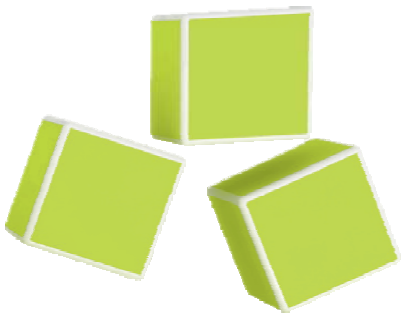
AUDIT & ADVISORY • TAX • LEGAL • CONSULTING

bakertilly

Blockchain: Praktische Anwendungen jenseits von Kryptowährungen

bakertilly.de

Praktische Anwendungen der Blockchain rücken in den Fokus



Als sich 1991 Haber und Stornetta erstmals mit kryptographisch verbundenen Informationsblöcken beschäftigten, konnten sie noch nicht ahnen, welche Wellen die 17 Jahre später eingeführte, erste Blockchain-Anwendung losbrechen würde.[1]

Bekannt geworden als das Protokoll hinter dem Bitcoin, verschoben sich die Diskussionen um die Potenziale dieser Technologie zu Unternehmen, Börsenhändlern und Finanzdienstleistern. Wenngleich der Kryptowährungshype der Jahre 2016 und 2017 nun hinter uns zu liegen scheint, steht die Blockchain mit ihren enormen Möglichkeiten noch ganz am Anfang. Gegenüber dem Risiko der hohen Preisvolatilität des Bitcoins und anderen Kryptowährungen bietet die Technologie eine Vielzahl von Ansätzen über die Funktion als reines Spekulations-/Anlageobjekt hinaus. Nachdem sich Baker Tilly im Sommer 2018 ausführlich mit den Chancen und Herausforderungen der finanziellen Nutzungsmöglichkeiten von Blockchain-Währungen beschäftigt hat, widmet sich diese Publikation nun den praktischen Anwendungen der Blockchain. Dabei soll dieser Beitrag zu einem besseren Verständnis der gegenwärtig stattfindenden technologischen Disruptionen beitragen, um darauf aufbauend neue Geschäftsmodelle zu entwickeln und Governance-Systeme zu optimieren.

Vor- und Nachteile der Technologie hinter dem Bitcoin

Die vielfältigen Einsatzgebiete der Blockchain-Technologie machen sie zu einem universalen Disruptor in jeder Branche. Die Vorteile, je nach ihrer individuellen Ausgestaltung, sind dabei in der Regel fallende Kosten für Suchanfragen, Koordination und Entscheidungsfindung verbunden mit fallenden Kosten für die Durchsetzung wirtschaftlicher Vereinbarungen und eine Zunahme an Datenintegrität, Manipulationsschutz, Korruptionsresistenz sowie Anreize für die direkte Zusammenarbeit ohne Intermediäre. Diese Fülle an gewichtigen Vorteilen gegenüber klassischen Datenaustausch-Protokollen ist so immens, dass diese Technologie nicht außen vor gelassen werden kann.

Demgegenüber steht jedoch auch eine Anzahl an noch ungelösten Herausforderungen und Umsetzungshemmnissen. Der Energieverbrauch des PoW-Algorithmus vom Bitcoin zur Konsensfindung beträgt jetzt bereits mehr als der von Irland[2], obwohl zurzeit nicht einmal genügend Transaktionen validiert werden könnten, um die Zahlungsströme einer deutschen Großstadt aufrechtzuerhalten. Solange noch Infrastrukturschwierigkeiten, wie die Transaktionsverarbeitungskapazitäten sowie die geringe Zugänglichkeit für die breite Bevölkerung, bestehen, werden Blockchain-Lösungen in ihren Kinderschuhen steckenbleiben.

1) Vgl. HABER/STORNETTA (1991), S. 99-111.
2) Vgl. DE VRIES (2018), S. 1.

Die Unverfälschbarkeit der Datenkette

Das Ziel der Blockchain-Technologie ist die Erzeugung „digitaler Datensicherheit“ gemessen am „Trust-Level“ notariell beglaubigter Dokumente in physischer Form. Um dieser Vertrauensvorgabe gerecht zu werden, ist eine der Haupteigenschaften der Blockchain ihre Offenheit gegenüber allen Netzwerkteilnehmern.

Das heißt, jeder Teilnehmer hat Zugang zu allen jemals auf der Blockchain aufgezeichneten Informationen (beispielsweise Transaktionen). Durch ihre weiteren Eigenschaften – wie Dezentralisierung, Mining, mathematische Konsensfindung – markiert die Nutzung der Blockchain-Technologie gleichzeitig auch die Entstehung von Distributed Ledger Informationen. Die Begriffe Blockchain und Distributed Ledger Technology (DLT) stellen somit Synonyme dar. Um die Sicherheit von auf einer Blockchain gespeicherten Daten – auch bezeichnet als Blockchain Data-Safety-Property – in Bezug auf digitale Änderungen oder Manipulationen jeglicher Art zu verstehen, stellen Sie sich den „Block“ als ein Objekt vor, welches maßgeblich in drei Dimensionen unterteilt ist: **Daten, Hashwert, Vorgänger.**

Daten

Im Bitcoin-Blockchain-Netzwerk entsprechen Daten „Mengen/Wert“-Transaktionen von Besitzer A zu Besitzer B.

Hashwert

Ein Hashwert ist ein einzigartiger und eindeutiger digitaler Fingerabdruck des entsprechenden Blocks sowie dessen gesamten Dateninhaltes. Der „geforderte“ Block-Hashwert wird dabei bei der Block-Generierung netzwerkseitig berechnet. Jede Änderung des Blockdateninhaltes führt dabei zur Veränderung des Hashwertes.

Fälschungssicherer Kettenstruktur-Aufbau

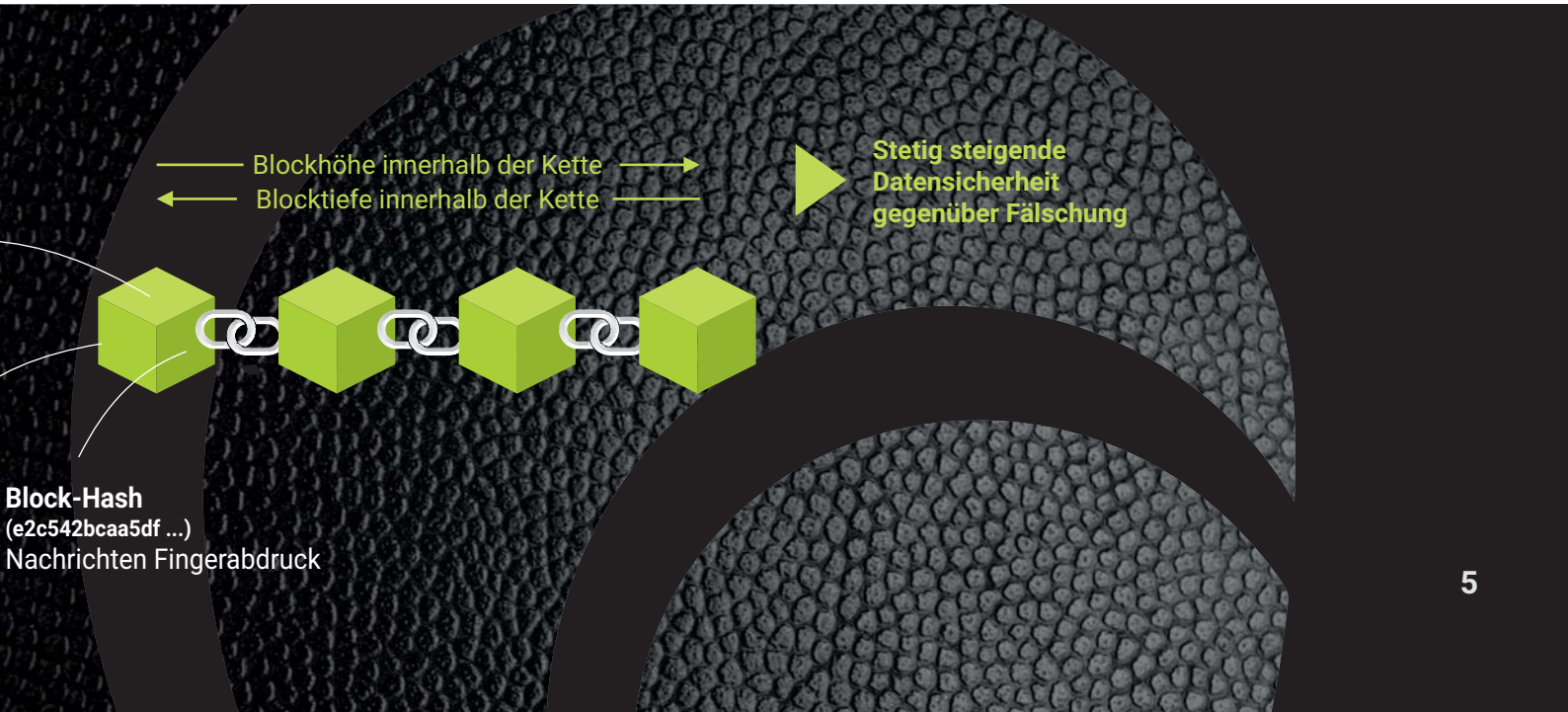
Daten
Nachrichten-Inhalt

Block-Hash-Vorgänger
(b8aef92bcc6df...)
Nachrichten-Verkettung

Block-Hash-Vorgänger

Die Verkettung der Daten mit Hilfe des Block-Vorgänger-Hashwertes des zuvor generierten Blocks führt letztendlich zur Entstehung der Blockchain – eine in sich valide Datenkette aufeinander aufbauender Informationen. Dabei würde die geringfügigste Datenänderung zuvor generierter und validierter Netzwerk-Block-Hashwerte die Konsistenz aller nachfolgend generierten Blöcke der Kette maßgeblich beeinflussen („Out of Consensus“).

Die Unverfälschbarkeit der auf einer Blockchain gespeicherten Daten resultiert aus der logischen Verzahnung dieser drei Informationsdimensionen miteinander mittels komplexer Mathematik. Die Fortschreibung der Datenkette durch weitere geforderte „Block-Hashwerte“ führt somit zur Unabänderbarkeit eindeutiger sowie einzigartiger digitaler Signaturen. Die Block-Fingerabdrücke können im Bruchteil von Sekunden mittels nur einer Rechenoperation von jedem Rechner individuell auf die Integrität ihres Dateninhalts validiert werden. Die nachstehende Abbildung verdeutlicht den Sachverhalt graphisch.



Die Prinzipien der Datensicherheit und Sparsamkeit

Um die Sicherheit der Verschlüsselung auf einer Blockchain gespeicherter Daten zu verstehen, ist es wichtig, die zugrundeliegende Verschlüsselungstechnologie (Public Key Kryptographie) zur Hashwert-Erstellung zu kennen. Technisch betrachtet ist ein Hashwert eine hexadezimale Zeichenfolge, bestehend aus Zahlen von 0 bis 9 und Buchstaben von a bis f. Die Verschlüsselung von Klartext-Informationen zu einem auf Validität überprüfbaren Hashwert mittels mathematisch eindeutiger Schlüssel-Paar-Kombination ist hierbei ein komplexer Vorgang. Aus Informationsverarbeitungssicht können „gehashte" Informationen nur mittels privater Schlüssel entschlüsselt werden. Eine 100%ige Überprüfung der Daten auf Echtheit kann jedoch durch einen frei verfügbaren öffentlichen Schlüssel erfolgen. Das bedeutet, solange der private Schlüssel unter „Verschluss" bleibt, besitzt nur der tatsächliche Informationsverfasser Zugang zu seinen Daten. Die Echtheitsüberprüfung und Zertifizierung der Daten kann aber jeder Netzwerkteilnehmer selbständig mittels öffentlich (public) verfügbarer Schlüssel automatisch vornehmen.

Die praktisch „nicht hackbare Datenverschlüsselung" durch die Hash-Funktion, die fortschreitende Verschränkung dieser Informationen miteinander sowie die informationstechnologisch eindeutige und fehlerfreie Datenüberprüfung mittels öffentlich zugänglichem Schlüssel, machen die Blockchain nach heutigem Wissensstand zu einem sehr sicheren Werkzeug für die dezentrale Datenorganisation – und setzen die damit verbundene Notwendigkeit bestmöglichen Datenschutzes um. Die Fähigkeit der automatischen Datenverifizierung resultiert dabei aus der eindeutigen Informationsverschränkung und ihrer stetigen Fortschreibung in der Datenkette. Kurz gesagt: Eine Blockchain wächst mit zunehmendem „Alter" im Verhältnis zu den auf ihr gesicherten Daten kontinuierlich im Volumen an und benötigt somit entsprechend freien Festplattenplatz. So beläuft sich die zu speichernde Datenmenge der Blockchain-Lösung „Bitcoin" heutzutage auf insgesamt mehr als 217 GB. Die Optimierung der Datensparsamkeit durch wirksame Informationskomprimierung wird daher eine zunehmend wichtige Rolle in der Zukunft der Blockchain-Technologie spielen.

Vielfältige Möglichkeiten zur Nutzung der Blockchain

Mittels der Blockchain-Technologie wird es möglich, digitale Informationen dezentral zu organisieren. Dabei werden alle relevanten Daten auf allen Rechnern im System verteilt und in Echtzeit laufend miteinander synchronisiert. Kurzum ist die Blockchain also die synchrone Kopie eines verifizierten Datenpakets auf allen angeschlossenen Netzwerkknoten (Nodes).

Zu jedem Zeitpunkt existiert damit im Rechnernetzwerk genau ein akzeptierter Datenvaliditätszustand, den alle Netzwerkknoten teilen und akzeptieren. Die konzeptionellen Nutzungsmöglichkeiten dieser Technologie übersteigen daher die gegenwärtig real existierenden Blockchain-Anwendungen, genannt dezentrale Applikationen (dApps), um ein Vielfaches. Bereits jetzt ist jedoch erkennbar, dass die Blockchain als künftige Grundlagentechnologie zur Datenbankverwaltung in vielen verschiedenen Branchen eine wesentliche Rolle spielen kann.

Zahlreiche Industriezweige beginnen die Signifikanz dieses Technologiedurchbruchs zu verstehen und entwickeln Konzeptvorstellungen für den Technologieeinsatz. So arbeiten Branchengrößen wie Microsoft, IBM, SAP, Amazon oder Oracle bereits heute an neuartigen Cloud-Blockchain-basierten Plattformlösungen (BaaS) für morgen. Neben diesen konkreten Implementierungstätigkeiten entsteht darüber hinaus ein wissenschaftlich geprägter Diskurs über weitere Einsatzmöglichkeiten der Technologie. Zahlreiche Studien und Analysen beleuchten die Vor- und Nachteile der Blockchain-Technologie, um universelle Antworten auf bestehende Technologierestriktionen der Blockchain zu finden. Trotz der zu bewältigenden Herausforderungen zeichnet sich aus einer Vielzahl an Umfrageergebnissen ein Einsparungs- und Vereinfachungspotenzial für die Abwicklung existierender Geschäftsprozesse ab – mittels Nutzung der Blockchain-Technologie. Allen voran stehen dabei die von Deubel et al. identifizierten Industriezweige[3]

- Finanzdienstleistungen,
- Medien- & Werbeindustrie,
- Supply Chain Management,
- Energiewirtschaft/CO_2-Ausstoß,
- E-Commerce und
- Gesundheitswesen.

3) Vgl. DEUBEL et al. (2017), S. 1.

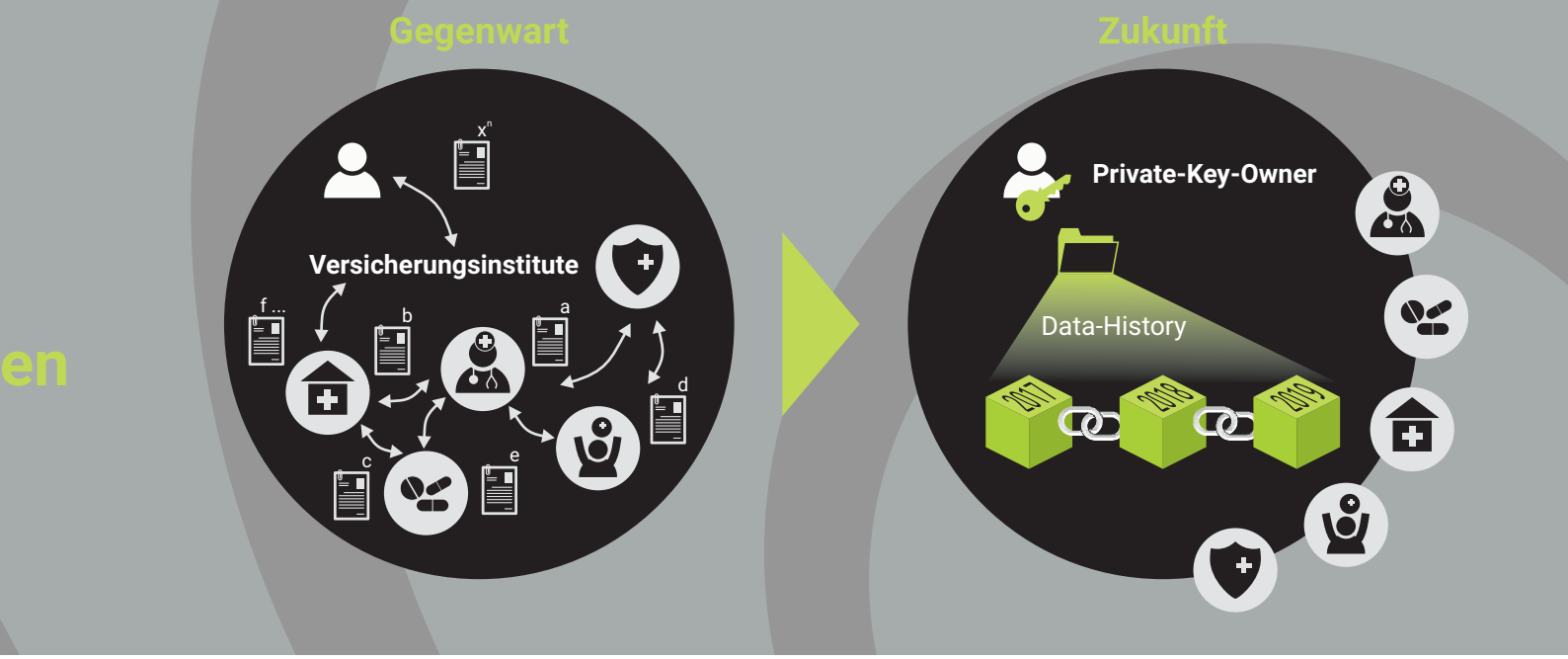
Disruption durch die Blockchain: Die Gesundheitsakte

Die zukünftige Vernetzung im Gesundheitswes

In einem Zeitalter der digitalen Wirtschaft, der zunehmenden Verbreitung von disruptiven Technologien sowie einer Durchdringung des Alltages mit Technologien, wie Smart Home, digitalem Entertainment on Demand, Fitness und Health Apps und der nahezu vollständigen Vernetzung sämtlicher Lebensbereiche, steigt auch die Erwartungshaltung an eine Vernetzung im Gesundheitswesen.

Der verzögerungsfreie und ungestörte Datenfluss wird zur Selbstverständlichkeit – die Industrie 4.0 lebt es uns vor. Die Funktionalität von Smartphones und deren integrierten Apps schafft schier unendliche Möglichkeiten und setzt die Benchmark für eingebettete Systeme. Im Gesundheitssystem dagegen sehen wir uns derzeit mit einer immens hohen Fragmentierung konfrontiert. Dateninseln sowie hohe Anforderungen an Datensicherheit erschweren den Austausch von Daten, behindern und unterdrücken einen effizienten Datenfluss und stehen somit nicht nur dem gewohnten „User-Erlebnis“ entgegen, sondern erschweren auch eine effiziente und effektive Behandlung. Es existieren verschiedene Datensätze bei den verschiedenen Diagnose- und Therapie-Beteiligten, welche meist parallel und inkonsistent fortgeschrieben werden. Eine komplette Patientenakte mit der Garantie auf Vollständigkeit und Richtigkeit gibt es somit schlichtweg nicht. Stattdessen entwickeln sich verschiedene Datensätze unabhängig voneinander fort. Gleichzeitig ist eine Trendwende zu beobachten: Der Patient wird zunehmend mündiger, holt Zweitmeinungen ein, wählt Ärzte und Spezialisten eigenständig aus und nimmt aktiv an der Diagnose und Behandlung teil. Diese Demokratisierung der Medizin führt zwangsläufig zum zunehmenden Wunsch nach der Kontrolle über die eigenen Daten. Eine zunehmende Mobilität von Menschen auf europäischen und internationalen Arbeitsmärkten ist ein weiterer Aspekt, der die Nachfrage nach digitalen und damit mobilen Krankenakten steigen lässt.

Die Anwendungsgebiete der elektronischen Krankenakte sind dabei vielfältig. Gemeinsam ist allen die Vernetzung von Anamnesen, Diagnostik und Therapie. Auch können weitere Bereiche im Ökosystem Medizin, wie etwa Forschung und Entwicklung, Abrechnung sowie Versicherungen, integriert werden. So können anonymisierte Patientendaten der Forschung und damit dem Aufbau von Datenbanken zur Verfügung gestellt werden (Big Data). Gleichzeitig können die Wirkungen von Therapien und Medikamenten nicht nur an die behandelnden Ärzte, sondern auch die Pharmaindustrie zurückgespielt werden. Ärzte und Krankenhäuser können ihre Befunde und Therapien nahtlos an Apotheken, Therapeuten und Nachsorgeinstitute weitergeben. Laborbefunde können vor, während und nach der Behandlung digital eingebunden werden und somit allen gleichzeitig zur Verfügung gestellt werden. Weitere Anwendungsgebiete können in der Telemedizin bestehen. Hier werden Ärzte online oder via App konsultiert. Dabei kann es sich um den Erstbesuch in minderschweren Fällen handeln, die Einbindung



von Spezialisten in der Anamnese, Diagnose oder Therapie sowie die anschließende Nachsorge und physiotherapeutische Behandlung. Auch kann die Telemedizin Entwicklungsländern eine medizinische Grundversorgung zur Verfügung stellen oder in anderen infrastrukturschwachen (bzw. ländlichen Gegenden) ein höheres Niveau der Gesundheitsversorgung gewährleisten. Als gemeinsame Anforderung lässt sich der nahtlose, zeitnahe, vollständige und konsistente Austausch von Patientendaten formulieren, was nur in Form einer digitalen Patientenakte möglich ist.

Bei der elektronischen Verarbeitung von Patientendaten, deren digitalem Versand und Abruf über verschiedene Geräte und Plattformen, ist die Datensicherheit zentrales Element. Dabei soll zum einen die Sicherheit der Daten gegen Verlust, Verfälschung sowie unberechtigten Zugriff geschützt werden. Zum anderen soll eine Anonymisierung und Aggregation zu Massendaten möglich sein, um diese der Forschung und möglicherweise auch Versicherungskonzernen zur Verfügung stellen zu können. Das alleinige Vertrauen des Patienten in die Integrität eines einzelnen Dienstleisters, der seine Daten verwaltet, stößt an seine Grenzen, wenn Doubletten erstellt werden und diese weitergegeben werden müssen oder sollen. Ebenso ist hier die Datensicherheit von der verwendeten Speicherlösung des Anwenders – meist einer Cloud-Anwendung – abhängig. Anstelle der Speicherung auf einem zentralen Server werden die Daten als verschlüsselte Kopie innerhalb der Blockchain gespeichert und somit auf einer Vielzahl von Rechnern gleichzeitig verfügbar gemacht. Durch Abgleich untereinander werden die Daten validiert und authentifiziert. Der Patient behält dabei jederzeit die vollständige Kontrolle über seine Daten. Gleichzeitig können die Daten – einmal in der Blockchain hinterlegt – nicht verloren gehen. Einen Zugriff kann ausschließlich der Patient gewähren und dabei Umfang, Detaillierungsgrad und Anonymisierungsgrad sowie Zeitdauer festlegen. Weiterhin sind die Daten gegen Veränderung und Fälschung sicher, da jede Interaktion mit dem Datensatz gespeichert wird und somit auditierbar, nachvollziehbar und transparent ist. Somit kann auch im Anschluss der Behandlung eine sachgerechte Abrechnung auf Basis der erbrachten ärztlichen Leistungen und Fallziffern automatisiert erfolgen. Versicherungen können diese anonymisiert – oder nach Patientenfreigabe individualisiert – prüfen und zur Zahlung freigeben.

Die Digitalisierung von Patientendaten ermöglicht damit einen bisher nicht dagewesenen Effizienzgewinn in der Behandlung von Patienten und erstmalig eine vollständige Integration in eine Prozesskette. Die Blockchain-Technologie kann dadurch ein zentrales Element in der Verschlüsselung und Sicherung der Daten darstellen.

Disruption durch die Blockchain: Initial-Coin-Offerings

Eine zentrale Funktion des Kapitalmarktes – Investoren und Unternehmer zusammenzuführen – hat sich seit Jahrzehnten prozessual kaum verändert. Über Börsengänge, Platzierungen und spezielle Investmentformen erstreckt sich der fest definierte Instrumentenkasten, der besonders in Deutschland hohe Standards an den Gläubigerschutz stellt.

Seit 2015 ist jedoch, mit dem ersten Aufkommen von sog. Initial-Coin-Offerings (ICOs), erheblich mehr Dynamik in diese Prozesse gekommen. Während die technologischen Neuerungen und digitalen Handels- und Abwicklungssysteme grundlegend den Sekundärmarkt des Börsenhandels in den letzten Jahrzehnten umgestaltet haben, versprechen nun Blockchain-Anwendungen gewaltige Effizienzsteigerungen auf den immer noch komplexen und kostenintensiven Wertpapieremissionsmärkten. Als Alternative zu klassischen Börsengängen, die in der Regel mit einem langwierigen Prozess der Listung und Kontrolle von Publizitätspflichten und Regulierungsauflagen einhergehen, hat sich insbesondere im internationalen Start-up- und FinTech-Bereich das neue Finanzierungskonzept etabliert. Unter Nutzung der Blockchain-Technologie erfolgt am Kapitalmarkt ein einfacherer, zügigerer und kostengünstigerer Zugang zu Crowdinvestment-Mitteln. Hierbei kann über das Internet ein fast unbegrenzter Kreis potenzieller Investoren angesprochen werden. Dabei werden zur Eigenkapitalaufnahme keine Aktien, Anleihen oder ähnliche Titel emittiert, sondern den Kapitalgebern vom Unternehmen digital hergestellte sog. Coins oder Token zur Verfügung gestellt, die in ihrer technologischen Ausgestaltung genau spezifizierte Eigenschaften aufweisen. Daher unterscheidet die FinTech-Branche bereits jetzt die Begriffe „Kryptowährung“, „Altcoin“und „Token“.

Die Untergliederung zwischen Altcoin und Token mittels der Finanzierungsformen ICO und Token Sales lässt sich dabei wiederum grundlegend unterscheiden in die Emission von Krypto-Coins, für welche Unternehmen vor der Ausgabe eine eigene Blockchain programmieren müssten, und Krypto-Token, die als Derivate auf bereits existierenden Krypto-Coin-Blockchains (wie beispielsweise von Ethereum) aufbauen. So stellt sich für jedes Unternehmen ganz konkret die Frage, wie sie ihren ICO individuell ausgestalten wollen: Angefangen bei sogenannten Utility-Token, die dem Besitzer das Nutzungsrecht für Dienstleistungen gewähren, über Security-Token, welche als digitalisierte Wertpapiere mit der Aussicht auf Wertsteigerung angesehen werden können, bis hin zu Equity-Token, welche den Besitzern auch Anteilsrechte einräumen, sind kaum technische Grenzen gesetzt.

Der Theorie nach soll es so insbesondere für Unternehmen mit digitalen Geschäftsmodellen möglich werden, in kürzerer Zeit mit weniger regulatorischen Einschränkungen Kapital zu sammeln, und für Gläubiger, ihr (Wagnis)Kapital in ein noch diversifizierteres Portfolio an Digitalunternehmen zu investieren. Innovative Geschäftsmodelle können damit auch bereits von Anfang an durch innovative Finanzierungsmaßnahmen unterstützt werden und die Investoren erhalten in Abhängigkeit von der Unternehmensentwicklung, einhergehend mit der Entwicklung der unternehmensspezifischen Kryptowährung, hohe Erfolgsbeteiligungen bzw. hohe Wertsteigerungen ihrer initial gekauften Token. Ebenso öffnen Krypto-Token den Anlagemarkt für Kleinanleger: Im Gegensatz zu klassischen Aktienkäufen unterliegen Kryptowährungen keinerlei Stückelungsbeschränkung. So könnten sich Geringverdiener bereits mit Cent-Beträgen an ICOs beteiligen und ggf. davon profitieren. Diese gewichtigen Vorteile sind nicht von der Hand zu weisen und werden mittelfristig die Finanzbranche weiter verändern.

Wie man dieses Mittel erfolgreich anwendet, hat das Berliner Start-up Wyskers mit seinem auf der Ethereum-Blockchain aufbauenden Token „wys“ gezeigt. Mit einem attraktiven

Geschäftsmodell, welches auf einem innovativen Werbesystem für Online Shopping basiert, transparenten Nutzungsrechten sowie einem nicht als Vermögensanlage klassifizierten Krypto-Utility-Token konnten von über 2.000 Investoren etwa 3.000 Ether eingenommen werden, um damit weitere Investitionen in die Wyskers-Plattform und die technische Umgebung zu tätigen.[4] Wyskers zählt damit zum ersten von acht deutschen Starts-ups, die überhaupt einen ICO erfolgreich abgeschlossen haben, wie Sebastian Kirsch von der Wirtschafts-Woche im Herbst 2018 recherchiert hat.[5]

Leider zeigte sich auch, dass im ICO-Hype auf das Hoch der überhöhten Erwartungen das Tal der Enttäuschungen folgte. Vielerorts ebnete gerade die als flexibilisierender Vorteil gepriesene Unreguliertheit der token-basierten „Börsengänge" den Weg für als innovative Geschäftsmodelle getarnte Betrugsmodelle und für zahlreiche Verbraucherabzocken. So stellten Hugo Benedetti von der EMS Business School und Leonhard Kostovetsky von der Carrol School of Management des Boston Colleges in einer Studie, in der sie alle seit Anfang 2017 (global) erfolgreich durchgeführten ICOs betrachteten, fest, dass nicht einmal die Hälfte der Start-ups nach Kapitalaufnahme durch ICOs mehr als vier Monate überlebte; fast ein Drittel verstummte, tauchte ab oder löste sich auf, etwa ein Zehntel der investierten Gelder floss dabei direkt in Betrügereien.[6]

Ein aktuelles Beispiel dafür ist die Berliner Aktiengesellschaft Envion, welche ihre Krypto-Token im Wert von anfänglich einem US-Dollar pro Token an etwa 30.000 Investoren emittierte. Zu Beginn des Jahres 2018 kamen so nach eigenen Angaben des Unternehmens knapp 100 Millionen Dollar zusammen – ein großer Finanzierungserfolg.[7] Im weiteren Jahresverlauf stellte sich jedoch heraus, dass Envion nicht einmal ein tragfähiges Geschäftsmodell besaß. Durch Prospektbetrug, verschleierte Inhaberschaftsstrukturen und gebrochene Versprechen könnten die Investoren so gut wie leer ausgehen: Der Tokenwert ist mittlerweile auf einstellige Cent-Beträge gefallen. Es zeigt sich, dass von den (internationalen) Regulierungsbehörden genauso wie bei den Banken- und Finanzaufsichten mehr Vereinheitlichung und Sicherheit geschaffen werden muss, um ICOs als legitimes Mittel der Kapitalaufnahme breitenwirksam im 21. Jahrhundert ankommen zu lassen.[8] Der Wandel von dubiosen ICOs zu wesentlich strikter regulierten „Security Token Offerings" (STOs), zum Schutz der Investoren, ist daher ein signifikantes Thema für das Jahr 2020. Wesentliche technische Entwicklungsschritte hinsichtlich der „geordneten" Digitalisierung physischer Vermögensgegenstände/Assets via strukturierter und von Gesetzes wegen genehmigter STO-Emissionen ließen sich Ende 2018 bereits in ihren Anfängen erkennen.

Die verschiedenen Arten von Token

Krypto-währung – Digitales **Zahlungsmittel** basierend auf kryptographischer Verschlüsselung; Wert bestimmt sich vor allem durch Angebot und Nachfrage

Equity-Token – Digitales **Wertpapier,** welches dem Besitzer auch den Besitz über den dahinter stehenden Vermögenswert ermöglicht; Wert bestimmt sich durch die Wertentwicklung des Vermögensgegenstandes

Utility-Token – Digitaler **Coupon,** der dem Besitzer ein Nutzrecht auf Dienstleistungen innerhalb eines Netzwerkes einräumt; Wert bemisst sich vor allem durch den Nutzwert der zugänglichen Funktionalität/Plattform

Security-Token – Digitales **Wertpapier,** welches die Gewinnbeteiligung des Besitzers an einer Unternehmung ermöglicht; kein Besitzrecht/Mitspracherecht an dahinter stehender Unternehmung; Preis bemisst sich nach individuellem Erfolg

Debt-Token – Digitale **Schuldverschreibung;** Wert bemisst sich nach der Höhe der Schuld, den vereinbarten Zinsen sowie der Kreditwürdigkeit des Schuldners

4) Mit Ende des ICOs am 31.01.2018 hatte Wyskers damit etwa eine Viertel Million EUR eingenommen. Der Umrechnungskurs von 853,18€/Ether ist seitdem allerdings auf unter 100€/Ether abgestürzt (Stand 18.12.2018: 81,74 €/Ether). Wie viel real nutzbares Kapital der ICO dem Unternehmen damit tatsächlich eingebracht hat, lässt sich daher nur schwer bewerten.

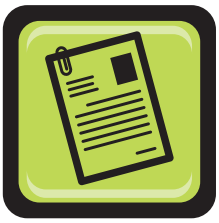
5) Vgl. KIRSCH (2018), S. 1.

6) Vgl. BENEDETTI/KOSTOVETSKY (2018), S. 1.

7) Vgl. KYRIASOGLOU (2018), S. 1.

8) Was konkret passieren muss, damit die Vorteile dieses Instruments wirklich zum Tragen kommen können, beleuchtet ausführlich die Publikation „Blockchain: Kryptische Phantasie oder Finanzmarkt der Zukunft" von Baker Tilly aus dem Mai 2018.

Disruption durch die Blockchain: Smart Contracts



Hinter dem Begriff Smart Contract, häufig übersetzt als „intelligenter Vertrag“, verbirgt sich der Sachverhalt eines maßgeschneiderten Computerprogramms, basierend auf der Blockchain-Technologie. Das Programm spiegelt dabei den Sachverhalt eines real existierenden, „physischen“ Vertrages mit realer Wertigkeit wider.

Der Begriff Smart Contract ist dabei insbesondere im Hinblick auf die häufige Übersetzung problematisch. Smart Contracts und der dahinterstehende Code spiegeln den Vertrag in digital-kryptischer Form wider. Wie ein Vertragsdokument muss diese Verschriftlichung jedoch korrekterweise von einem Vertrag im rechtlichen Sinne abgegrenzt werden, welcher eine Einigung in Form zweier korrespondierender Willenserklärungen und damit ein rein geistiges Konstrukt darstellt. Smart Contracts sind daher keine Verträge im rechtlichen Sinne, sondern vielmehr deren digitale Verschriftlichung.

Smart Contracts sind transparent und können ohne die Verifizierung von Dritten bestehen. Bei der Erfüllung von vorher hinterlegten Bedingungen lösen diese entsprechend verankerte Aktionen aus. Der wesentliche Unterschied von Smart Contracts zu herkömmlich signierten „Papier-Verträgen“ ist deren ausschließlich digitale Existenz, verbunden mit einer dezentralisierten und absolut fälschungssicheren Existenzspeicherung dank Blockchain. Durch Erreichung eines hohen Niveaus an Datensicherheit gegenüber nachträglicher Datenmanipulation schaffen Smart Contracts die Grundlage, Vertragsformulierungen eindeutig abzuspeichern und ihre Durchführung mittels rechentechnisch logischer Regel-Prüfungsprogrammierung zu automatisieren. Die manuelle Überwachung der Vertragserfüllung zwischen zwei Parteien entfällt und wird stattdessen durch automatisierte Softwareausführung sichergestellt.

Die Fähigkeit der autonomen Weiterverarbeitung intelligenter Verträge stellt aus ökonomischer Sicht eine kosteneffektivere Lösung des „Mittelmann-Existenz-Problems“ dar. Unabhängig vom jeweiligen Anwendungsumfeld (beispielsweise Automobil-, Gesundheits-, Finanz-, Logistik-, Versicherungs- als auch Identifikationsbereich) besitzen über Programmiercode gespiegelte Vertragsbeziehungen folgende Vorteile gegenüber der rein analogen Verschriftlichung:

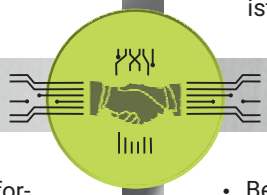
Möglichkeiten von Smart Contracts

Vernetzung von Maschinen

- Smart Contracts ermöglichen den Aufbau eines verbindlichen Rahmens, in dem Maschinen oder Software-Agenten autonom tätig werden können.
- Im umfassend vernetzten Internet der Dinge könnten so z. B. selbstfahrende LKW Lieferungen erledigen, die von Software-Mitarbeitern veranlasst wurden, sich über Smart Contracts bezahlen lassen, unterwegs selbstständig Strom einkaufen und Maut-Gebühren bezahlen.

Digitale Identität

- Sammlung aller persönlichen Daten in einer verschlüsselten Blockchain.
- Beispielhaft könnten dadurch alle Daten, die der Staat über einen Bürger gesammelt hat, umfassend nutzbar gemacht werden, indem Smart Contracts selbst tätig werden. Wenn nach den gesammelten Informationen ein Bürger für Zuschüsse berechtigt oder umgezogen ist, werden alle Bescheide automatisch erstellt und Zahlungen veranlasst.



Einfacher Vertrag

- Digitalisierter Vertrag, welcher transparent alle Informationen unwiderrufbar aufzeichnet, automatisch Aktionen durchführt und dies alles in Echtzeit abwickelt.
- Beispielhaft könnte so ein Schenkungsvertrag auch ohne notarielle Beglaubigung gültig abgebildet werden oder ein Werk-/Dienstvertrag effizienter abgewickelt werden.

Bedarfsgerechte Abrechnung

- Bezahlung erfolgt als Mikrotransaktion pro verbrauchter Einheit.
- Beispielhaft könnte so in Echtzeit der Stromverbrauch oder die Internetnutzung abgerechnet werden.

Vorteile

- Schnelligkeit, Sicherheit und Dezentralität der Verarbeitung
- Entfall eines Intermediärs
- Kostenreduzierung
- Manipulationsfreiheit
- Smart Contract Parteien müssen sich weder begegnen noch persönlich kennen

Demgegenüber stehen die folgenden Nachteile, die in Abhängigkeit ihres jeweiligen Anwendungsumfelds unterschiedlich starke Signifikanz besitzen:

Nachteile

- Programmierfehler und ambivalente Programmierung könnten mitunter zu hohen finanziellen Verlusten führen
- Absicherung gegenüber Hacking oftmals noch unzureichend
- Gegenwärtig existiert noch keine juristische Grundlage für diese Art der Verträge; insbesondere die Gefahr einer verbotenen Eigenmacht durch Selbstausführung des automatisierten Vertragsgebildes ist rechtlich problematisch
- Komplexe Verträge benötigen sehr detaillierte Entwicklungsrichtlinien und Bedingungsbeziehungen, um sämtliche Vertragsbestandteile softwaretechnisch korrekt abzubilden, weswegen gegenwärtig eher simple Vertragsbeziehungen durch Smart Contracts abgebildet werden

Eine besonnene Abwägung der aufgeführten Vor- und Nachteile, verbunden mit einer rationalen Fortschrittsbeurteilung der Smart Contract Ökonomieentwicklung zeigt auf, dass ein weit verbreiteter Einsatz von alltagstauglichen intelligenten Verträgen und zugehörigen dApps schätzungsweise noch etwa drei bis fünf Jahre entfernt ist.

Die Skalierbarkeit des Geschäfts-modells durch die Blockchain

Unter dem Begriff der Skalierbarkeit wird die Wachstums- und Funktionsfähigkeit von Hard- sowie Software bei steigenden Anwender- und Transaktionszahlen verstanden. Die IT-Geschichte zeigt, dass die Skalierung von Technologien zur „Oberseite“ notwendiger Verarbeitungsgeschwindigkeit für einen massentauglichen Alltagseinsatz leichter zu erreichen ist als zur „Unterseite“.

Als Vergleich hierfür dient die exponentielle Steigerung gegenwärtiger Prozessor-Rechenleistung. Wie so oft bei technologisch vielversprechenden Errungenschaften sieht sich auch die Blockchain-Technologie mit wesentlichen Herausforderungen konfrontiert. Eine dieser Herausforderungen ist die Lösung der Skalierbarkeit. Die wichtigsten Aspekte der Problematik können folgendermaßen unterteilt werden:

Skalierungskontroversen

- Zielkonflikte zwischen Technologie-Dezentralität, -Sicherheit und -Skalierbarkeit
- Mempool-Clearance
- Obligatorische Blockgröße (1 MB) für optimale Datendistribution
- Echtzeit-Transaktionsverarbeitungsgeschwindigkeit des Blockchain-Netzwerks
- Energieverbrauch des PoW-Algorithmus zur Block-Hasherstellung
- Energieverschwendung zur Blockchain-Fortschreibung im Vergleich zu anderen Konsens-Algorithmen

Wie bei jeder jungen Technologie wird versucht, den Technologierestriktionen mit einer Anzahl verschiedener technischer Lösungsansätze zu begegnen. In Abhängigkeit von der Blockchain-Typisierung sowie der zugrundeliegenden Recheneinheit (BTC, BCH, ETH) zeichnen sich bereits Lösungen ab. Erste Praxisergebnisse zur signifikanten Skalierungsverbesserung der Blockchain-Technologie sind zeitnah zu erwarten.

Herausforderungen bei der Skalierung

Transaktions-volumen

- Datenobergrenzen für Blöcke sowie die zur Verfügung stehenden Validierungs-Nodes (Miner) begrenzen das mögliche Transaktions-volumen.
- Im Vergleich zu Visa, welches vier- bis fünfstellige Transaktions-volumina pro Sekunde abwickelt, schaffen es Bitcoin und Ether durchschnittlich nicht einmal, zehn Transaktionen pro Sekunde zu verarbeiten.

Energie-verbrauch

- Zur Fortschreibung der Blockchains werden meist PoW-Algorithmen verwendet, die ihre Verlässlichkeit durch die hohe Rechenleistung des gesamten Netzwerkes aufrechterhalten.
- Die Rechner jedoch haben beispielsweise beim Bitcoin bereits einen Energieverbrauch pro Transaktion von über 400 kWh. Jährlich bedeutet dies also einen Gesamtenergieverbrauch von über 40 TWh und damit einen Verbrauch, der z. B. dem des Iraks gleichkommt.

Trade-offs

- Bestünde das Ziel, den Intermediär Visa völlig durch beispielsweise Bitcoins zu ersetzen, würde die gesamte Energieerzeugung der Menschheit aktuell nicht dafür ausreichen (Eine BTC-Transaktion verbraucht dreimal so viel Energie wie 100.000 Visa-Transaktionen).
- Kontroversen in der Weiterentwicklung betreffen nun die Daten-grenzen der Blöcke, die Verbesserung/Ersetzung der Konsens-Algorithmen sowie Mechanismen zur schnellen Transaktions-validierung unter Beibehaltung der Sicherheit und Dezentralität.

Ausblick:
Blockchain in der Wirtschaft

Nach mehr als zehn Jahren stellt die Blockchain des Bitcoin-Netzwerks immer noch eines der sichersten Werkzeuge zur Übermittlung elektronisch eindeutiger Informationen dar. Technologisch betrachtet ermöglicht die Blockchain die Erzeugung einzigartiger digitaler Inhalte jeglicher Ausprägungsart, die in ihrer maximalen Gesamtanzahl jedoch absolut begrenzt werden können. So ist es nur eine Frage der Zeit, wann der notwendige Wissensaufbau weit genug fortgeschritten ist und Blockchain-Use-Cases in zahlreichen Wirtschaftszweigen Anwendung finden werden. Das noch recht junge Zeitalter der dApp-Programmierung hält dabei bereits jetzt in den folgenden Wirtschaftsbereichen Einzug:

- Banken- und Finanzdienstleitungen
  → Cross Border Payments
- Verbrauchsgüterindustrie
  → lückenlose Nahrungsmittel-rückverfolgbarkeit
- Identifikations- & Gesundheitswesen
  → IBM Trusted Identity Management
- Immobilienwirtschaft
  → Commercial Real Estate
- Versicherungswirtschaft
  → transparente, automatisierte Schadensfall-Ersatz-Abwicklung
- Medien- & Werbeindustrie
  → Schutz geistigen Eigentums, Verhinderung von Raubkopien
- Internet of Things (IoT)
  → sensorgetriebene, autonome Maschinen-/Anlagenüberwachung

Die weltweit aktive Weiterentwicklung der Blockchain-Technologie zur dezentralen Speicherung validierter Daten sowie deren korrekte autonome Weiterverarbeitung dank kollektiver und dennoch verteilter Netzwerkrechenleistung wird von zahlreichen Technologieexperten als zukunftsweisende Netzwerkstruktur für die künftige Datenhaltung erachtet. Diese Auffassung teilen wir von Baker Tilly ebenso. Prognosen bezüglich Kosteneinsparungspotenzialen, der prägnanten Erhöhung von Prozessabwicklungsgeschwindigkeiten sowie zusätzliche Venture Capital Investitionen untermauern unsere Auffassung zusätzlich.

Schlussendlich führt der Einsatz von Blockchain-Technologie zu einem Datennetzwerk, in dem keine zueinander konkurrierenden Informationsversionsstände existieren, die zu widersprüchlichen Aussagen führen könnten. Die Entwicklung einer Netzwerkarchitektur zur dezentralisierten, redundanzfreien Informationsaufbewahrung via Blockchain-Technologie wird daher immer stärker in den Fokus der Forschung rücken und wahrscheinlich in viele unserer Lebensbereiche spürbar Einzug halten.

Literaturverzeichnis

BENEDETTI, HUGO / KOSTOVETSKY, LEONARD (2018): Digital Tulips? Returns to Investors in Initial Coin Offerings, https://ssrn.com/abstract=3182169, aufgerufen am 18. Januar 2019.

DEUBEL, MARCO / MOORMANN, JÜRGEN / HOLOTIUK, FRIEDRICH (2017): Nutzung der Blockchain-Technologie in Geschäftsprozessen: Analyse am Beispiel des Zahlungsverkehrs, https://www.researchgate.net/publication/321752213, aufgerufen am 18. Januar 2019.

DE VRIES, ALEX (2018): Bitcoin's Growing Energy Problem, https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6, aufgerufen am 18. Januar 2019.

HABER, STUART/ STORNETTA, W. SCOTT (1991): How to time-stamp a digital document, in: Journal of Cryptology. 3 (2): S. 99–111.

KIRSCH, SEBASTIAN (2018): Anleger erleiden mit deutschen ICOs Verluste bis zu 90 Prozent, https://www.wiwo.de/finanzen/boerse/kryptowaehrungen-anleger-erleiden-mit-deutschen-icos-verluste-bis-zu-90-prozent/23117376.html, aufgerufen am 18. Januar 2019.

KYRIASOGLOU, CHRISTINA (2018): Wie Envion Anleger um 100 Millionen Dollar brachte, http://www.manager-magazin.de/unternehmen/energie/envion-ag-investoren-klagen-gegen-100-millionen-ico-a-1224035.html, aufgerufen am 18. Januar 2019.

Diese Broschüre ist unter der Mitarbeit von Julian Glatter, Florian Klawun, Alexander Paul und Marie-Therese Wirtz entstanden.

Autoren

AUDIT & ADVISORY
TAX
LEGAL
CONSULTING

Tibor Abel ist Partner bei Baker Tilly. Er verfügt über mehr als 15 Jahre Erfahrung in der Prüfung und Beratung von Technologieunternehmen. Seine Tätigkeitsschwerpunkte sind neben der Jahres- und Konzernabschlussprüfung von mittelständischen Unternehmen insbesondere die Betreuung von Start-ups und E-Commerce-Unternehmen. Tibor Abel ist Wirtschaftsprüfer und Steuerberater und setzt sich intensiv mit disruptiven Geschäftsmodellen auseinander.
tibor.abel@bakertilly.de

Dirk Luther ist Partner bei Baker Tilly. Als Wirtschaftsprüfer/Steuerberater verfügt er über mehr als 28 Jahre Erfahrungen in der Prüfung und Beratung von mittelständischen Unternehmen und Konzernen sowie von staatlich finanzierten Einrichtungen und öffentlichen Unternehmen, insbesondere Forschungseinrichtungen. Dirk Luther ist Mitglied des Fachausschusses für öffentliche Unternehmen und Verwaltungen (ÖFA) des Instituts der Wirtschaftsprüfer.
dirk.luther@bakertilly.de

Prof. Dr. Martin Pätzold verantwortet als Head of den Bereich Innovation & Research bei Baker Tilly. Er war von 2013 bis 2017 Mitglied des Deutschen Bundestages. Die Berufung an die Hochschule Mittweida hat Prof. Dr. Martin Pätzold für das Themengebiet „Wettbewerb in der digitalen Wirtschaft“ erhalten. Wissenschaftlich setzt er sich mit den Folgen der Digitalisierung für die Geschäftsmodelle von Unternehmen auseinander.
martin.paetzold@bakertilly.de

Now, for tomorrow

Follow us:

AUDIT & ADVISORY • TAX • LEGAL • CONSULTING

Baker Tilly bietet mit 35.000 Mitarbeitern in 145 Ländern ein breites Spektrum individueller und innovativer Beratungsdienstleistungen in den Bereichen Audit & Advisory, Tax, Legal und Consulting an. Weltweit entwickeln Wirtschaftsprüfer, Rechtsanwälte, Steuerberater und Unternehmensberater gemeinsam Lösungen, die exakt auf jeden einzelnen Mandanten ausgerichtet sind, und setzen diese mit höchsten Ansprüchen an Effizienz und Qualität um.

bakertilly

Baker Tilly
T: +49 800 8481111
kontakt@bakertilly.de

bakertilly.de