab (Walport 2015). Der Abwicklungsprozess einer Transaktion geschieht dabei in Echtzeit. Durch das zentrale Register werden laut Walport (2015) außerdem zusätzlich die Gemeinkosten in Bezug auf die Registrierung und Verwaltung von Wertpapieren reduziert.

Geiling (2016) merkt jedoch an, dass die Transaktionsabwicklung diversen regulatorischen Bestimmungen unterliegt und derzeit noch nicht abschätzbar ist, inwieweit die Blockchain Risiken tatsächlich reduziert. Auch die DTCC (2016) kritisiert, dass die Realisierung von Echtzeit-Abwicklungen nicht von der Blockchain, sondern vielmehr von der Modernisierung aktueller Gesetze abhängt.

Im Umfeld des Kapitalmarkts findet die Blockchain zudem Verwendung, indem Unternehmensanteile in Blockchain-Systemen abgespeichert und verwaltet werden. Ein prominentes Praxisbeispiel dieser Anwendung ist die Plattform Nasdaq Linq (NASDAQ 2015). Um Besitzanteile zu registrieren und transferieren wird hierbei ein auf Bitcoin basierender Colored Coins Ansatz verwendet. Es ist dabei zu beachten, dass dabei nicht der tatsächliche Wert der Anteile in Bitcoins abgebildet, sondern lediglich eine Information über den Wert der Anteile repräsentiert wird (EvryLabs 2015). Die Implikationen dieses Anwendungsfalles für unterschiedliche Stakeholder werden in Yermack (2015) diskutiert, wobei vor allem Transparenz sowie der vereinfachte Handel mit Anteilen Gegenstand der Diskussion sind.

4.2.1.3 Compliance

Insbesondere in der Finanzwirtschaft findet Blockchain auch Anwendung im Bereich der Compliance. In diesem Rahmen werden vor allem zwei Einsatzmöglichkeiten der Blockchain diskutiert: zum einen als zentrales Register zur konsolidierten Buchführung und zum anderen wiederum als »Konsortiums-Blockchain« für Kundendaten.

Peters und Panayi (2015) beschreiben ersteren Anwendungsfall im Bankwesen. Dabei stellen die Autoren zunächst dar, dass Banken aktuell eine Vielzahl unterschiedlicher Kontenbücher für verschiedene Zwecke unterhalten und diverse Maßnahmen implementieren, 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-Systemen können diese Prozesse laut Peters und Panayi (2015) weitgehend automatisiert werden. McKinsey & Company (2015) schreiben, dass die Blockchain die vertrauenswürdige Konsolidierung einzelner Kontenbücher in ein Datenmodell ermöglicht. Nützlich erscheint hierbei besonders die Umgehung des Double-Spending-Problems in Blockchain-Systemen (vgl. Kapitel 2.2.3). Manipulationen in der Buchhaltung wie das Zurückdatieren von Verträgen auf andere Perioden, können laut Yermack

(2015) durch die Irreversibilität und zuverlässigen Zeitstempel von Transaktionen verhindert werden. Das Unternehmen Balanc3 verwendet die Eigenschaften der Blockchain bereits, um entsprechende Buchhaltungssysteme mit hoher Datenintegrität anzubieten (Peters und Panayi 2015).

Die Erfüllung diverser Gesetze und Regelungen zur Geldwäscheprävention wie beispielsweise »Know Your Customer« (KYC) birgt für Finanzinstitute hohe Kosten und verzögert Transaktionen teilweise maßgeblich (Deloitte 2016). Zudem werden KYC-Prozesse in unterschiedlichen Finanzinstituten jeweils individuell durchgeführt (Deloitte 2016). Ein branchenweites Kundenregister basierend auf einem Blockchain-System könnte laut Deloitte (2016) den mehrfachen Aufwand hinsichtlich der KYC- Überprüfungen eliminieren sowie die verschlüsselte Übertragung von Kundendaten erleichtern (Deloitte 2016). In Kombination mit der Verwendung von Smart Contracts könnten außerdem diverse Aspekte automatisiert werden. Als Beispiel hierfür führt Deloitte (2016) an, dass Zahlungen nur an Kunden mit ausreichender KYC-Historie zugelassen werden. Obwohl einige Unternehmen bereits KYC-Lösungen für Banken anbieten (Deloitte 2016) existiert eine entsprechende Konsortiums-Lösung nach bestem Wissen der Autoren noch nicht, weshalb der Anwendungsfall nicht weiter betrachtet wird.

4.2.1.4 Weitere Anwendungsmöglichkeiten

Andere Anwendungsfälle, die im Rahmen der Finanzwirtschaft diskutiert werden und teilweise bereits umgesetzt wurden, umfassen den Einsatz im Rahmen von Zentralbanken (Peters und Panayi 2015; Winkler 2015), Handelsfinanzierung (EvryLabs 2015) und Interbankenhandel (Geiling 2016). Für einen Überblick über mögliche Anwendungsfälle von Smart Contracts in der Finanzbranche, zum Beispiel für automatische Derivate, sei auf den Report von Tuesta et al. (2015) verwiesen.

Weitergehend diskutieren einige Autoren außerdem die Möglichkeit, gesamte Finanzmärkte basierend auf Blockchain-Systemen aufzubauen. Wie zuvor erwähnt, sehen Condos et al. (2016) die Möglichkeit, dass sämtliche herkömmlichen Prozesse im Rahmen von Finanztransaktionen mittels der Blockchain durch ein System ersetzt werden, in dem Teilnehmer direkt miteinander handeln. MacDonald et al. (2016) analysieren in diesem Kontext die Blockchain nach ökonomischen Theorien und kommen zu dem Schluss, dass die Blockchain mehr als eine neuartige Technologie darstellt, die durch Banken angewendet wird, um Prozesse zu verbessern. Vielmehr konkurriert sie laut den Autoren mit traditionellen Banken, indem ökonomisch effiziente Finanztransaktionen über dezentrale Blockchain-Systeme durchgeführt werden können.

Lee (2016) entwickelt das konkrete Beispiel eines alternativen Kapitalmarkts basierend auf einem Blockchain-System und untersucht mögliche Auswirkungen. In Lees Konzept werden Firmenanteile über ein Blockchain-System ausgegeben, verwaltet und gehandelt. In Kapitel 3 wurde bereits beschrieben, wie die Verwaltung von Unternehmensanteilen über ein Blockchain-System umgesetzt wurde (vgl. NASDAQ 2015). Während die Plattform in diesem Fall durch NASDAQ als zentrale Partei eingesetzt und verwaltet wird, ist Lees Plattform für einen direkten Handel konzipiert. Lee (2016) bemerkt dazu, dass ihr Konzept als alternativer Markt zu dem bestehenden Kapitalmarkt entworfen wurde und diesen nicht ersetzen soll. Als Vorteile eines solchen alternativen Marktes zählt Lee (2016) unter anderem erhöhte Transparenz, die Möglichkeit durchgehend zu handeln, schnelle Abwicklungszeiten und verringerte Transaktionskosten. Die Umsetzung eines Szenarios des direkten Finanzhandels kann jedoch als fragwürdig angesehen werden. McKinsey & Company (2015) bemerken dazu, dass die Blockchain bisher keine Preisfindungsmethode oder vollständige Anonymität bieten kann. Diese essentiellen Leistungen werden traditionell durch Börsen übernommen (McKinsey & Company 2015).

Die Blockchain eröffnet darüber hinaus möglicherweise neue Geschäftsfelder für Finanzdienstleister. So könnten Kryptowährungen als Investitionsvehikel verwendet werden. Briere et al. (2013) zeigen, dass durch eine Aufnahme von Bitcoins in ein Investmentportfolio signifikante Diversifikationseffekte realisiert werden können, da nur eine geringe Korrelation zu klassischen Investments besteht.

Wright und De Filippi (2015) bemerken überdies, dass die Blockchain die Einführung von Mikrozahlungen für Onlinedienste ermöglichen könnte. Somit könnten die Urheber von Onlineinhalten durch die geringen Transaktionskosten in Blockchain-Systemen Gebühren per Aufruf zum ersten Mal effizient realisieren. Als Folge könnte sich laut den Autoren die Abhängigkeit von werbebasierten Einkommensmodellen verringern. Diese Mikrozahlungen könnten zudem Probleme wie Spam oder die Bezahlung von Inhalt-generierenden Nutzern lösen (Wright und De Filippi 2015).

4.3 Die Blockchain im öffentlichen Sektor

Abgesehen von der Verwendung in Bereichen der Wirtschaft, wie beispielsweise im Rahmen neuer Organisationsformen oder alternativer Finanzmärkte, wird zudem eine mögliche Rolle der Blockchain im öffentlichen Sektor diskutiert (vgl. Ølnes 2015). In der Literatur werden hierbei vornehmlich zwei verschieden disruptive Szenarien beschrieben: zum einen die Idee, gesamte Staaten vergleichbar mit einer DAO über Blockchain-Systeme zu organisieren, sowie zum anderen die Möglichkeit, mittels der Blockchain einzelne Bereiche des öffentlichen Sektors effizienter zu gestalten. Hinsichtlich letzteren Szenarios erwarten beispielsweise 73% der 816 vom World Economic Forum (2015) befragten Experten aus der globalen IT-Branche, dass in den kommenden 10 Jahren erstmalig Steuern durch eine Regierung über ein Blockchain-System eingezogen werden. Dieses Anwendungsbeispiel wird auch von Walport (2015) aufgegriffen und als technologisch bereits möglich eingestuft. Als Vorteile werden z.B. eine erhöhte Transparenz und eine Verringerung der administrativen Kosten in Bezug auf die Bezahlung und Einforderung von Steuern genannt. Walport (2015) identifiziert dabei hauptsächlich die adäquate Ausbildung relevanter Beteiligter im Umgang mit der Blockchain als Hindernis. Überdies werden in Walport (2015) diverse weitere Anwendungsfälle der Blockchain im öffentlichen Sektor, die von transparenteren internationalen Zahlungen zur Entwicklungshilfe über konditionale Sozialhilfeleistungen reichen, diskutiert. Insbesondere in Ländern, in denen Korruption und Ineffizienzen in der Verwaltung ein Problem sind, erscheint die Implementierung von Blockchain-Systemen aufgrund ihrer Eigenschaften sinnvoll. Tsilidou und Foroglou (2015) beschreiben beispielsweise die Möglichkeit, mittels der Blockchain korruptionsfreie und transparente Wahlen zu ermöglichen, bei denen ein öffentlicher Schlüssel als Stimme gilt.

Duivestein et al. (2015) schreiben, dass sich das Konzept einer DAO generell auch auf gesamte Regierungen anwenden lässt. Laut Swan (2015) lässt sich somit potenziell eine voll repräsentative Demokratie erreichen und der Staatsapparat erheblich effizienter aufbauen, da viele Prozesse über Smart Contracts automatisiert werden könnten. Als Beispiel nennt Swan (2015) wiederum Wahlen. In Atzori (2015) werden sowohl Anwendungen der Blockchain in Einzelbereichen des Staates als auch als Alternative zu regulären Staaten analysiert. Die Autorin kommt zu dem Schluss, dass genehmigungsbasierte Blockchain-Systeme geeignet sind, um Einzelbereiche der öffentlichen Verwaltung zu verbessern. Das Konzept gesamter Staaten basierend auf Blockchain-Systemen weist jedoch vielfältige Probleme auf (Atzori 2015), die eine Umsetzung fragwürdig erscheinen lassen.

Möglicherweise kann die Blockchain zum Beispiel zur sozialen Inklusion in Entwicklungsländern beitragen (Pilkington 2016). So schreibt Scott (2016) in einem Arbeitspapier der Vereinten Nationen, dass Bitcoin in Ländern mit einer schlechten Banken-Infrastruktur eine alternative Methode zur Verwaltung persönlicher Geldbestände darstellen könnte. Ein Bitcoin-Wallet bzw. die darin enthaltenen privaten Schlüssel können somit die Funktion eines Kontos einnehmen (Scott 2016). Hileman (2015) entwickelt einen Index, der das Potenzial von Bitcoin als alternative Währung in 178 Ländern abbildet; das Ergebnis deutet vor allem auf großes Potenzial in Ländern, in denen die staatliche Währung stark inflationär ist oder Schwarzmärkte vorherrschen. Scott (2016) bemerkt dazu, dass die Blockchain zwar in Ländern mit schwachen Institutionen und geringem Vertrauen einzelner Parteien untereinander die größten Auswirkungen haben könnte, diese Länder allerdings auch in der Regel Probleme haben, solch eine Technologie effektiv zu implementieren.

4.4 Die Blockchain im Rechtswesen

Die Blockchain könnte auch Anwendungsfelder im Rechtswesen bieten (Swan 2015). Von besonderer Relevanz erscheinen hierbei die Eigenschaften der Blockchain als manipulationssichere Datenbank sowie die Konzepte der Smart Contracts und DAOs. Kiviat (2015) bemerkt, dass insbesondere Anwendungsfälle im Bereich der Verifikation von Urheberschaft und Dokumenteninhalten, der Übertragung von Eigentumsrechten und der Vertragsdurchsetzung von Interesse sind. Erstere Anwendungsfälle werden zum Beispiel im Kontext des Rechtemanagements digitaler Objekte von Herbert und Litchfield (2015) und Fujimura et al. (2015) entwickelt. Fairfield (2015) schreibt dazu, dass die Blockchain signifikante Vorteile gegenüber herkömmlichen Methoden bieten kann, um digitale Eigentumsrechte effizient zu verfolgen. Durch die Möglichkeit, durchsetzbare Verträge, deren Rechtsvorschriften in Quellcode formalisiert sind, mittels Smart Contracts zu implementieren, könnte sich laut Wright und De Filippi (2015) zudem der Prozess der Vertragserstellung demokratisieren. Koblitz und Menezes (2015) schreiben, dass folglich viele Anwälte durch die verbreitete Einführung von Smart Contracts obsolet werden könnten. Schwachstellen herkömmlicher rechtlicher Verträge, die durch die Mehrdeutigkeit sprachlicher Ausdrücke entstehen, können laut Wright und De Filippi (2015) durch die Eindeutigkeit von Code in Smart Contracts umgangen werden. Obwohl Smart Contracts Vorteile im Vertragsrecht bieten können, treten damit auch neue Risiken auf. Während Vertragsparteien in herkömmlichen Verträgen jederzeit frei sind, den Vertrag zu brechen, wird ein Smart Contract laut Wright und De Filippi (2015) nach seiner Implementierung automatisch ausgeführt. Zudem benennen die Autoren das zuvor erwähnte Problem, bestehende rechtliche Schutzmechanismen, beispielsweise für Verbraucher, in Smart Contracts zu implementieren.

Wie bereits unter Anwendungen im öffentlichen Sektor beschrieben, finden sich auch im juristischen Umfeld weiterführende Konzepte, die über die Verbesserung einzelner Prozesse hinausgehen. Abramowicz (2015) erläutert, dass beispielsweise eine Erweiterung des Bitcoin-Protokolls eine Art der Rechtsprechung ermöglicht, die er »Peer-to-Peer Recht« nennt. Diese kann laut dem Autor in Szenarien sinnvoll sein, in denen offizielle Entscheidungsträger korrupt sind oder hohe Kosten bestehen. Die Grundidee hierbei ist, dass sich mit Hilfe der Blockchain menschliches Urteilsvermögen aggregieren sowie koordinieren und somit in Bezug auf rechtliche Entscheidungen anwenden lässt (Abramowicz 2015). Eine mögliche Anwendung sieht der Autor vor allem in Nischenbereichen wie beispielsweise dem Schiedswesen. Dennoch merkt Abramowicz (2015) an, dass eine solche Verwendung in nächster Zeit nicht zu erwarten ist und diverse ernstzunehmende Probleme hinsichtlich einer Umsetzung bestehen. So stünden Peer-to-Peer Entscheidungen kritischen Stimmen nach häufig nicht im Einklang mit demokratischen Grundprinzipien.

Darüber hinaus kann die Blockchain auch für bösartige Zwecke verwendet werden (Wright und De Filippi 2015). Abgesehen von der Bezahlung illegaler Güter und Dienstleistungen mit Kryptowährungen (vgl. Böhme et al. 2015), können in Zukunft beispielsweise auch Smart Contracts für illegale Zwecke verwendet werden, beispielsweise für die automatische Bezahlung bei Veröffentlichung vertraulicher Informationen (vgl. Juels et al. 2015).

Auch im Bereich der Privatsphäre werden Anwendungen der Blockchain diskutiert; Wilson und Ateniese (2015) beispielsweise entwickeln ein Modell zur Verbesserung des Verschlüsselungsprogramms »Pretty Good Privacy« (PGP), in dem die Verifikation von PGP-Zertifikaten über Bitcoin-Transaktionen abläuft und Zertifikate in der Blockchain gesichert werden.

4.5 Die Blockchain im Internet der Dinge

Wie nachfolgend ausgeführt wird, findet die Blockchain möglicherweise Verwendung in einem weiteren aufstrebenden Bereich: dem Internet der Dinge (IdD). Das Kernkonzept hinter diesem Begriff ist die Idee, Alltagsgegenstände mit Fähigkeiten zur Wahrnehmung, Erkennung, Vernetzung und Verarbeitung auszustatten, die es ihnen ermöglichen, mit anderen Objekten und Diensten über das Internet zu kommunizieren um ein nützliches Ziel zu erreichen (Whitmore et al. 2015).

Der IT-Marktforschungsanbieter Gartner schätzt, dass die Zahl der installierten IdD-Geräte auf 26 Milliarden im Jahr 2020 ansteigen wird, während die Zahl 2009 noch 0,9 Milliarden betrug (Gartner 2013). Obwohl sich der Sektor gerade erst am Anfang seiner Entwicklung befindet (vgl. Wortmann und Flüchter 2015), argumentieren Pureswaran und Brody (2015), dass er bereits einen Neuanfang benötigt. Eine der größten Herausforderungen für das IdD scheint dabei die Interoperabilität der unterschiedlichen Geräte zu sein (Vermesan et al. 2013). In einer Publikation über potenzielle Forschungsbereiche im Kontext des IdD stellt Stankovic (2014) die Frage, welches Architekturmodell geeignet ist, um eine effektive Konnektivität, Kontrolle, Kommunikation sowie nützliche Anwendungen für die heterogenen Geräte und Applikationen im IdD zu unterstützen.

Die Antwort bietet laut Mattila und Seppälä (2015) möglicherweise die Blockchain. Um die Interoperabilität und eine kommerzielle Nutzung der einzelnen Geräte zu ermöglichen, ist es laut Mattila und Seppälä (2015) notwendig, eine gemeinsame Plattform und Standards zu schaffen. Gemäß den Autoren bildet die Blockchain potenziell das fehlende Stück, um verschiedene Stufen der IdD-Architektur zu verbinden. In Anbetracht der Aussage, dass die Interoperabilität einzelner IdD-Systeme laut einer Studie von Manyika et al. (2015) für durchschnittlich 40% der potenziellen Wertschöpfung im IdD-Bereich notwendig ist, erscheint die Entwicklung einer übergreifenden Plattform umso dringender.

Laut Porter und Heppelmann (2014) besteht ein IdD-Technology-Stack aus drei Bestandteilen: dem IdD-Objekt mit seinen diversen Komponenten, Protokollen zur Kommunikation zwischen dem Objekt und einer Cloud sowie der Cloud selbst. Die Cloud enthält wiederum unter anderem eine Datenbank zur Speicherung von Objektdaten, eine Plattform zur Entwicklung und Ausführung von IdD-Anwendungen, die Regeln und Geschäftslogik für den Betrieb der Geräte, sowie Software, die den autonomen Betrieb, die Kontrolle und die Optimierung der Geräte steuert (Porter und Heppelmann 2014; Wortmann und Flüchter 2015).

Mattila und Seppälä (2015) argumentieren, dass die Unterscheidung zwischen dem Gerät und der Cloud im Falle der Verwendung eines Blockchain-Systems als Netzwerk der einzelnen Geräte und Anwendungen nichtig ist, da die Geräte aufgrund der P2P-Architektur als Teile des Netzwerks selbst eine Cloud bereitstellen. Ein kritischer Punkt könnte in diesem Szenario deshalb die Leistungsfähigkeit der Komponenten sein; wenn diese ausreichend ist, so kann ein P2P-Netzwerk der einzelnen Geräte laut Mattila und Seppälä (2015) die Cloud-Services autonom zu einem Bruchteil der Kosten übernehmen. Insbesondere für Produkte mit geringen Produktionskosten und langen Produktlebenszyklen sind die Kosten für die Aufrechterhaltung einer klassischen Cloud-Architektur überproportional hoch, weshalb diese nicht notwendigerweise funktional oder profitabel über den gesamten Produktlebenszyklus bleibt (Mattila und Seppälä 2015). Durch die Implementierung eines autonomen P2P-Netzwerks mittels der Blockchain könnte die Notwendigkeit eines externen Cloud-Services und die damit verbundenen Kosten reduziert bzw. eliminiert werden (Mattila und Seppälä 2015; Pureswaran und Brody 2015).

Insbesondere die Konzepte der Smart Contracts und DAOs könnten überdies im IdD Verwendung finden. In Zusammenarbeit mit Samsung implementierte IBM einen Proof-of-concept namens ADEPT[2], im Rahmen dessen eine Waschmaschine autonom Handlungen durchgeführt hat (Pureswaran et al. 2015). In dem Konzept bildet die Blockchain die Grundlage des Systems (Forte et al. 2015). Die Ethere-um-Blockchain wurde dazu aufgrund ihrer Fähigkeit, Smart Contracts und DAOs implementieren zu können, ausgewählt (Panikkar et al. 2015). Die Waschmaschine war unter anderem fähig, mittels Smart Contracts ihr eigenes Waschmittel zu bestellen und zu

[2] Autonomous Decentralized Peer-to-Peer Telemetry (Pureswaran et al. 2015).

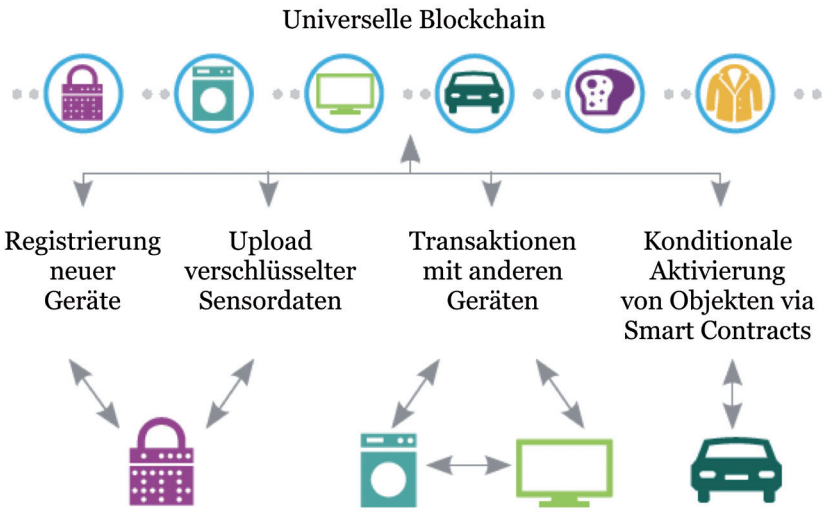

Abbildung 7:
Die Blockchain als universelle IdD-Plattform (in Anlehnung an Pureswaran und Brody 2015, S.11)

bezahlen, wenn es zu Neige ging (Forte et al. 2015; Pureswaran et al. 2015) oder im Falle eines Schadens über die Blockchain ihren Garantie-Status zu überprüfen und einen geeigneten Handwerker zu bestellen, der abhängig vom Garantie-Status bezahlt werden kann (Panikkar et al. 2015). Darüber hinaus wurde im Rahmen des ADEPT-Prototypen ein Handelsplatz für Energieversorgung geschaffen. Beispielsweise konnte die Waschmaschine darüber mit dem Micro-Grid einer Gemeinde kommunizieren und im Gegenzug für Energie mittels eines Vertrages zwischen dem Besitzer und der Gemeinde eine bestimmte Anzahl an Waschgängen für Gemeindemitglieder anbieten (Panikkar et al. 2015). Diese Anwendungen suggerieren, dass durch die Verwendung der Blockchain ein bislang fehlender funktionaler Wert (Pureswaran und Brody 2015) für IdD-Geräte geschaffen werden kann.

Als Herausforderung im Umfeld des IdD wird zudem häufig Vertrauen zwischen den Geräten genannt (vgl. Sicari et al. 2015). Pureswaran und Brody (2015) argumentieren, dass durch die Verifikation von Transaktionen mittels des dezentralen Konsensmechanismus die Notwendigkeit für Vertrauen gegenüber anderen Geräten im IdD eliminiert wird. Als weiteres Problem wird die eindeutige Identifizierung einzelner Geräte genannt, das durch die vielen unterschiedlichen Aufgaben und Datenformate der einzelnen Geräte verschärft wird (Gubbi et al. 2013). Die Blockchain könnte ein unveränderbares Register der Identität einzelner Geräte bieten (Bogart und Rice 2015), indem ein Gerät direkt durch den Hersteller in einer universellen Blockchain registriert wird und fortan als Entität, verknüpft mit Produktinformationen oder zum Beispiel seiner jeweiligen Transaktionshistorie, darin auftritt (Panikkar et al. 2015).

Wie diese Anwendungsbeispiele zeigen, bildet die Blockchain im IdD die Grundlage für Transaktionen und die Koordination interagierender Geräte, die nicht notwendigerweise vertrauenswürdig sind (vgl. Pureswaran und Brody 2015). Außerdem dient sie der Implementierung von Smart Contracts und dem direkten Wertaus-tausch zwischen den Geräten (Bogart und Rice 2015). Diese Rolle wird in Abbildung 7 exemplarisch dargestellt.

In einem solchen Szenario würde sich die Wertschöpfungslogik im IdD laut Mattila und Seppälä (2015) stark verändern. Eine Logik, die auf der exklusiven Kontrolle von Produktionsfaktoren beruht, würde sich dahingehend wandeln, dass IdD-Komponenten mehr als nur Daten, sondern beispielsweise auch Bandbreite, Rechenleistung oder Energie teilen können. Mit Hilfe der Blockchain, so die Autoren, können die Komponenten zuverlässige und verteilte Handelsplätze bilden, in denen Objekte, die sich nicht notwendigerweise vertrauen müssen, handeln und kooperieren können. Generell könnten durch diesen Handel in Echtzeit liquide Märkte entstehen (Pureswaran und Brody 2015), in denen Angebot und Nachfrage mit erhöhter Transparenz und Autonomie koordiniert werden (Wright und De Filippi 2015).

Zhang und Wen (2015) modellieren ein entsprechendes IdD-Geschäftsmodell, in dem Objekte, die als DACs implementiert werden, eine zentrale Rolle einnehmen. Eine exemplarische Geschäftstransaktion ist der Austausch von Nutzerdaten gegen Geld für die Energieversorgung. Pureswaran und Brody (2015) schreiben, dass aktuelle IdD-Geschäftsmodelle zumeist auf der Analyse von Nutzerdaten beruhen, was laut den Autoren jedoch problematisch ist, da beispielsweise Unternehmen ihre gesammelten Daten nicht teilen möchten. Auch Wörner und von Bomhard (2014) merken an, dass eine Nutzung der Sensordaten von IdD-Geräten für dritte Parteien nicht möglich ist, da die Daten entweder in privaten Netzwerken gespeichert sind oder kein Anreiz für die Eigner der Sensordaten besteht, diese zu teilen. Wörner und von Bomhard (2014) entwerfen deshalb ebenfalls ein Modell, in dem Daten von IdD-Geräten über die Bitcoin-Blockchain gehandelt und somit oben genannte Probleme gelöst werden. Gemäß Mattila und Seppälä (2015) wird durch die Verwendung eines Blockchain-Systems außerdem das Problem umgangen, dass Daten in unterschiedlichen Formaten bereitgestellt werden, da die Blockchain als Plattform für einheitliche Formate dienen kann. Zudem merken die Autoren an, dass es mittels der Blockchain möglich ist, beliebige Analysen der Sensordaten in variablem Umfang zu ermöglichen, ohne dabei den tatsächlichen Inhalt offenzulegen (vgl. Zyskind et al. 2015).
Indem Hersteller die Cloud selbst (Mattila und Seppälä 2015) sowie die Zuständigkeit für Wartungen (Pureswaran und Brody 2015) in das Netzwerk aus Geräten transferieren, können Infrastrukturkosten gespart werden. Jedoch bestehen trotz potenzieller Vorteile auch Herausforderungen in Bezug auf die Umsetzung eines Blockchain-basierten IdD. Abgesehen von möglichen rechtlichen Problemen (vgl. Wright und De Filippi 2015) nennen Panikkar et al. (2015) beispielsweise die Skalierbarkeit von Blockchain-Systemen oder die möglicherweise unzureichende Anonymität innerhalb dieser.

5. POTENTIALE UND RISIKEN DER BLOCKCHAIN

Im Rahmen von Kapitel 5 werden zunächst die strukturellen Chancen und Risiken der Blockchain aufgearbeitet. Darauf aufbauend werden spezifische Hindernisse bei der Blockchain-Implementierung diskutiert und Empfehlungen abgeleitet.

5.1 Strukturelle Chancen und Risiken

Durch ihren Aufbau weisen Blockchain-Systeme diverse Chancen und Risiken auf. An dieser Stelle sei darauf hingewiesen, dass die nachfolgend aufgezeigten Attribute bei unterschiedlichen Blockchain-Implementierungen variieren können. Im Rahmen dieser Studie haben wir uns auf das Bitcoin-System und vergleichbare Systeme bezogen. Für andere Systeme, die bspw. in Kapitel 2.3 erläutert wurden, können die Chancen und Risiken variieren.

Zunächst ergeben sich durch den Einsatz kryptographischer Prinzipien diverse positive Eigenschaften. Weil die Verwendung von Daten in der Blockchain nur über einen privaten Schlüssel möglich ist, wird eine *detaillierte Zugangskontrolle* etabliert (Walport 2015). Da Adressen lediglich durch öffentliche Schlüssel dargestellt werden und nicht notwendigerweise an Identitäten geknüpft sind, werden Bitcoin bzw. Blockchain-Systeme allgemein außerdem oftmals als anonym beschrieben (Brito und Castillo 2013; Mainelli und von Gunten 2014). In Anbetracht der Tatsache, dass aufgrund der Transparenz von Blockchains Informationsflüsse analysiert und Identitäten teilweise zugeordnet werden können (vgl. Reid und Harrigan 2012), scheint jedoch die Bezeichnung *Pseudonymität* treffender zu sein, da ein öffentlicher Schlüssel als Pseudonym dient (Brito und Castillo 2013; Mainelli und von Gunten 2014). Auch durch die Verwendung von Hash-Funktionen ergeben sich verschiedene Chancen. Da Blöcke jeweils eine Referenz zu dem vorherigen Block sowie einen Zeitstempel enthalten und über Hashes miteinander verbunden sind, wird die *Integrität der in der Blockchain* enthaltenen Daten gewährleistet (Bogart und Rice 2015) und im Rahmen dessen der Nachweis eines im Nachhinein nicht unbemerkt veränderbaren Aufnahmezeitpunktes in die Blockchain ermöglicht (vgl. McKinsey & Company 2015; Walport 2015).

Auch die Kombination eines verteilten P2P-Netzes mit einem Konsensmechanismus zum Abgleich des Status der Blockchain ermöglicht vielfältige Chancen. Da sowohl die Blockchain selbst, als auch einzelne Mechanismen wie die Verifikation digitaler Signaturen (Franco 2015), vielfach bei allen Netzteilnehmern reproduziert wird, gibt es innerhalb des Netzwerks keinen Single Point of Failure (Walport 2015). Somit besteht eine große *Netzausfallsicherheit* (Xethalis et al. 2016) und damit einhergehende Datenverfügbarkeit (Peters und Panayi 2015). Durch die Verwendung des Konsensmechanismus wird zudem das Double Spending Problem wie zuvor dargelegt verhindert (Bonneau et al. 2015; Tschorsch und Scheuermann 2015). Jeder Netzknoten überprüft individuell, ob einzelne Transaktionen und gesamte Blöcke gültig sind (Antonopoulos 2014). Folglich ist *kein Vertrauen gegenüber einer einzelnen Instanz* (Bogart und Rice 2015; Walport 2015) *oder anderen Knoten erforderlich*; in Folge dessen sind zudem dritte Parteien für Aktionen innerhalb des Netzwerks und die Verwaltung der Blockchain obsolet (McKinsey & Company 2015; Zohar 2015).

Da Prozesse innerhalb des Netzwerks exakt nach einem jeweils entsprechend spezifizierten Programmcode ablaufen besteht zudem eine hohe Prozessintegrität (Bogart und Rice 2015). Durch die für jeden Netzknoten einsehbare Transaktionshistorie weisen Blockchain-Systeme zudem eine große Transparenz auf (vgl. Bogart und Rice 2015; Walport 2015; Xethalis et al. 2016).

Die Abwicklung einer Transaktion ist mit der Aufnahme in einen Block vollendet und beansprucht im Bitcoin-System nur ca. 10 Minuten (Böhme et al. 2015). Überdies existieren Methoden, die diese Zeitspanne verkürzen (vgl. Wattenhofer und Decker 2015). Alternative Blockchain-Systeme wie zum Beispiel Ripple weisen mit 5 bis 15 Sekunden deutlich kürzere Transaktionszeiten auf (Swanson 2014). Somit stellt die *kurze Dauer* der *Transaktionsabwicklung* eine weitere Chance der Blockchain dar.

Bereits im Bitcoin-Netzwerk wurde außerdem die Programmierbarkeit von Transaktionen ermöglicht (Barber et al. 2012). Durch diese *Programmierbarkeit* lassen sich komplexe, konditionale Transaktionen und Aktionen in Blockchain-Systemen kreieren (Deloitte 2016).

Trotz vieler inhärenter Vorteile weisen Blockchain-Systeme auch Schwachstellen und Probleme auf. So bringt beispielsweise der Konsens-Mechanismus durch PoW diverse Mängel mit sich. Im gesamten Netzwerk muss zu seiner Durchführung eine *große Menge an Energie* aufgewendet werden, wodurch sowohl Kosten, als auch erhebliche Umweltbelastungen entstehen (Becker et al. 2013). Zudem kann mit einer wachsenden Dateigröße der Blockchain und einer erhöhten Anzahl an Transaktionen eine Limitierung durch die Bandbreite oder die Rechenleistung mancher Netzteilnehmer auftreten (Barber et al. 2012). Im Bitcoin-Netzwerk ist die Blockgröße auf 1 Megabyte begrenzt (Franco 2015). Somit kann das System auch nur eine begrenzte maximale Anzahl an Transaktionen durchführen (McKinsey & Company 2015). Es existiert allerdings eine Vielzahl an Vorschlägen, um das Problem der *Skalierbarkeit* in Blockchain-Systemen zu lösen; für einen Überblick sei auf Croman et al. (2016) verwiesen. Unterschiedliche Blockchain-Modelle könnten sich zudem als inkompatibel erweisen (Silverberg et al. 2015) und folglich Probleme hinsichtlich der *Interoperabilität* aufwerfen. Eine Umgehung dieses Problems könnten sogenannte Pegged Sidechains bieten, die als Blockchain-Systeme, die Inhalte anderer Systeme validieren und transferieren können, zu verstehen sind (Back et al. 2014).

Ein weiteres Risiko ergibt sich durch die Public-Key Kryptographie. Wird ein *privater Schlüssel gestohlen oder geht verloren*, so sind die korrespondierenden Inhalte unweigerlich nicht mehr verwendbar (Condos et al. 2016; Xethalis et al. 2016). Werden zudem Transaktionsdetails fehlerhaft eingegeben und abgeschickt, so ist die Transaktion durch den Absender nicht mehr reversibel (Xethalis et al. 2016). Diese *Irreversibilität* kann andererseits auch als Chance angesehen werden (vgl. Zohar 2015). Wie zuvor erwähnt, ist *außerdem Anonymität nicht zwingend gewährleistet* (vgl. Reid und Harrigan 2012). Zudem existieren bekannte Attacken, mittels derer Blockchain-Systeme erfolgreich manipuliert werden können. Ein verbreitetes Beispiel hierfür ist die sogenannte 51%-Attacke, im Rahmen derer ein Angreifer Transaktionen in einem Block verändert, also beispielsweise an eine andere Zieladresse versendet, und ab dem ersten durch ihn veränderten Block für alle Blöcke erneut den PoW erbringt. Gleichzeitig muss er die übrigen Netzknoten überholen, wofür eine Rechenleistung von mindestens 50% des gesamten Netzwerks für einen garantierten Erfolg der Attacke notwendig ist (Franco 2015). Eine weitere Attacke in Relation zum PoW stellt das sogenannte »Selfish Mining« dar (Eyal und Sirer 2014). Hierbei erhält ein Angreifer eine relativ größere Vergütung im Verhältnis zu seinem tatsächlichen Rechenaufwand (Courtois und Bahack 2014). Andere Attacken ermöglichen effektiv doppelte Transaktionen und umfassen zum Beispiel die Race-Attacke, bei der Schwächen in der Informationspropagation im Netzwerk ausgenutzt werden, sowie die Finney-Attacke, die von der Zurückhaltung gefundener Blöcke Gebrauch macht (Franco 2015).

Eine Zusammenfassung der im Rahmen dieser Studie identifizierten, strukturellen Chancen und Risiken von Blockchain-Systemen ist Tabelle 4 zu entnehmen.

Chancen	Risiken
Detaillierte Zugangskontrolle (Walport 2015)	Hoher Energiekonsum durch PoW (Becker et al. 2013)
Pseudonymität (Brito und Castillo 2013; Mainelli und von Gunten 2014)	Geringe Skalierbarkeit (Croman et al. 2016)
Hohe Datenintegrität (Bogart und Rice 2015)	Mangelnde Interoperabilität der Systeme (vgl. Silverberg et al. 2015)
Hohe Netzausfallsicherheit (Xethalis et al. 2016)	Sicherung privater Schlüssel (vgl. Condos et al. 2016; Xethalis et al. 2016)
Kein Vertrauen für Interaktionen notwendig (vgl. Bogart und Rice 2015; Walport 2015)	Irreversibilität von Transaktionen (Xethalis et al. 2016)
Hohe Prozessintegrität (Bogart und Rice 2015)	Keine garantierte Anonymität (vgl. Reid und Harrigan 2012)
Große Transparenz (vgl. Bogart und Rice 2015; Walport 2015; Xethalis et al. 2016)	Mögliche Attacken (vgl. Franco 2015; Eyal und Sirer 2014)
Kurze Dauer der Transaktionsabwicklung (vgl. Swanson 2014)	
Programmierbarkeit der Transaktionen (Deloitte 2016)	

Tabelle 4: Strukturelle Chancen und Risiken von Blockchain-Systemen

5.2 Hindernisse und Empfehlungen hinsichtlich der Umsetzung

In Tabelle 5 werden mögliche Hindernisse zusammengefasst aufgeführt. Unter den Aufzählungspunkten wird zudem zur Veranschaulichung jeweils ein konkretes Beispiel genannt.

Eine Vielzahl an Unternehmen arbeitet inzwischen mittels unterschiedlicher Strategien an der Implementierung von Blockchain-Systemen (vgl. Bogart und Rice 2015). Eine Recherche durch Burelli et al. (2015) hat dabei ergeben, dass die Unternehmen vor allem vier Strategien verfolgen: eine In-House-Entwicklung verschiedener Lösungen, Investitionen in Blockchain-Unternehmen, Partnerschaften mit Blockchain-Unternehmen oder die Gründung eigener fachbezogener Accelerators.

Diverse Unternehmensberatungen und Finanzinstitutionen geben zudem Handlungsempfehlungen für Unternehmen in Bezug auf die Blockchain ab. Eine übergreifende Empfehlung ist dabei der Fokus auf Kollaboration und die Etablierung branchenweiter Standards (vgl. DTCC 2016; EvryLabs 2015; McKinsey & Company 2015; Silverberg et al. 2015). Diese Empfehlung erscheint sinnvoll in Anbetracht der Tatsache, dass zuvor dargelegte Anwendungsfälle auf der Implementierung einer zentralen Blockchain-Plattform, an der mehrere Unternehmen teilnehmen, beruhen. Auch über die Hälfte der Befragten der Studie der Cofinpro AG und des IT Finanzmagazins (2016) gaben Kollaboration als die momentan beste Strategie an, während nur 2% eine eigenständige Entwicklung für geeignet hielten. Das Konsortium R3CEV beispielsweise vereint diverse internationale Finanzunternehmen mit dem Ziel, einheitliche Standards für die Blockchain im Finanzsektor zu erarbeiten (Geiling 2016). Trotz der vermeintlichen Vorteile offener und gemeinsamer Plattformen erwarten Garfinkel et al. (2016), dass Gewinne zukünftig vornehmlich durch die Eigentümer effizienter Blockchain-Plattformen realisiert werden. McKinsey & Company (2015) empfehlen Marktteilnehmern zudem, kurzfristig im Umfeld der Blockchain zu forschen und den Einfluss auf ihr Geschäftsfeld zu evaluieren. McKinsey & Company (2015) erwarten außerdem, dass sich erste Umsetzungen der Blockchain in Kapitalmärkten auf spezifische Anwendungsbereiche fokussieren werden. Dementsprechend empfehlen die Autoren Unternehmen im Kapitalmarktbereich, sich hinsichtlich einer Implementierung der Blockchain zunächst auf den Bereich der Transaktionsabwicklung sowie damit verbundene manuelle Prozesse zu fokussieren, da in diesem Bereich große Vorteile durch die Blockchain bei geringem Einfluss auf bestehende Geschäftsmodelle zu erwarten sind. In EvryLabs (2015) wird dahingegen auf Engagements im Bereich internationaler Überweisungen hingewiesen, da laut den Autoren dieser Bereich die größten Kundenvorteile birgt und somit zu einem Wettbewerbsvorteil führen kann.

Limitierungen des aktuellen Stands der Technik (McKinsey & Company 2015): • Skalierbarkeit aktueller Systeme (vgl. Van de Velde et al. 2016) • Verrechnung offener Positionen zur Risikominimierung bei Transaktionen in momentanen Systemen nicht möglich (McKinsey & Company 2015)
Regulierung und Gesetzgebung (McKinsey & Company 2015; Silverberg et al. 2015; Van de Velde et al. 2016): • Einordnung von Smart Contracts vor Gericht (Silverberg et al. 2015)
Standards und Governance-Strukturen (DTCC 2016; Silverberg et al. 2015; Van de Velde et al. 2016): • Gewährleistung der Interoperabilität unterschiedlicher Systeme für bestimmte Anwendungen (Silverberg et al. 2015) • Mangel an Standards (Cofinpro AG und IT Finanzmagazin 2016)
Operationales Risiko im Zuge der Systemumstellung (Van de Velde et al. 2016): • Technische Probleme bei der Implementierung eines Blockchain-Systems (Van de Velde et al. 2016)
Hindernisse in Bezug auf Anonymität (Van de Velde et al. 2016): • Adäquate und von dem jeweiligen Blockchain-System unabhängige Sicherung privater Schlüssel (Van de Velde et al. 2016)

Tabelle 5: Hindernisse hinsichtlich der Einführung der Blockchain

6. FAZIT UND AUSBLICK

Die Blockchain ist ein junges, sich rapide weiterentwickelndes Gebiet und verspricht vielfältige Einsatzmöglichkeiten (Glaser und Bezzenberger 2015). Wie Giaglis und Kypriotaki (2014) konstatierten, werden die Ergebnisse der Forschung über die Möglichkeiten und Grenzen dieser Technologie das Ergebnis der »Revolution« bestimmen, die durch digitale Währungen losgetreten wurde.

Im Rahmen des vorliegenden Papiers wurde eine umfangreiche Analyse der aktuellen Literatur zum Thema Blockchain und insbesondere zu Anwendungsgebieten der Blockchain durchgeführt. Dabei wurde deutlich, dass die Struktur von Blockchain-Systemen direkte Interaktion, wie zum Beispiel Werttransaktionen zwischen Individuen, die sich nicht vertrauen müssen, sicher und effizient ermöglicht und eine manipulationssichere Datenstruktur darstellt. Die Grundkonzepte, wie Kryptowährungen, Smart Contracts und Dezentrale Autonome Organisationen, sowie Anwendungen der Technologie bauen hauptsächlich auf diesen Eigenschaften auf. Da diese Eigenschaften besonders in der Finanzbranche wichtig sind, finden sich aktuell die meisten Anwendungen in diesem Bereich. Im Vordergrund steht hierbei die effizientere Gestaltung von Zahlungssystemen.

Diese Beobachtung wird durch die Ergebnisse einer Analyse von 222 Unternehmen aus dem Umfeld der Blockchain bestätigt. Ferner hat diese gezeigt, dass sich eine Vielzahl an Unternehmen auf die Erschaffung infrastruktureller Grundlagen fokussiert. Dies ist vermutlich darauf zurückzuführen, dass sich die Technologie noch in ihrer Entwicklung befindet und momentan hoher Bedarf nach Infrastruktur für die Implementierung spezifischer Anwendungen besteht. Besonders interessant erscheint, dass die Blockchain Interaktionen nicht nur effizienter gestalten, sondern viele Vorgänge vollends automatisieren kann. So werden selbstausführende Verträge, die von bestimmten Ereignissen abhängen und Organisationen, die autonom Handlungen vornehmen und direkt von ihren Anteilseignern gesteuert werden, mittels der Blockchain möglich. Dennoch bestehen sowohl technische als auch rechtliche Hürden, die es vor einem verbreiteten Einsatz zu überwinden gilt.

Hinsichtlich weiterer Anwendungsszenarien werden vor allem Einsatzgebiete in Bereichen der Wirtschaft, des öffentlichen Sektors sowie im juristischen Sektor diskutiert. Erste Praxiskonzepte lassen zudem darauf schließen, dass die Blockchain in der Rolle als universelle Plattform, die Interaktionen autonomer Objekte ermöglicht, besonders den Bereich des »Internet der Dinge« bedeutend voranbringen kann.

Neben den vorgestellten Hindernissen und Empfehlungen hinsichtlich geeigneter Einsatzzwecke von Blockchain-Lösungen sind die Autoren der Meinung, dass weitere Faktoren bei der Entscheidung über die Nutzung von Blockchain-Systemen berücksichtigt werden müssen. So erscheint die Erwägung einer Blockchain-Lösung nur dann als sinnvoll, wenn gewisse Grundlagen vorhanden sind, wie die Möglichkeit des Aufbaus eines Peer-to-Peer Netzwerks. Darüber hinaus sollte es möglich sein, Besitz, Transaktionen und Eigenschaften als Metadaten elektronisch abbilden zu können. Zudem kann die Blockchain eine Rolle spielen, wenn ein zentraler Stakeholder ersetzt werden soll bzw. fehlendes Vertrauen in die bestehende Lösung oder den aktuellen Anbieter vorherrscht. Ein weiterer Grund für eine Blockchain-Lösung kann die Forderung nach einer transparenten und nachvollziehbaren Transaktionshistorie sein. Ferner kann die Einführung einer Blockchain im Zusammenhang mit der Entwicklung neuer Geschäftsmodelle stehen. Dabei sollte ebenfalls berücksichtigt werden, dass die Automatisierungsvorteile von Smart Contracts dann am größten sind, wenn die Prozessschritte und ihre Konsequenzen umfassend

vordefiniert werden können. Des Weiteren sollte betrachtet werden, wer die Blockchain betreiben bzw. kontrollieren soll/muss und wie Nutzer im Netzwerk authentifiziert und identifiziert werden sollen/müssen.

Generell fällt die mehrheitliche Meinung über die Möglichkeiten der Blockchain momentan regelrecht euphorisch aus. Ohne Zweifel ergeben sich viele interessante Anwendungsoptionen – der ultimative Einfluss der Technologie bleibt dennoch abzuwarten. Eines erscheint in Anbetracht der aktuellen Entwicklungen allerdings sicher: die Blockchain wirft viele neue Fragen auf und stellt somit einen interessanten Gegenstand für zukünftige Forschung dar. Aus diesem Grund arbeitet das Fraunhofer FIT und seine Projektgruppe Wirtschaftsinformatik gemeinsam am Aufbau eines Blockchain-Labors. Dieses Labor bietet ein ideales Umfeld für umfassende und wissenschaftlich fundierte Untersuchungen sowie die Erarbeitung von praxistauglichen Lösungen.

7. LITERATURVERZEICHNIS

Abramowicz, M. B. (2015) Peer-to-Peer Law, Built on Bitcoin, Abgerufen am 02.06.2016, von http://scholarship.law.gwu.edu/faculty_publications/1109/.

Ahamad, S., Nair, M. and Varghese, B. (2013) A survey on crypto currencies, Proceedings of the 4th International Conference on Advances in Computer Science (ACS 2013), December 13-14, Delhi, India.

Ametrano, F. M. (2014) Hayek Money: the Cryptocurrency Price Stability Solution, Abgerufen am 02.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270.
AngelList (2016a) Bitcoin Startups, Abgerufen am 30.05.2016, von https://angel.co/bitcoin.

AngelList (2016b) Blockchains Startups, Abgerufen am 02.06.2016, von https://angel.co/blockchains.

Antonopoulos, A. M. (2014) Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O´Reilly Media, Sebastopol, CA.

Atzori, M. (2015) Blockchain Technology and Decentralized Governance: Is the State Still Necessary?, Abgerufen am 17.05.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713&download=yes.

Back, A. (2002) Hashcash - A Denial of Service Counter-Measure, Abgerufen am 02.06.2016, von http://www.hashcash.org/papers/hashcash.pdf.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P. (2014) Enabling Blockchain Innovations with Pegged Sidechains, Abgerufen am 02.06.2016, von https://www.blockstream.com/sidechains.pdf.

Badev, A., and Chen, M. (2014) Bitcoin: Technical Background and Data Analysis, Abgerufen am 02.06.2016, von http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf.

Barber, S., Boyen, X., Shi, E., and Uzun, E. (2012) Bitter to Better - How to Make Bitcoin a Better Currency, in: Financial Cryptography and Data Security. 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers, A. D. Keromytis (ed.). Springer, Berlin, Heidelberg: 399-414.

Baur, A. W., Bühler, J., Bick, M. and Bonorden, C. S. (2015) Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co, in: Open and Big Data Management and Innovation. 14th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2015, Delft, The Netherlands, October 13-15, 2015, Proceedings, M. Janssen, M. Mäntymäki, J. Hidders, B. Klievink, W. Lamersdorf, B. van Loenen and A. Zuiderwijk (eds.). Springer International Publishing, Basel, Cham: 63–80.

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P. and Böhme, R. (2013) Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency, in: The Economics of Information Security and Privacy, R. Böhme (ed.). Springer, Berlin, Heidelberg: 135–156.

Bentov, I., Lee, C., Mizrahi, A. and Rosenfeld, M. (2014) Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake, ACM SIGMETRICS Performance Evaluation Review, 42, 3, 34–37.

Bernstein, P. A. (1996) Middleware: A Model for Distributed System Services, Communications of the ACM, 39, 2, 86–98.
BitFury Group (2016) Digital Assets on Public Blockchains, Abgerufen am 03.06.2016, von http://bitfury.com/content/5-white-papers-research/bitfury-digital_assets_on_public_blockchains-1.pdf.

BitFury Group and Garzik, J. (2015) Public versus Private Blockchains. Part 1: Permissioned Blockchains, Abgerufen am 03.06.2016, von http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf.

Bliss, R. R. and Steigerwald, R. S. (2006) Derivatives clearing and settlement: A comparison of central counterparties and alternative structures, Economic Perspectives, 30, 4, 22–29.

Blockchain.info (2016) Marktkapitalisierung, Abgerufen am 02.06.2016, von https://blockchain.info/de/charts/market-cap.

Blundell-Wignall, A. (2014) The Bitcoin Question: Currency vs. Trust-less Transfer Technology, Abgerufen am 02.06.2016, von http://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Question-2014.pdf.

Bogart, S. and Rice, K. (2015) The Blockchain Report: Welcome to the Internet of Value, Abgerufen am 02.06.2016, von https://needham.bluematrix.com/sellside/EmailDocViewer?encrypt=4aaafaf1-d76e-4ee3-9406-7d0ad3c0d019&mime=pdf&co=needham&id=sbogart@needhamco.com&source=mail&utm_content=buffer0b432&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015) Bitcoin: Economics, Technology, and Governance, The Journal of Economic Perspectives, 29, 2, 213–238.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. and Felten, E. W. (2015) SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, 2015 IEEE Symposium on Security and Privacy, May 17-21, San Jose, CA.

Briere, M., Oosterlinck, K. and Szafarz, A. (2013) Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins, Abgerufen am 02.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324780.

Brito, J. and Castillo, A. (2013) Bitcoin: A Primer for Policymakers, Abgerufen am 02.06.2016, von http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf.

Burelli, F., John, M., Cenci, E., Otten, J., Courtneidge, R., and Clarence-Smith, C. (2015) Blockchain and Financial Services: Industry Snapshot and Possible Future Developments, Abgerufen am 03.06.2016, von https://www.innovalue.de/publikationen/InnovalueLockeLord-BlockchaininFinancialServices2015.pdf.

Buterin, V. (2014) A Next-Generation Smart Contract and Decentralized Application Platform, Abgerufen am 02.06.2016, von https://github.com/ethereum/wiki/wiki/White-Paper.

Christensen, C. M. (1997) The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, Harvard Business School Press, Boston, MA.

Cofinpro AG and IT Finanzmagazin (2016) Blockchain. Zukunft oder Ende des Bankings?, Abgerufen am 02.06.2016, von http://cofinpro.de/blockchain/.

CoinGecko (2016) 360° Überblick auf die Charts von Kryptowährungen, Abgerufen am 30.08.2016, von https://www.coingecko.com/en.

CoinMarketCap (2016) Crypto-Currency Market Capitalizations, Abgerufen am 02.06.2016, von http://coinmarketcap.com.

Condos, J., Sorrell, W. H. and Donegan, S. L. (2016) Blockchain Technology: Opportunities and Risks, Abgerufen am 02.06.2016, von http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf

Courtois, N. T. and Bahack, L. (2014) On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency, Abgerufen am 02.06.2016, von http://arxiv.org/pdf/1402.1718v5.pdf.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., Song, D. and Wattenhofer, R. (2016) On Scaling Decentralized Blockchains (A Position Paper), Abgerufen am 02.06.2016, von http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf.

Decker, C. and Wattenhofer, R. (2013) Information Propagation in the Bitcoin Network, Proceedings of the IEEE 13th International Conference on Peer-to-Peer Computing (P2P 2013), September 9-11, Trento, Italy.

Deloitte (2016) Blockchain: Enigma. Paradox. Opportunity, Abgerufen am 02.06.2016, von https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-blockchain-enigma-paradox-opportunity-report.pdf.

DeRose, C. (2016) 'Smart Contracts' Are the Future of Blockchain, Abgerufen am 03.06.2016, von http://www.americanbanker.com/bankthink/smart-contracts-are-the-future-of-blockchain-1078705-1.html.

Diffie, W. and Hellman, M. E. (1976) New Directions in Cryptography, IEEE Transactions on Information Theory, 22, 6, 644–654.

DTCC (2016) Embracing Disruption: Tapping the Potential of Distributed Ledgers to improve the Post-Trade Landscape, Abgerufen am 03.06.2016, von http://www.dtcc.com/~/media/Files/PDFs/DTCC-Embracing-Disruption.pdf.

Duivestein, S., van Doorn, M., van Manen, T., Bloem, J. and van Ommeren, E. (2015) Design to Disrupt. Blockchain: cryptoplatform for a frictionless economy, Abgerufen am 03.06.2015, von http://labs.sogeti.com/wp-content/uploads/2015/08/D2D-3_EN-web.pdf.

Duncan, N. B. (1995) Capturing Flexibility of Information Technology Infrastructure: A Study of Resource Characteristics and Their Measure, Journal of Management Information Systems, 12, 2, 37–57.

Edwards, P.N., Jackson, S.J., Bowker, G.C. and Knobel, C.P. (2007) Understanding Infrastructure: Dynamics, Tensions, and Design. Report of a Workshop on »His-tory & Theory of Infrastructure: Lessons for New Scientific Cyberinfrastructures«, Abgerufen am 04.08.2016, von https://deepblue.lib.umich.edu/bitstream/handle/2027.42/49353/UnderstandingInfrastructu-re2007.pdf;jsessionid=BBC10AF-3646CC3C6EF22F13A30732A4A?sequence=3.

Euro Banking Association (EBA) (2015) Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios. An exploration for transaction banking and payments professionals, Abgerufen am 03.06.2016, von https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf.

Eikmanns, B. C. and Sandner, P. G. (2015) Bitcoin: The Next Revolution in International Payment Processing? An Empirical Analysis of Potential Use Cases, Abgerufen am 03.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2619759.

EvryLabs (2015) Blockchain: Powering the Internet of Value, Abgerufen am 03.06.2016, von https://www.evry.com/globalassets/insight/bank2020/blockchain---powering-the-internet-of-value.pdf.

Eyal, I. and Sirer, E. G. (2014) Majority Is Not Enough: Bitcoin Mining Is Vulnerable, in Financial Cryptography and Data Security. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers, N. Christin and R. Safavi-Naini (eds.). Springer, Berlin, Heidelberg: 436-454.

Fairfield, J. A. T. (2015) Bitproperty, Southern California Law Review, 88, 4, 805–874.

Forte, P., Romano, D. and Schmid, G. (2015) Beyond Bitcoin - Part I: A critical look at blockchain-based systems, Abgerufen am 03.06.2016, von https://eprint.iacr.org/2015/1164.pdf.
Franco, P. (2015) Understanding Bitcoin: Cryptography, Engineering, and Economics, Wiley, Chichester.

Freeman, P.A. (2007) Is 'Designing' Cyberinfrastructure – or, Even, Defining It – Possible?, Abgerufen am 04.08.2016, von http://firstmonday.org/ojs/index.php/fm/article/view/1900/1782.

Fujimura, S., Watanabe, H., Nakadaira, A., Yamada, T., Akutsu, A. and Kishigami, J. J. (2015) BRIGHT: A Concept for a Decentralized Rights Management System Based on Blockchain, Proceedings of the IEEE 5th International Conference on Consumer Electronics - Berlin (ICCE-Berlin 2015), September 6-9, Berlin, Germany.

Garfinkel, H., Drane, J. and Marsh, C. (2016) What's next for blockchain in 2016?, Abgerufen am 03.06.2016, von http://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-qa-whats-next-for-blockchain.pdf.

Gartner (2013) Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, Abgerufen am 21.04.2016, von http://www.gartner.com/newsroom/id/2636073.

Geiling, L. (2016) Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, Abgerufen am 03.06.2016, von http://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2016/bj_1602.pdf;jsessionid=E49CCB3A6F5A648F1D39A68AA4B6DCD4.1_cid298?__blob=publicationFile&v=3.

Giaglis, G. M. and Kypriotaki, K. N. (2014) Towards an Agenda for Information Systems Research on Digital Currencies and Bitcoin, in: Business Information Systems Workshops. BIS 2014 International Workshops, Larnaca, Cyprus, May 22-23, 2014, Revised Papers, W. Abramowicz and A. Kokkinaki (eds.). Springer International Publishing, Basel, Cham: 3-13.

Glaser, F. and Bezzenberger, L. (2015) Beyond Cryptocurrencies - A Taxonomy Of Decentralized Consensus, Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), May 26-29, Münster, Germany.

Global Legal Research Center (2014) Regulation of Bitcoin in Selected Jurisdictions, Abgerufen am 02.06.2016, von http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf.

Godsiff, P. (2015) Bitcoin: Bubble or Blockchain?, Abgerufen am 06.06.2016, von http://www.nemode.ac.uk/wp-content/uploads/2015/10/Godsiff-2015-KES-AMSTA.pdf.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013) Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, 29, 7, 1645–1660.

Haas, P., Blohm, I. and Leimeister, J. M. (2014) An Empirical Taxonomy of Crowdfunding Intermediaries, Proceedings of the 35th International Conference on Information Systems (ICIS 2014), December 14-17, Auckland, New Zealand.

Haas, P., Blohm, I., Peters, C. and Leimeister, J. M. (2015) Modularization of Crowdfunding Services – Designing Disruptive Innovations in the Banking Industry, Proceedings of the 36th International Conference on Information Systems (ICIS 2015), December 13-16, Fort Worth, Texas.

Hanseth, O. and Lyytinen, K. (2010) Design theory for dynamic complexity in infor-mation infrastructures: the case of building internet, Journal of Information Technology, 25, 1, 1-19.

Herbert, J. and Litchfield, A. (2015) A Novel Method for Decentralised Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology, Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015), January 27-30, Sydney, Australia.

Hileman, G. (2015) The Bitcoin Market Potential Index, Abgerufen am 03.06.2016, von: http://www.lse.ac.uk/economicHistory/study/PhDProgramme/JOb-Market-papers/Bitcoin-Market-Potential-Index-Hileman.pdf.

HM Treasury (2014) Digital currencies: call for information, Abgerufen am 01.04.2016, von https://www.gov.uk/

government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information.

Hughes, T.P. (1987) The Evolution of Large Technical Systems, in: The Social Con-struction of Technological Systems, W.E. Bijker, T.P. Hughes and T. Pinch (eds.). MIT Press, Cambridge, MA.

Jacob, F., Mittag, J. and Hartenstein, H. (2015) A Security Analysis of the Emerging P2P-Based Personal Cloud Platform MaidSafe, Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, August 20-22, Helsinki, Finland.

Juels, A., Kosba, A. and Shi, E. (2015) The Ring of Gyges: Using Smart Contracts for Crime, Abgerufen am 03.06.2016, von http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf.

Kayworth, T. and Sambamurthy, S. (2000) Facilitating Localized Exploitation and Enterprise-Wide Integration in the Use of IT Infrastructures: The Role of PC/LAN Infrastructure Standards, The DATA BASE for Advances in Information Systems, 31, 4, 54–80.

Kazan, E., Tan, C.W. and Lim, E. T. K. (2014) Towards a Framework of Digital Platform Disruption: A Comparative Study of Centralized & Decentralized Digital Payment Providers, Proceedings of the 25th Australasian Conference on Information Systems (ACIS 2014), December 8-10, Auckland, New Zealand.

Kiviat, T. I. (2015) Beyond Bitcoin: Issues in Regulating Blockchain Transactions, Duke Law Journal, 65, 3, 569–608.

Kling, R. (1992) Behind the Terminal: The Critical Role of Computing Infrastructure In Effective Information Systems' Development and Use, in: Challenges and Strategies for Research in Systems Development, W. Cotterman and J. Senn (eds.). Wiley, Chichester, New York: 365-414.

Kling, R. and Scacchi, W. (1982) The Web of Computing: Computing Technology as Social Organization, in: Advances in Computers, M.C. Yovits (ed.). Academic Press, New York: Vol. 21, 1–90.

Koblitz, N. and Menezes, A. J. (2015) Cryptocash, cryptocurrencies, and cryptocontracts, Designs, Codes and Cryptography, 78, 1, 87–102.

Kõlvart, M., Poola, M. and Rull, A. (2016) Smart Contracts, in: The Future of Law and eTechnologies, T. Kerikmäe und A. Rull (eds.). Springer International Publishing, Basel, Cham: 133–147.

Lamport, L., Shostak, R. and Pease, M. (1982) The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems, 4, 3, 382–401.

Lee, L. (2016) New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, Hasting's Business Law Journal, 12, 2, 81-132.

Loader, B. D. and Dutton, W. H. (2012) A decade in Internet time: the dynamics of the Internet and society, Information, Communication & Society, 15, 5, 609–615.

MacDonald, T. J., Allen, D. and Potts, J. (2016) Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking, Abgerufen am 03.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2749514.

MaidSafe (2016) Who we are, Abgerufen am 02.06.2016, von http://maidsafe.net/company.html.

Mainelli, M. and Smith, M. (2015) Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology), The Journal of Financial Perspectives, 3, 3, 38–59.

Mainelli, M. and von Gunten, C. (2014) Chain Of A Lifetime: How Blockchain Technology Might Transform Personal

Insurance, Abgerufen am 03.06.2016, von http://www.longfinance.net/images/Chain_Of_A_Lifetime_December2014.pdf.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D. (2015) The Internet of Things: Mapping the value beyond the hype, Abgerufen am 03.06.2016, von https://www.mckinsey.de/sites/mck_files/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf.

Marian, O. (2013) Are Cryptocurrencies Super Tax Havens?, Michigan Law Review First Impressions, 112, 38–48.

Mattila, J. (2016) The Blockchain Phenomenon. The Disruptive Potential of Distributed Consensus Architectures, Abgerufen am 03.06.2016, von http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf.

Mattila, J. and Seppälä, T. (2015) Blockchains as a Path to a Network of Systems, Abgerufen am 03.06.2016, von http://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-45.pdf.

McKinsey & Company (2015) Beyond the Hype: Blockchains in Capital Markets, Abgerufen am 03.06.2016, von http://www.mckinsey.com/industries/financial-services/our-insights/beyond-the-hype-blockchains-in-capital-markets.

Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A. (2001) Handbook of Applied Cryptography, 5th ed., CRC Press, Boca Raton, FL.

Mizrahi, A. (2015) A blockchain based property ownership recording system, Abgerufen am 03.06.2016, von http://chromaway.com/papers/A-blockchain-based-property-registry.pdf.

Morabito, V. (2016) The Future of Digital Business Innovation. Trends and Practices, Springer International Publishing, Cham, Basel.

Mougayar, W. (2015) The Crypto-Technology and Bitcoin Landscape, Abgerufen am 30.03.2016, von http://startupmanagement.org/2015/03/03/the-crypto-technology-and-bitcoin-landscape/.

Mullender, S. (1990) Introduction, in: Distributed Systems, S. Mullender (ed.). ACM Press, New York, NY.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, Abgerufen am 03.06.2016, von https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E. W., Miller, A. and Goldfeder, S. (2016) Bitcoin and Cryptocurrency Technologies, Abgerufen am 02.06.2016, von https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf.

NASDAQ (2015) Nasdaq Linq Enables First-Ever Private Securities Issuance Documented With Blockchain Technology, Abgerufen am 03.06.2016, von http://ir.nasdaq.com/releasedetail.cfm?ReleaseID=948326.

National Institute of Standards and Technology (2015) Secure Hash Standard (SHS), Abgerufen am 03.06.2016, von http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

Ølnes, S. (2015) BEYOND BITCOIN - Public Sector Innovation Using the Bitcoin Blockchain Technology, Abgerufen am 03.06.2016, von http://ojs.bibsys.no/index.php/Nokobit/article/view/264/228.

Panikkar, S., Nair, S., Brody, P. and Pureswaran, V. (2015) ADEPT: An IoT Practitioner Perspective, Abgerufen am 22.04.2016, von https://de.scribd.com/doc/252917347/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.

Peters, G. W. and Panayi, E. (2015) Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet

of Money, Abgerufen am 03.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2692487.

Peters, G. W., Panayi, E. and Chapelle, A. (2015) Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective, Abgerufen am 03.06.2016, von http://arxiv.org/pdf/1508.04364.pdf.

Pilkington, M. (2016) Blockchain Technology: Principles and Applications, Abgerufen am 03.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660.

Porra, J. (1999) Colonial Systems, Information Systems Research, 10, 1, 38–69.

Porter, M. E. and Heppelmann, J. E. (2014) How Smart, Connected Products Are Transforming Competition, Harvard Business Review, 92, 11, 64-88.

Pureswaran, V. and Brody, P. (2015) Device democracy. Saving the future of the Internet of Things, Abgerufen am 03.06.2016, von http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF.

Pureswaran, V., Panikkar, S. and Nair, S. (2015) Empowering the edge. Use case abstract for the ADEPT proof-of-concept, Abgerufen am 03.06.2016, von http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03666USEN&attachment=GBE03666USEN.PDF.

PwC (2016) Blurred lines: How FinTech is shaping Financial Services, Abgerufen am 03.06.2016, von http://www.pwc.com/gx/en/advisory-services/FinTech/PwC FinTech Global Report.pdf.

Reid, F. and Harrigan, M. (2012) An Analysis of Anonymity in the Bitcoin System, in: Security and Privacy in Social Networks, Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony and A. Pentland (eds.). Springer, New York, NY: 197-223.

RippleLabs (2016) What is Ripple?, Abgerufen am 23.05.2016, von https://ripple.com.

Rosenfeld, M (2012) Overview of Colored Coins, Abgerufen am 03.06.2016, von https://bitcoil.co.il/BitcoinX.pdf.

Santander Innoventures, Oliver Wyman and Anthemis Group (2015) The Fintech 2.0 Paper: rebooting financial services, Abgerufen am 07.04.2016, von https://www.finextra.com/finextra-downloads/newsdocs/the fintech 2 0 paper.pdf.

Schäfer, G. (2003) Netzsicherheit: Algorithmische Grundlagen und Protokolle, dpunkt.verlag, Heidelberg.

Schoder, D. and Fischbach, K. (2002) Peer-to-Peer, Wirtschaftsinformatik, 44, 6, 587–589.

Schollmeier, R. (2001) A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing (P2P 2001), August 27-29, Linköping, Sweden.

Scott, B. (2016) How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?, Abgerufen am 03.06.2016, von http://www.unrisd.org/80256B3C005BCCF9/%28httpAuxPages%29/196AEF663B617144C1257F550057887C/$file/Brett%20Scott.pdf.

Sicari, S., Rizzardi, A., Grieco, L. A. and Coen-Porisini, A. (2015) Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, 76, 146–164.

Siegel, D. (2016) Understanding The DAO Attack, Abgerufen am 29.08.2016, von http://www.coindesk.com/understanding-dao-hack-journalists/.

Silverberg, K., French, C., Ferenzy, D. and Van den Berg, S. (2015) Banking on the Blockchain. Reengineering the Financial Architecture, Abgerufen am 03.06.2016, von https://www.iif.com/file/13405/download?token=XmUGI83c.

Stallings, W. (2003) Network Security Essentials: Applications and Standards, 2nd ed., Pearson Education, Upper Saddle River, NJ.

Stankovic, J. A. (2014) Research Directions for the Internet of Things, IEEE Internet of Things Journal, 1, 1, 3–9.

Star, L. S. and Ruhleder, K. (1996) Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces, Information Systems Research, 7, 1, 111–134.

Swan, M. (2015) Blockchain. Blueprint for a New Economy, O´Reilly Media, Sebastopol, CA.

Swanson, T. (2014) Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management, Abgerufen am 03.06.2016, von https://s3-us-west-2.amazonaws.com/chainbook/Great+Chain+of+Numbers+A+Guide+to+Smart+Contracts%2C+Smart+Property+and+Trustless+Asset+Management+-+Tim+Swanson.pdf.

Swanson, T. (2015) Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, Abgerufen am 03.06.2016, von http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

Szabo, N. (1997) Formalizing and Securing Relationships on Public Networks, Abgerufen am 03.06.2016, von http://journals.uic.edu/ojs/index.php/fm/article/view/548/469#1.

Tasca, P. (2015) Digital Currencies: Principles, Trends, Opportunities, and Risks, Abgerufen am 03.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657598.
Tschorsch, F. and Scheuermann, B. (2015) Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, Abgerufen am 03.06.2016, von https://eprint.iacr.org/2015/464.pdf.

Tsilidou, A. L. and Foroglou, G. (2015) Further applications of the blockchain, Abgerufen am 03.06.2016, von https://www.researchgate.net/publication/276304843_Further_applications_of_the_blockchain.

Tuesta, D., Alonso, J., Vegas, I., Cámara, N., Pérez, M. L., Urbiola, P. and Sebastián, J. (2015) Smart contracts: the ultimate automation of trust?, Abgerufen am 03.06.2016, von https://www.bbvaresearch.com/wp-content/uploads/2015/10/Digital_Economy_Outlook_Oct15_Cap1.pdf.

Van de Velde, J., Scott, A., Sartorius, K., Dalton, I., Shepherd, B., Allchin, C., Dougherty, M., Ryan, P. and Rennick, E. (2016) Blockchain in Capital Markets. The Prize and the Journey, Abgerufen am 03.06.2016, von http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/feb/BlockChain-In-Capital-Markets.pdf.

Van Valkenburgh, P., Dietz, J., De Filippi, P., Shadab, H., Xethalis, G., Bollier, D., Crawford, C., Narayan A. and Narayan, A. (2015) Distributed Collaborative Organisations. Distributed Networks & Regulatory Frameworks, Abgerufen am 20.05.2016 von http://bollier.org/sites/default/files/misc-file-upload/files/DistributedNetworksandtheLaw report%2C Swarm-Coin Center-Berkman.pdf.

Vermesan, O., Friess, P., Guillemin, P., Sundmaeker, H., Eisenhauer, M., Moessner, K., Le Gall, F. and Cousin, P. (2013) Internet of Things Strategic Research and Innovation Agenda, in: Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, O. Vermesan and P. Friess (eds.). River Publishers, Aalborg: 7–152.

Vora, G. (2015) Cryptocurrencies: Are Disruptive Financial Innovations Here?, Modern Economy, 6, 7, 816-832.

Walport, M. (2015) Distributed Ledger Technology: beyond block chain, Abgerufen am 03.06.2016, von https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

Wan, T. and Hoblitzell, M. (2014) Bitcoin. Fact. Fiction. Future., Abgerufen am 03.06.2016, von http://dupress.com/articles/bitcoin-fact-fiction-future/.

Wattenhofer, R. and Decker, C. (2015) A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels, in: Stabilization, Safety, and Security of Distributed Systems. 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings, A. Pelc and A. A. Schwarzmann (eds.). Springer International Publishing, Basel, Cham: 3–18.

Weill, P. and Broadbent, M. (1998) Leveraging the New Infrastructure, Harvard Business School Press, Cambridge, MA.

Whitmore, A., Agarwal, A. and Da Xu, L. (2015) The Internet of Things - A survey of topics and trends, Information Systems Frontiers, 17, 2, 261–274.

Wilson, D. and Ateniese, G. (2015) From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain, in: Network and System Security. 9th International Conference, NSS 2015, New York, NY, USA, November 3-5, 2015, Proceedings, M. Qiu, S. Xu, M. Yung and H. Zhang (eds.). Springer International Publishing, Basel, Cham: 368–375.

Winkler, R. (2015) Fedcoin - how banks can survive blockchains, Abgerufen am 03.06.2016, von https://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000368569.pdf.

Wood, G. and Buchanan, A. (2015) Advancing Egalitarianism, in: Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data, D. LEE Kuo Chuen (ed.). Elsevier, London, San Diego, CA, Waltham, MA, Oxford: 385–402.

World Economic Forum (2015) Deep Shift - Technology Tipping Points and Societal Impact, Abgerufen am 03.06.2016, von http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

Wörner, D. and von Bomhard, T. (2014) When Your Sensor Earns Money: Exchanging Data for Cash with Bitcoin, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2014), September 13-17, Seattle, Washington.

Wortmann, F. and Flüchter, K. (2015) Internet of Things. Technology and Value Added, Business and Information Systems Engineering, 57, 3, 221–224.
Wright, A. and De Filippi, P. (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia, Abgerufen am 03.06.2016, von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

Xethalis, G. E., Moriarty, K. H., Claassen, R. and Levy, J. B. (2016) An Introduction to Bitcoin and Blockchain Technology, Abgerufen am 03.06.2016, von http://www.kayescholer.com/docs/IntrotoBitcoinandBlockchainTechnology.pdf.

Yermack, D. (2015) Corporate Governance and Blockchains, Abgerufen am 03.06.2016, von http://www.nber.org/papers/w21802.pdf.

Zhang, Y. and Wen, J. (2015) An IoT Electric Business Model Based on the Protocol of Bitcoin, Proceedings of the 18th International Conference on Intelligence in Next Generation Networks (ICIN 2015), February 17-19, Paris, France.

Zimmerman, A. (2007) A Socio-Technical Framework for Cyberinfrastructure De-sign, Proceedings of the e-Social Science Conference, October 7-9, Ann Arbor, MI, USA.

Zohar, A. (2015) Bitcoin: Under the Hood, Communications of the ACM, 58, 9, 104–113.

Zyskind, G., Nathan, O. and Pentland, A. (2015) Enigma: Decentralized Computation Platform with Guaranteed Privacy, Abgerufen am 01.05.2016, von http://arxiv.org/pdf/1506.03471v1.pdf.

8. ÜBER UNS

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Das Fraunhofer-Institut für Angewandte Informationstechnik FIT beschäftigt rund 110 Wissenschaftler, darunter Informatiker, Sozial- und Wirtschaftswissenschaftler, Psychologen und Ingenieure. Unter einer gemeinsamen Leitung findet eine enge Zusammenarbeit mit dem Lehrstuhl für Informationssysteme an der RWTH Aachen statt. Die interdisziplinären Teams haben es sich zur Aufgabe gemacht, die Zukunft mit neuen marktorientierten Produkten zu gestalten, indem sie Wissen aus der Informationstechnologie mit Fragen aus anderen Lebensbereichen verknüpfen. Daraus resultieren die Validierung, der Entwurf und die Implementierung für innovative Kundenlösungen. Die Forschungsbereiche umfassen Kooperationssysteme, Life Science Informatik, Risikomanagement und Entscheidungsunterstützung, User-Centered Computing sowie wirtschaftsinformatische Fragestellungen.

Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT
Die bundesweit erste Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT vereint die Forschungsbereiche Finanz- & Informationsmanagement an den Standorten Augsburg und Bayreuth. Die ausgewiesene Expertise an der Schnittstelle von Finanzmanagement, Informationsmanagement und Wirtschaftsinformatik sowie die Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichen Niveau mit einer kunden- und lösungsorientierten Arbeitsweise zu verbinden, sind unsere herausragenden Merkmale.

www.fit.fraunhofer.de/wi

Prof. Dr. Gilbert Fridgen
Fraunhofer-Institut für Angewandte Informationstechnik FIT
Projektgruppe Wirtschaftsinformatik
Universität Bayreuth
+49 921 55-4711
gilbert.fridgen@fit.fraunhofer.de

Prof. Wolfgang Prinz PhD
Fraunhofer-Institut für Angewandte Informationstechnik FIT
Schloss Birlinghoven
53754 Sankt Augustin
+49 2241 14-2730
wolfgang.prinz@fit.fraunhofer.de

Prof. Dr. Nils Urbach
Fraunhofer-Institut für Angewandte Informationstechnik FIT
Projektgruppe Wirtschaftsinformatik
Universität Bayreuth
+49 921 55-4712
nils.urbach@fit.fraunhofer.de

Prof. Dr. Thomas Rose
Fraunhofer-Institut für Angewandte Informationstechnik FIT
Schloss Birlinghoven
53754 Sankt Augustin
+49 2241 14-2798
thomas.rose@fit.fraunhofer.de

www.fit.fraunhofer.de/blockchain