DEUTSCHER MARKETING VERBAND

COMPETENCE CIRCLE **#CCTIM**

BLOCKCHAIN-TECHNOLOGIE REVOLUTIONIERT DIE DATING-KULTUR UND LIEFERKETTE

Editorial

Der Competence Circle **Technologie, Innovation & Management #ccTIM** ist ein Kompetenzzentrum für Künstliche Intelligenz und weitere technologische Trends, denn die fortschreitende Globalisierung stellt uns vor neue Herausforderungen.

Inwiefern Roboter wie auch RFID, Blockchain, Tokens und andere Innovationen im Marketing, Vertrieb und Business Development eingesetzt werden, steht dabei im Fokus. Wie schaffen wir "Added Value" für die Gesellschaft und für unsere Kunden mit neuen Technologien?

Über die Autoren

Professor Dr. Urs E. Gattiker ist CEO beim Compliance-, Marketing- Technologie- und Softwarespezialisten drkpi® CyTRAP Labs in Zürich. Beim Deutschen Marketing Verband ist er stellv. Beirat der Region Südwest, Co-Leiter vom Competence Circle "Technologie, Innovation & Management" (#ccTIM) und Präsident vom Marketing Club Lago am wunderschönen Bodensee.

Taina Temmen ist Co-Founder und COO von EDITIVE, einem SaaS-Startup für Content Collaboration. Zuvor war sie bei der Maschinen- und Anlagenbaugruppe Wintersteiger AG für Produktmanagement und Business Development für vier Geschäftsfelder verantwortlich sowie Bereichsleiterin bei der Diehl Metall Stiftung & Co. KG für strategisches Marketing und Innovations-Management. Sie ist im Vorstand vom Deutschen Marketing Verband (DMV) und koordiniert die Competence Circles. Sie ist Mitglied im Marketing Club Lago.

Taina Temmen
Vorstand Deutscher Marketing Verband
Ressort für Content & Social Media

pink markiert = 1:1 Wikipedia

Abstract

Eine Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen, Blöcke genannt, die mittels kryptografischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptografisch sicheren Streuwert des vorhergehenden Blocks. Eine der ersten Anwendungen von Blockchain ist die Kryptowährung Bitcoin.

Blockchain-Technologie auch Distributed Ledger Technologie genannt sind manipulationssichere und manipulationsgeschützte digitale Ledger. Diese werden ohne zentrale Datenbank und in der Regel ohne zentrale Behörde (d.h. Regierung oder auch Bank) implementiert. Auf ihrer grundlegenden Ebene ermöglichen sie es einer Gemeinschaft von Benutzern, Transaktionen in einem gemeinsamen Ledger innerhalb dieser Gemeinschaft zu erfassen, so dass unter normalem Betrieb des Blockchain-Netzwerks keine Transaktion nach ihrer Veröffentlichung geändert werden kann.

Ist mit Blockchain die Neugestaltung oder das Remaking der Lieferkette, der Dating-Kultur und vom Risiko Management bald Realität? Diese und weitere Herausforderungen diskutieren wir im aktuellen Whitepaper. Der Leser soll dadurch besser verstehen, wie die Blockchain-Technologie funktioniert und wie diese optimal in Unternehmen eingesetzt werden kann.

kürzen?

Inhalt

Die Leitfrage

Wie können Unternehmen strategisch von der Blockchain profitieren?

- Sowohl für Start-ups als auch für Mittelständler können verteilte Ledger-Technologien neue Geschäfts- und Betriebsmodelle ermöglichen.
- Um Mehrwert zu schaffen, müssen Unternehmen die Blockchain-Technologie systematisch mit ihrer Strategie und ihren Fähigkeiten verknüpfen.
- Firmen müssen ihre Daten als Anlagegut verwalten, um z.B. Vertrauen, Transparenz und Sicherheit in der Lieferkette zu optimieren.
- Ohne SMART Metrics ist es unmöglich zu entscheiden, ob ein Blockchain-System besser ist als eine andere Lösung.
- Jede Transaktion verursacht Kosten, die je nach Blockchain- Typ, Transaktionsanzahl, Netzwerkgröße usw. stark abweichen können (0,50 – 7 Euro und ggf. sogar mehr).
- Zukunftsorientierte und messbare Prioritäten für die nächsten 3 Jahre zu setzen ist ein Muss.

Einführung

Die Blockchain-Technologie sorgt aktuell für Gesprächsstoff über ganze Industriegrenzen hinweg. Blockchain bedeutet auf Deutsch "Blockkette". Es handelt sich um eine dezentralisierte Datenbank bei der beispielsweise der Kunde und der Lieferant einer Transaktion direkt miteinander verknüpft werden. Der wesentliche Unterschied zum herkömmlichen System ist, dass dabei auf eine zentrale Datenbank verzichtet wird. Ebenfalls sind die Daten auf Servern dezentral verteilt.

In ihrer einfachsten Form sind Blockketten Speichergeräte - eine Art Datenbank - zur Aufzeichnung und Verifizierung von Transaktionen und Auftragsbedingungen. Eine Blockchain zeichnet Informationen über eine beliebige Anzahl von Dingen auf, wie beispielsweise:
Wer besitzt ein bestimmtes Objekt, wer kaufte von wem ein bestimmtes Bild oder wer tauschte ein Sicherheitsventil mit welchem Teil in einem Aufzugsschacht aus und wurde das ersetzte Ventil sicher und komplett entsorgt?

Was Blockketten jedoch so mächtig macht, ist die Tatsache, dass sie verteilt und digital sind. Wenn Transaktionen zwischen den Parteien stattfinden, werden die verteilten digitalen Kopien des Ledgers sofort und gleichzeitig aktualisiert. Die Aufzeichnung jeder Transaktion wird durch fortschrittliche Berechnungsalgorithmen und kryptografische Sperren dauerhaft aufgezeichnet. Je nach den Regeln der betrachteten Blockkette können die Teilnehmer entweder identifiziert werden oder anonym bleiben.

Wenn man heute das Wort Blockchain hört, denken viele zuerst einmal an die digitale Kryptowährung Bitcoin. Bitcoin ist eine digitale Währung, die elektronisch hergestellt, gehandelt und verwahrt wird. Blockchain als Protokoll und im Sinne einer verteilten Datenbank entstand 2008, als Satoshi Nakamoto dieses im Whitepaper zu Bitcoin beschrieb. 2009 wurde von ihm die erste Implementierung der Software Bitcoin veröffentlicht. Dies war der Startschuss für die Blockchain-Technologie.

Während die Blockchain-Technologie ursprünglich als Mechanismus für vertrauenswürdige digitale Währungen vorgeschlagen wurde, haben sich ihre Einsatzmöglichkeiten weit über diesen speziellen Anwendungsfall hinaus erweitert.

In diesem Whitepaper fokussieren wir uns er auf eine kurze Erklärung der Blockchain als Technologie. Anhand von Fallbeispielen erläutern wir, in welchen B2C- und B2B-Bereichen die DLT im Vormarsch ist. Spezieller Fokus liegt dabei darauf, wie Unternehmen mit Hilfe der Blockchain-Technologie interne und externe Prozesse optimieren können, um beispielsweise ihren Kunden ein verbessertes Einkaufserlebnis zu bieten. Dabei interessiert uns wie z.B. Mittelständler die Blockchain-Technologie einsetzen, um der Globalisierung im Konkurrenzkampf gegen Marktmonopole erfolgreich die Stirn zu bieten. Kurz, wie können Unternehmen strategisch von der Blockchain-Technologie profitieren?

Grafik 1 unten illustriert in sechs Schritten, was mit einer Transaktion in einer Blockchain passiert.

Schlagworte

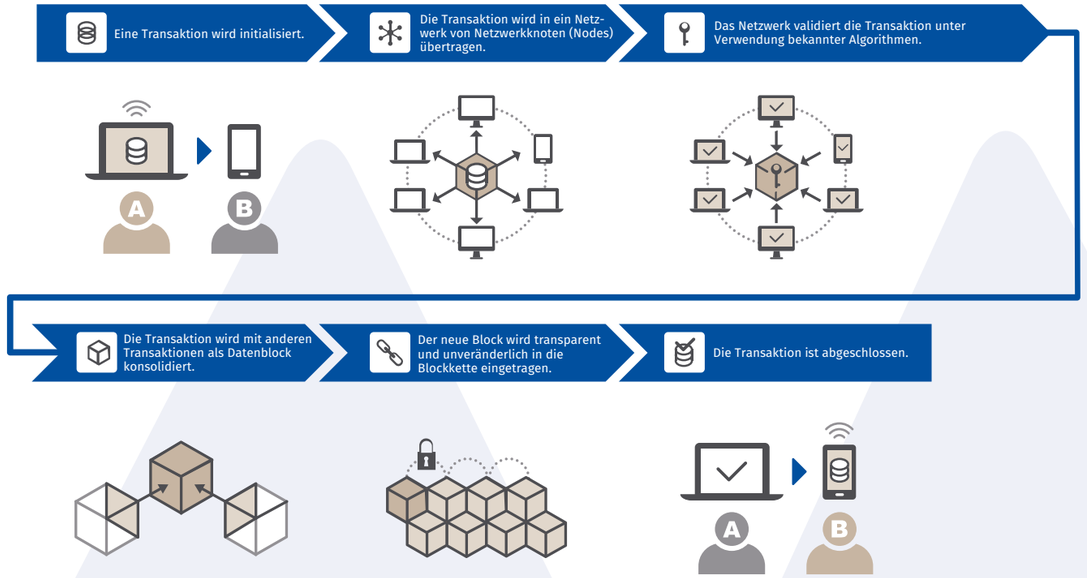
Bitcoin, Blockchain, #ccTIM, Cybersecurity, Datenschutz, Digitalisierung, DLT, #DMV, Finanzmarkt, Klimawandel, Konsensusmodell, Kosten, Asymmetric-key, Cryptography, Smart Contract, Fälschung, Lieferkette, Kryptowährung, Blockchain-Technologie

Zitiervorschlag

Gattiker, Urs E. & Temmen, Taina (Januar 2020).
Kann die Blockchain-Technologie die Lieferkette und die Dating-Kultur revolutionieren? Whitepaper. Düsseldorf: Deutscher Marketing Verband e.V. (DMV). Aufgerufen am 2019-12-05 auf https://MCLago.com/download/39/ und https://drkpi.com/download/10

COMPETENCE CIRCLE **TECHNOLOGIE, INNOVATION & MANAGEMENT #CCTIM** DMV Whitepaper **Nr. 01 | Januar 2020**

Wie funktioniert eine Blockchain?



Grafik 1: Funktion einer Blockchain in sechs Schritten

1. Was ist eine Blockchain?

Bevor wir all diese wichtigen Fragen beantworten können, erklären wir zunächst, was die Blockchain-Technologie beinhaltet.

Blockchain ist eine dezentrale Datenbank, die auch Distributed Ledger Technologie (dezentral geführte Kontobuchtechnologie) oder DLT bezeichnet wird. Es gibt viele verschiedene Möglichkeiten zur Implementierung einer Blockchain. Doch alle beinhalten sicherlich folgende vier Komponenten (für eine gute Einführung siehe auch Yaga, Mell, Roby and Scarfone, 2018):

1. Distributed Ledger Technologie (DLT) oder digital verteiltes Kassenbuch
   Als Ledger bezeichnet man die Reihe von Blöcken, die die Aufzeichnung der Transaktionen in der Reihenfolge dieser Transaktion sind. DLT bzw. das digital verteilte Kassenbuch erlaubt die transparente Dokumentation von Transaktionen. Anstatt nur ein einziges Kassenbuch an einem einzigen Ort, gibt es viele gleichberechtigte Kassenbücher an verschiedenen Orten.

2. Das Konsensprotokoll ermöglicht es allen Mitgliedern der Gemeinschaft, sich auf die im Hauptbuch gespeicherten Werte zu einigen. Diese Kopien der Kassenbücher werden in einem automatisierten Konsensprozess konsistent gehalten. Damit wird sichergestellt, dass diese Kopien identisch sind. Wenn zwischen einem Absender und einem Empfänger eine Datentransaktion stattfindet, wird erst mit den anderen Computern im Netzwerk verglichen, ob diese Änderung gültig ist. Ist die vorgeschlagene Änderung gültig, wird die Transaktion in einen neuen Block gepackt und an den letzten Block, d.h. an die Transaktion, drangehängt.

   Jede Transaktion ist ein Datensatz, der einen Hashwert, also einen eindeutigen digitalen Fingerabdruck hat. Dieser Hashwert des vorangegangenen Datensatzes wird ebenfalls mit dem nächsten Datensatz gespeichert. So entsteht eine Verkettung von Blöcken, die Blockchain.

   Durch den Hashwert ist eine nachträgliche Änderung der Daten nicht möglich. Erzwingt man dies, ist die Integrität des Gesamtsystems beschädigt. Das wird dokumentiert und jeder Nutzer kann es somit sehen und nachvollziehen.

3. Die digitale Währung [Diese kann durch Währungen wie z.B. $ oder Euro ersetzt werden.] gilt als Belohnung für diejenigen, die bereit sind, die Arbeit zur Weiterentwicklung des Hauptbuchs/Ledgers/Kassenbuches zu leisten. Diese Komponenten arbeiten zusammen, um ein System bereitzustellen, das die Eigenschaften von Stabilität, Unwiderlegbarkeit und Vertrauensverteilung aufweist, die letztendlich die Ziele des Systems sind.

4. Bei privaten oder geschlossenen Blockchains muss festgelegt werden, wer Schreib- und wer nur Lese-Rechte hat. In einer öffentlichen Blockchain haben alle Lese- und Schreib-Rechte.

"Bitcoin ist ein Trugbild/Täuschung, aber Blockchain ist genial"
– Warren Buffett, CEO und Chairman, Berkshire Hathaway (Februar 2019)

Ob private oder öffentliche Blockchains, diese beinhalten immer die vier Komponenten wie oben beschrieben. Beide - private und öffentliche - Blockchains haben viele Dinge gemeinsam, wie beispielsweise:

- Bei privaten und öffentlichen Blockchains handelt es sich um dezentrale Peer-to-Peer-Netzwerke, bei denen jeder Teilnehmer eine Kopie eines gemeinsamen Nur-Anhang-Ledgers von digital signierten Transaktionen führt.

- Beide halten die Replikate der Transaktionen über ein Protokoll, das als Konsens bezeichnet wird, synchron. Das heißt, jeder Teilnehmer in der Blockchain hat dieselben Transaktionen oder dieselbe Kopie eines Kassenbuches auf seinem Server.

- Öffentliche und private Blockchains bieten beide bestimmte Garantien für die Unveränderlichkeit des Ledgers. Ein Beispiel ist das Konsensprotokoll, das dazu beiträgt, die Transaktionen zu verifizieren.

Eine Blockchain wird privat oder halbprivat genannt, wenn der Konsens-Prozess nur von einer begrenzten und vordefinierten Teilnehmerzahl erreicht werden kann. Der Schreibzugriff wird von einem Unternehmen vergeben, und die Leserechte können öffentlich oder eingeschränkt sein. Weitere Faktoren erklären wir gleich unten.

Private DLTs werden auch „permissioned" Blockchains genannt, d.h. Blockketten fungieren als geschlossene Ökosysteme, in denen Benutzer nicht frei in das Netzwerk einsteigen, die aufgezeichnete Historie einsehen oder eigene Transaktionen durchführen können. Bei einer „permissionless" (oder public) Blockchain kann jeder ohne notwendige Autorisierung auf der Blockchain lesen und schreiben.

Private Blockketten eignen sich besser für Geschäftsanwendungen, insbesondere in regulierten Branchen wie Banken und dem Finanzwesen, vorbehaltlich der Kenntnis ihrer Kunden und der Anti-Geldwäsche Vorschriften. Private Blockketten sind in der Regel auch besser in der Governance. Das Fehlen eines geordneten Verfahrens zur Aktualisierung des Ledger-Protokolls als Reaktion auf sich ändernde Umstände hat dazu geführt, dass Streitparteien sich sowohl bei Ethereum als auch bei Bitcoin in verschiedene inkompatible Währungen gespalten haben.

Einige zugelassene Blockchain-Netzwerke wie z.B. eine Federated Blockchain erfordern, dass alle Benutzer berechtigt sind, zu senden und zu empfangen. Hier sind die Transaktionen weder anonym noch pseudoanonym. In solchen Systemen arbeiten die Parteien zusammen. Hier wird ein gemeinsamer Geschäftsprozess gesichert, um so zu verhindern, dass weder Betrug (z.B. zwischen Lieferanten) noch freeriding (Trittbrett fahren) stattfinden kann (siehe Yang, Choi, Misch, Yang, & Dunham, 2018). Das heißt, Personen, die sich schlecht verhalten oder das Konsensprotokoll verletzen, können identifiziert werden. Bei schlechtem Verhalten oder Verstößen wissen die Beteiligten, welche Partei es ist. Das zeigt dann auch, welche Rechtsmittel zur Verfügung stehen und wie sie eingesetzt werden können, um die Rechtsverstöße im zuständigen Justizsystem zu verfolgen.

Blockchain baut auf 2 bekannten Technologien auf

Distributed Computing

1960 "architecture"
1970s mit Ethernet

Mehrere Softwarekomponenten auf verschiedenen Computern, werden als einziges System ausgeführt.

Asymmetrische Kryptografie

1974 Merkles Puzzle
1977 Rivest, Shamir & Adelman

Jeder kann den öffentlichen Schlüssel zum Verschlüsseln von Daten verwenden.

Nur der Besitzer des privaten Schlüssels kann jedoch die verschlüsselte Nachricht entschlüsseln.

Grafik 2: Die zwei wichtigsten Pfeiler der Blockchain-Technologie

Grafik 2 zeigt, dass die Blockchain auf zwei gut etablierten Ansätzen basiert ist: Distributed Computing und Asymmetrische Kryptografie. Beide Pfeiler werden seit Jahren genutzt und weiterentwickelt.

Unten beschreiben wir die vier heute bekannten Arten von Blockchains.

1.1 Was ist eine Public Blockchain?

Eine Public (oder Permissionless) Blockchain ermöglicht jedem, im offenen Ökosystem zu partizipieren. Dabei muss das Protokoll des Netzwerkes genutzt werden. Die Peer-to-Peer (P2P) Transaktionen finden im dezentralisierten Netz statt, d.h. kein Mittelsmann ist nötig.

Das zugrundeliegende Blockchain-Protokoll bietet ein Betriebssystem, das einer Gruppe von Personen ermöglicht, sich mit einem Ziel vor Augen zu organisieren, obwohl sie sich nicht kennen bzw. dadurch auch (noch) nicht vertrauen können.

Bei Blockchains, die Bitcoins, Litcoin oder Zcash handeln, können z.B. Produkte mit diesen Kryptowährungen bezahlt werden. Das geschieht, ohne dass man die wirkliche Identität des Lieferanten oder des Kunden kennt.

Doch viele Finanzexperten sind skeptisch. Beispielsweise Berkshire Hathaway's stellvertretender Vorstandvorsitzender Charlie Munger ist der Meinung, dass der Handel mit Kryptowährungen „nur Demenz" sei und diese als Vermögenswerte nichts taugen. Nichtdestotrotz, die Blockchain- Technologie bietet Möglichkeiten, bestimmte Abläufe besser zu organisieren und sicherer zu machen, wobei die Zahlung mit Fiatgeld [Als Fiatgeld wird eine nationale Währung bezeichnet, die nicht an den Preis eines Rohstoffes wie Gold oder Silber gebunden ist. Weitere Informationen finden Sie hier: https://www.ig.com/ch/trading-glossar/fiatgeld-defintion] abgewickelt werden kann. Unten stellen wir einige der Blockchain Möglichkeiten vor (siehe auch Tabelle 1).

	Zugang	Hauptmerkmale	Typischer Anwendungsfall
1.1 Public (öffentlich)	uneingeschränkt	unveränderlich und verteilt	universell einsetzbare Kryptowährungen Bsp. Bitcoin
1.2 Privat	beschränkt auf eine einzige Einheit, Lesen kann öffentlich / nicht eingeschränkt sein	je nach Bedarf, unveränderlich und verteilt auf wenige Parteien	internes Audit, Datenbankmanagement, Lieferkette innerhalb des Unternehmens und seiner Tochtergesellschaften. Bsp.: IMF u. World Bank testen "Learning Coin"
1.3 Halbprivat (semi-public)	beschränkt auf Mitglieder, z.B. ein Unternehmen, das eine Blockchain für seine Lieferkette nutzt, bringt Lieferanten und Distributoren auf die Blockchain	(unveränderlich und verteilt)	Life-Cycle Management / Supply Chain Mgmt. für Hersteller wie Lieferanten u. Verteiler Bsp.: Golisan, Arteia (Kunst)
1.4 Konsortium	Beschränkt auf Konsortiumsmitglieder, Lesen der Einträge kann öffentlich sein, doch ein Kassenbuch führen können nur Mitglieder, d.h. read-only Datenbank	Im Rahmen eines Auswahl- und Konsensverfahrens, dürfen nur bestimmte Teilnehmer in Block gebündelte Transaktionen anhängen.	Konsortiumspezifische Anwendungsfälle wie z.B. Handel zwischen Konsortialmitgliedern Bsp. Interbank Information Network (IIN), die digitale Währung namens Libra/Facebook.

Note. Angepasst und erweitert gemäß Uhlmann, 2017 S. 17.

1.2 Was ist eine Private Blockchain?

Diese stehen einer bestimmten Gruppe von Personen, z.B. Firmen mit zentralen Verantwortlichkeiten innerhalb eines Unternehmens (beispielsweise Tochtergesellschaften und Länderniederlassungen) zur Verfügung. Der jeweilige Verantwortliche kümmert sich um die Instandhaltung der Blockchain. Das Unternehmen bestimmt z.B. wer welche Aktionen ausführen darf und wer Zugang zu bestimmten Daten auf der Blockchain erhält.

1.3 Was ist eine Semi-Public (halbprivate) Blockchain?

Halbprivate kettenbasierte oder Blockchain Anwendungen werden von einem einzigen Unternehmen ausgeführt. Dieses gibt jedem Benutzer Zugriff, der sich qualifiziert. In der Regel richtet sich diese Applikation an Business-to-Business-Anwender.

Als Beispiel können wir ein Unternehmen nennen, das seine Lieferanten oder Anbieter wie auch Distributoren auf die Blockchain nimmt. Dies ermöglicht die genaue Nachverfolgung von beispielsweise einer Maschinenkomponente,

einem Aufzugsersatzteil oder von einem Medikament, und zwar über die gesamte Wertschöpfung; von der Herstellung bis zum Verkauf (siehe auch Wanger-Baumann, 2019).

Auch Wartungsarbeiten können eingebaut werden, d.h. wenn ein Techniker ein neues Ersatzteil einbaut, kann auch diese Information in die Blockchain eingegeben werden.

1.4 Was ist eine Konsortium Blockchain?

Eine Konsortium Blockchain bringt z.B. Banken zusammen, die einen für sie wichtigen und oft getätigten Service schneller und genauer abwickeln wollen. Das auf Blockchain-Technologie basierte Interbank Information Network (IIN) wurde 2017 von der JPMorgan Chase zusammen mit der australischen ANZ-Bank und der Royal Bank of Canada eingerichtet. Es ermöglicht Probleme aufgrund fehlerhaften oder aus Compliance-Gründen aufgehaltenen Zahlungen schneller zu lösen. Dies kann sonst bis zu mehrere Wochen dauern, wenn mehrere Banken entlang der gesamten Zahlungskette involviert sind.

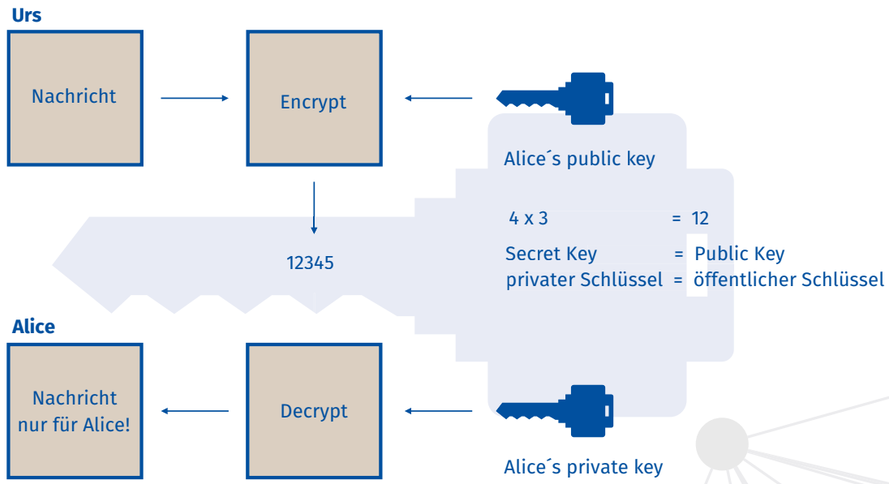
Rund 5 bis 20% der Zahlungen scheitern an Fehlern oder Compliance Problemen laut JPMorgan Chase und deren Experten. Die neuen Blockchain Features zur schnelleren Lösung von Compliance-Fragen und Fehlern in Zahlungen werden seit Oktober 2019 von den 220 Bankmitgliedern der IIN genutzt (Noonan, 2019-04-21).

Ein weiteres Beispiel ist Facebook's Währung Libra, die von einem gleichnamigen Verein getragen wird, der im Sommer 2019 in der Schweiz gegründet wurde. Diesem gehörten anfangs einige Schwergewichte wie Mastercard, Visa als auch Mobilfunk-Konzerne Iliad und Vodafone an. Beim Verfassen dieses Whitepapers war noch nicht klar ersichtlich, wie diese Blockchain genau funktionieren wird. Doch scheint hier eine Konsortium Blockchain zu entstehen, die bestimmten Teilnehmern wie Vereinsmitgliedern erlaubt, im Rahmen eines Konsensverfahrens in Blöcke gebündelte Transaktionen anzuhängen. Facebook Mitglieder oder andere Nutzer können also nur die Datenbank einsehen, aber nichts daran ändern. Um diese Technologie zu entwickeln, ist das Konsortium auf Blockchain-Wissen angewiesen. Dieses Wissen soll von Blockchain-Dienstleistern wie Anchorage, Bison Trails, Coinbase und Xapo kommen. Diese sind alles Mitglieder des Librar Vereins. Wenn Libra die regulatorischen Hürden in Europa und USA meistert, wird es einer Vielzahl von Menschen den Umgang mit einem Wallet und Krypto-Assets näher bringen. [Eine gute Einführung wie sich die verschiedenen Interessensgruppen im Libra Projekt einbringen gibt es hier https://www.nzz.ch/wirtschaft/libra-chance-und-risiko-fuer-facebook-mastercard-uber-ld.1513350] Im Oktober 2019 wurde dann bekannt, dass neben PayPal auch Mastercard und Visa nicht mehr dabei sind. Primärer Grund soll dabei gewesen sein, dass der regulatorische Widerstand von z.B. Frankreich wie auch der USA zu stark schien. Library wird deshalb sicherlich nicht wie geplant bis Ende 2020 lanciert.

1.5 Was macht die Blockchain sicher?

Im November 2008 hat jemand unter dem Pseudonym Satoshi Nakamoto das digitale Zahlungsmittel Bitcoin beschrieben. Im Januar 2009 wurde dann eine Open-Source Software dazu veröffentlicht. Das Netzwerk basiert auf einer Datenbank, die dezentral organisiert ist, der Blockchain. Dabei werden mit Hilfe der Kryptografie alle Transaktionen darin verschlüsselt gespeichert.

Wie funktioniert Kryptographie? Ein Beispiel:



Grafik 3: Wie asymmetrische Kryptografie in der Praxis funktioniert.

COMPETENCE CIRCLE **TECHNOLOGIE, INNOVATION & MANAGEMENT #CCTIM** DMV Whitepaper **Nr. 01 | Januar 2020**

Grafik 3 illustriert wie Kryptografie genutzt werden kann. Dabei ist die Schlüsselverwaltung sehr wichtig, speziell der private Schlüssel. Geht dieser verloren, können die verschlüsselten Transaktionen nicht mehr entschlüsselt werden.
Um den Ablauf in Grafik 3 zu illustrieren, haben wir eine Transaktion zwischen Urs und Alice angenommen. In einem Hauptbuch in der Blockchain ist festgehalten, welche Transaktion stattgefunden hat (z.B. Alice gab Urs 10 Bio-Eier). Dies geschieht anhand der Reihenfolge, in der sie stattgefunden hat. Zum Beispiel gab Alice, die Bio-Bäuerin, die Eier an Sandro den Spediteur weiter. Sandro lieferte die Eier an Fritz, dem Bio-Ladenbesitzer. Jeder dieser Schritte wurde in der Blockchain registrieret.

Ledger sind öffentlich und für alle Parteien zugänglich. Sie müssen manipulationssicher sein, d.h. keine Partei kann nach der Erfassung Ledger-Einträge hinzufügen, löschen oder ändern. Kurz gesagt, die Algorithmen, welche die Ledger führen, müssen immun gegen Angriffe sein, um sicherzustellen, dass das Ledger auch bei Fehlverhalten der Parteien sicher bleibt.

2. Einsatz der Blockchain: strategische Überlegungen

Sowohl für Start-ups als auch für Mittelständler können verteilte Ledger-Technologien neue Geschäfts- und Betriebsmodelle ermöglichen. Doch auf welchen Gebieten kann die Blockchain was bewegen? Sicher ist, dass wir uns auf zukunftsorientierte und messbare Prioritäten konzentrieren.

In einem Artikel haben McKinsey Berater den Finger auf die Wunde der Blockchain gelegt (Higginson, Nadeau und Kausik, Januar 2019). Dabei sind die Berater der Meinung, dass nur Nischen-Anwendungen was bringen. Beispiele sind hierfür Wertgegenstände, Rohstoffe, Ersatzteile und Maschinen in der Lieferkette zu verfolgen. Hier hilft die Blockchain die Effizienz zu steigern und die Transparenz der Transaktionen zu optimieren.

2.1 B2B-Applikationen der Blockchain-Technologie

Es zeigt sich verstärkt, dass bei solchen Projekten gilt, sich auf Prioritäten zu fokussieren, die zukunftsorientiert und messbar sind. Es geht darum in weniger als 3 Jahren gute Resultate liefern zu können. TradeLens, eine Plattform die von AP Moller und IBM entwickelt wurde, ist dafür ein Beispiel. Die beiden haben gemeinsam eine Logistikplattform eingeführt; ehemals papierbasierte Versandprozesse wurden digitalisiert und ermöglichten dadurch sofortigen und unveränderlichen End-to-End-Daten-Austausch, eine klassische Konsortium Blockchain (siehe Tabelle 1 oben).

Die Plattform ermöglicht eine effiziente und genaue Containerverfolgung und den Informationsaustausch zwischen den Mitgliedern der Plattform. Thailand war nach Singapur das zweite Mitglied der Association of Southeast Asian Nations, das begonnen hat, die Plattform zu nutzen (Tortermvasana, 2019-08-29).

Mehr als 100 verschiedene Unternehmen haben sich seit ihrer Gründung TradeLens angeschlossen.

Maersk und IBM bleiben die einzigen beiden Gesellschafter von TradeLens. Beide Unternehmen haben in die Technologie investiert und besitzen gemeinsam das geistige Eigentum. Die Blockchain und deren Ökosystem sind offen für andere Teilnehmer.

2.2 B2C-Applikationen der Blockchain-Technologie

Auch im B2C-Bereich gibt es Möglichkeiten. Das Ideale bei der Blockchain-Technologie ist, dass die Technologie jede Transaktion mit Uhrzeit und Akteur unveränderbar festhält. Dies entpuppt sich auch als interessant für den Kunstmarkt, um mit der Blockchain das Risiko für Fälschungen zu reduzieren. Man erhofft sich von der Blockchain eine Transaktionstransparenz und eine Verlässlichkeit von Informationen im Kunsthandel.

Beispielsweise erhält ein Werk eines Künstlers einen sogenannten Ledger. Auf diesem sind die Angaben zum Kunstwerk eingetragen. Diese können nicht mehr verändert werden. Wenn ein Künstler sein Werk so dokumentiert, kann ab dem Erstverkauf jeder Wechsel vom Besitzer des Bildes festgehalten werden. Bei Arteia (eine halbprivate Blockchain für Kunst inklusive Gemälde und Skulpturen) bestimmen die einzelnen Teilnehmer, wie Museen oder Galerien und deren Sammler (d.h. Kunden), wer Zugang zu den Daten hat.

Ebenfalls kann ein Luxusgut-Hersteller, wie von exklusiven Uhren, diese in eine Blockchain eintragen. Jede Uhr hat dann wie ein Kunstwerk ein Ledger. Dadurch wird aufgezeigt, wer die Uhr schon besessen hatte, den jetzigen rechtmäßigen Eigentümer und wann sie ggf. repariert wurde. Hier bestimmt der Hersteller, wer zur Blockchain Zugang hat.

Dies ist umso interessanter, da der Gebrauchtmarkt von Luxusgütern - im Fachjargon Certified Pre-Owned (CPO) Luxusgütern, wie Uhren, Schmuck aber auch Kleidern, rasant wächst. Schon heute macht er gut 8% des Gesamtmarktes aus (Lex 2019-03-30/31). Oft werden diese CPO-Produkte sowohl im virtuellen Handel (online) als auch in stationären Boutiquen verkauft. Meist authentifiziert, inspiziert und wenn nötig gewartet oder repariert von Experten. Der Hersteller kann es mit einem Zertifikat ausstatten und 2 Jahre Garantie gewähren.

All diese Informationen können in eine Blockchain gespeichert werden. Fakt ist aber, dass für den Erfolg einer Blockchain für Kunstwerke oder für Luxusgüter die Voraussetzung ist, dass möglichst viele Akteure der Blockchain beitreten und eine größtmögliche Offenheit für den Blockchain-Zugang gegeben ist. Ebenfalls gelingt dies nur bei Kunst oder Schmuck, wenn sich diese einem Blockchain-Verfahren bedienen und von Anfang an mit einem Hashwert verbunden werden.

Bei alten Kunstwerken muss die Expertise eines Assessors von heute zuerst in die Blockchain eingegeben werden. Ist diese falsch, ist die Blockchain für einen zukünftigen Käufer wenig hilfreich. Für neue Kunstwerke, bei denen der Künstler selber die Originaleingaben zum Bild oder der Skulptur macht, ist die Blockchain eine sehr interessante Option.

3. Compliance

Um Mehrwert zu schaffen, müssen Unternehmen die Blockchain-Technologie systematisch mit ihrer Strategie und ihren Fähigkeiten verknüpfen. Unsere Wirtschaft und Zusammenleben hängen davon ab, dass der Einzelne Kosten trägt, um zum Gemeinwohl beizutragen, wie z.B. seine Steuern bezahlt. Nichtdestotrotz, solche Regelungen sind anfällig für das Trittbrettfahren (free-riding), bei dem der Einzelne von den Beiträgen Anderer profitiert, ohne selbst Kosten zu tragen. Systeme zur Verfolgung und Sanktionierung von Trittbrettfahrern können die Zusammenarbeit stabilisieren (Yang, Choi, Misch, Xang & Dunham, 2018). Zum Beispiel erwartet das Unternehmen, dass es für die Produkte, die dem Kunden geliefert werden, bezahlt wird. Der Kunde erwartet, dass das Produkt gemäß Beschreibung oder bei Investitionsprodukten gemäß vorgenommener Produkttestresultate funktioniert. Finanz-Mechanismen versuchen, diese Risiken zu minimieren, wie z.B. Versicherungsangebote, wie die Exportrisikogarantie, übernehmen gegen eine Gebühr einen Teil der Fremdwährungsrisiken bei einem Exportauftrag.

Hier kann die Blockchain helfen, dass verschiedene Parteien sich gegenseitig absichern und dass Transaktionen sicher festgehalten werden. Doch auch hier gibt es einige Herausforderungen, um die Anforderungen in Sachen Compliance zu erfüllen und Kosten möglichst gering halten zu können.

In der Schweiz versucht der Bundesrat entsprechende Rahmenbedingungen oder Leitplanken zu setzen. Er will dabei kein eigenes Blockchain-Gesetz schaffen, wie dies andere Länder tun (siehe Liechtenstein - Sektion interessante Ressourcen weiter unten im Whitepaper). Um die Rechtssicherheit zu erhöhen und die Missbrauchsrisiken einzuschränken, schlägt er Änderungen bestehender Gesetzesbestimmungen vor. Die Vernehmlassung dazu wurde am 22. März 2019 eröffnet siehe: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-74420.html

3.1. Datenschutzgrundverordnung

Wichtig in Sachen Blockchain ist hier sicherlich die Datenschutzgrundverordnung
(DSGVO) der EU. Laut DSGVO werden personenbezogene Daten als solche bezeichnet, mit deren Hilfe direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, Geburtsdatum, usw. die Person identifiziert werden kann (siehe auch das Whitepaper vom Deutschen Marketing Verband, Gattiker, Temmen und Sinistra, 2018).

Das von der Europäischen Kommission initiierte EU Blockchain Observatory and Forum hat einen Report zur Blockchain und der DSGVO publiziert (2018-10). Darin wird unter anderem festgehalten, dass es keine DSGVO-konforme Blockchain-Technologie gibt. Nichtdestotrotz, anstatt dessen gibt es DSGVO-konforme Anwendungsfälle und Anwendungen.

Die französische Datenschutzbehörde “Commission Nationale de l’Informatique et des Libertés“ (CNIL) (September 2018) hat in dieser Hinsicht sehr hilfreiche Lösungen in ihrem 11-seitigen Leitfaden vorgeschlagen.

In Bezug auf zusätzliche Daten empfahl die CNIL die Anwendung von Lösungen, bei denen

1. **Daten in Klartextform außerhalb der Blockchain gespeichert werden und**

2. **nur Informationen, die die Existenz der Daten belegen, auf der Blockchain gespeichert werden sollen (d.h. kryptografische Verpflichtung, Fingerabdruck der Daten, die durch die Verwendung einer verschlüsselten Hash-Funktion erhalten wurden, etc.).**

Dies bedingt wie bereits erwähnt, dass eine Rückberechnung der Originaldaten praktisch nicht funktioniert. Ebenfalls soll die Zuordnung der anonymisierten Daten zu den Datensubjekten nur mit einem unverhältnismäßigen hohen Aufwand möglich sein.

Da wir sensible Personendaten wie beispielsweise Alter und Nachname nicht aus einer Blockchain löschen können, ist gemäß CNIL, der einzige mögliche Weg, diese personenbezogenen Daten erst gar nicht in eine Blockchain abzuspeichern. Damit die Sinnhaftigkeit beispielsweise von Lieferketten erhalten bleibt, sieht unser Ansatz wie folgt aus:

1. **Wir generieren eindeutige Identifizierungsmerkmale oder Identifikatoren mit einer Applikation und schreiben diese in eine einfache, von der Blockchain getrennt gehaltene Datenbanktabelle. Also für den Namen ID_A, für die Adresse ID_B etc. Wichtig hierbei ist, dass dies jedes Mal erneut geschieht. Wenn der Name Urs E. Gattiker nochmals auftaucht, bekommt dieser die ID ID_C. Die Applikation speichert also das Identifizierungsmerkmal in der Blockchain und nicht den Namen.**

2. **Wenn nun die Information abgeändert oder gelöscht werden muss, erfolgt das in der separaten SQL-Datenbank. Datenschutzanforderungen werden nun umsetzbar. Um die Sicherheit nochmals zu verbessern, fügen wir hier noch die Compliance-Anforderungen für Datenhaltung hinzu, d.h. wir wollen diese Daten redundant speichern und diese mindestens in die Kategorien Informationsdaten, widerrufliche Einwilligungsdaten und Archivierungsdaten einteilen.**

Wichtig ist auch eine Datenschutz-Folgenabschätzung (DSFA oder engl. PIA) durchzuführen. Der Artikel 35 der DSGVO sieht vor, dass wenn bei neuen Technologien ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, die DSFA gemacht werden muss. Es lohnt sich auch, wenn man dann zum Schluss kommen sollte, dass die Blockchain kein Risiko für persönliche Daten ist. Hiermit wäre dann dokumentiert, dass z.B. in der Anwendung keine personenbezogenen oder personenbeziehbaren Daten gespeichert sind und somit die Blockchain kein erhebliches Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.

COMPETENCE CIRCLE **TECHNOLOGIE, INNOVATION & MANAGEMENT #CCTIM** DMV Whitepaper **Nr. 01 | Januar 2020**

Stellen insgesamt in den Fließtexten highlighten?
Wenn ja, welche?

4. Kosten für eine Blockchain

Ein wichtiges Thema sind wie immer die Kosten. Was braucht es z.B. an Hardware, Software, Personal usw., um eine Blockchain aktiv zu halten. Auch hier gibt es verschiedene Faktoren die berücksichtigt werden müssen wie z.B. Transaktionsvolumen und Transaktionsgröße, Knoten-Hosting Verfahren und Konsensprotokoll (siehe auch Anhang 1).

Die vom Energieverbrauch und auch von der Hardware aus betrachtete wohl teuerste Lösung ist, wenn der Proof of Work (Nachweis der Arbeit) eingesetzt wird, wie z.B. bei Public Blockchains wie Bitcoin.

Eine Transaktion kostet bei ca. 250 Bytes je nach Zeit, usw. zwischen 0,05 und 0,50 Euro.
Meistens werden dazu aber mehrere Transaktionen benötigt, was diesen Beitrag um ein Mehrfaches erhöht, um die Transaktion abzuschließen. Ebenfalls ist wichtig zu berücksichtigen, je später eine Transaktion einem Block hinzugefügt wird, desto teurer wird diese Transaktion.

4.1 Energiekosten und CO2-Ausstoß

Nicht nur finanzielle Kosten, sondern auch der CO2-Ausstoß oder der Carbon Footprint einer Blockchain müssen heute aufgrund des Klimawandels berücksichtigt werden. Eine permissionless oder public/öffentlich Blockchain wie Bitcoin zeigt auf, welche enormen Kosten hier versucht werden. Bitcoin verursacht einen jährlichen CO2-Fußabdruck, fast gleich groß wie derjenige von ganz Dänemark. Bitcoin hat einen jährlichen Stromverbrauch wie Österreich und der Elektroschrottproduktion von Luxemburg (de Vries, nicht datiert, 2018-03).

Wenn das Wort Transaktion in ihrem Kopf eine Finanztransaktion hervorruft, ist dies angebracht. Die Bitcoin-Blockchain ist im Grunde genommen eine Liste aller Bitcoin-Transaktionen seit Beginn von Bitcoin. Auch hier fallen beträchtliche finanzielle und umweltbezogene Kosten an. Zum Beispiel, eine einzige solche Blockchain Transaktion auf Bitcoin entspricht dem CO2-Fußabdruck von 735.537 Visa-Transaktionen (Visa verarbeitet ca. 150 Mio. Transaktionen am Tag) oder 49.036 YouTube Stunden.

Anders ausgedrückt, wenn Alice ein Bitcoin an Peter verkauft, wird viel elektrische Energie benötigt. Das heißt, bis diese Transaktion abgeschlossen ist und somit auf der Blockchain im Ledger vermerkt und bestätigt ist, dass der Bitcoin nun Peter gehört, wird Strom benötigt. Dies entspricht dem Stromverbrauch eines durchschnittlichen US-Haushalts über 20,93 Tage. Anders ausgedrückt, eine Transaktion auf Bitcoin verbraucht soviel Strom wie 20,87 US-amerikanische Haushalte im Schnitt pro Tag. Ethereum schafft es, mit dem Tagesverbrauch von Strom von 0,94 US-Haushalten, eine Transaktion abzuschließen. Zum Vergleich, rund 24% vom totalen Energieverbrauch in einem Haushalt ist die Elektrizität neben z.B. Erdgas oder Heizöl (Eurostat, nicht datiert).

Bitcoin – oder eine „public permissionless“ Blockchain – ist für einen umweltbewussten Verbraucher nicht attraktiv, was die Umweltverträglichkeit betrifft. Das Gleiche gilt für ein Unternehmen, das sich gemäß seinem Corporate Social Responsibility Leitbild wegen Klimaschutz z.B. energiebewusst verhalten will.

4.2 Transaktionskosten

Wir alle fragen uns natürlich, was eine Blockchain-Lösung im Produktionsmaßstab für ein Unternehmen kosten würde.

Eine Konsortium Blockchain bringt z.B. Unternehmen zusammen, die einen für sie wichtigen und oft getätigten Service schneller und genauer abwickeln wollen. Beispielsweise plante JPMorgan Chase ein bestehendes Blockchain-Projekt, um bestimmte Abwicklungsfunktionen zu erweitern. Das auf Blockchain-Technologie basierte Interbank Information Network (IIN) wurde 2017 von JPMorgan Chase, der australischen ANZ-Bank, und der Royal Bank of Canada eingerichtet. Es ermöglicht Probleme wegen fehlerhaften oder aus Compliance-Gründen aufgehaltenen Zahlungen schneller zu lösen. Dies kann sonst manchmal Wochen dauern, wenn mehrere Banken entlang der gesamten Zahlungskette involviert sind (siehe https://drkpi.com/faq-semi-private-und-federated-blockchain/).

Rund 5 bis 20% der Zahlungen scheitern an Fehlern oder Compliance-Problemen laut JPMorgan Chase und deren Experten. Blockchain Features wurde deshalb im Oktober 2019 eingeführt. Bei einer Konsortium Blockchain, wie dem Interbank Information Network mit 220 Bankmitgliedern, wird ein Konsensmechanismus genutzt. In einem Code ist z.B. festgelegt, dass eine Transaktion bzw. ein Block oder eine Entscheidung innerhalb des Netzwerks nur als wahr angenommen werden darf, wenn mehr als eine festgesetzte Anzahl beteiligter Institute diese bestätigen. Dies hilft dem Konsortium einen Konsens zu erzielen. Dies bedeutet, dass man nicht wie in der privaten Blockchain auf die Entscheidung eines Einzelnen warten muss. Da wir hier in der Federated Blockchain eine definierte Mehrheitsentscheidung brauchen, sind betrügerische Aktivitäten von einzelnen Teilnehmern verhindert.

Trotzdem, die Kosten für diese Blockchains müssen berechnet werden. Die Kosten sind sehr unterschiedlich. Diese können z.B. zwischen 0,50 bis 7,00 Euro pro Transaktion ausmachen, wenn die Blockchain auf der Ethernet Plattform stattfindet.

Anders ausgedrückt, um eine Minimum Viable Blockchain (MVB) zu bauen, werden ca. 50 TEUR benötigt. Danach muss auch abgeklärt werden, wo und wie die Daten auf die Blockchain gebracht werden; wie z.B. beim Bauer, der die Eier sammelt, um diese der Handelskette Tesco (UK) zu verkaufen. Ebenfalls muss geklärt werden, wo noch Daten in die Blockchain eingefügt werden. Wichtig ist auch, dass klar ist, wie der Endnutzer (ein industrieller Kunde oder ein Konsument) kontrollieren kann, ob das gekaufte Werkzeug oder die Handtasche echt ist. Dafür reicht im ersten Schritt eine App, die die Ampelfarben anzeigt. Ebenfalls gilt es festzuhalten, was der Kunde im Falle von gelb oder rot (Fälschung) machen kann.

Dies sind alles Kosten, die ebenfalls miteinbezogen werden müssen. Das heißt wird die Technologie eingekauft oder muss diese wie eine App programmiert werden, kostet dies z.B. nochmals mindestens 20 TEUR für ein MVP (Minimum Viable Product). Leider werden diese Kosten von Beratern nicht genau beziffert, wenn diese Publikationen zum Thema veröffentlichen (z.B. EY April 2019). Mehrere MVPs sind fast immer bei solchen Projekten die Realität, bis es dann wirklich funktioniert.

Neben diesen Initialkosten zeigt das Beispiel sehr gut, dass wenn die Blockchain dann läuft, jedes Mal wo Daten in die Blockchain eingefügt werden müssen, Kosten anfallen. Deshalb kann dann passieren, dass die 10-er Packung Eier in der Blockchain aufgeführt wird, aber aus Kostengründen nicht jedes einzelne Ei. Grund ist sicherlich, dass auch der umweltbewusste Käufer nicht bereit ist, für jedes einzelne Ei rund 30% mehr im Laden zu bezahlen, nur weil es auf der Blockchain aufgeführt wird.

Unser Richtwert basiert auf unseren Erfahrungen mit Projekten. Die Kosten mit dem Testen inklusive zusätzlicher Technologien, usw, machen ein Budget von 500 TEUR notwendig. Doch wenn das Problem damit gelöst werden kann, sind die Kosten vielleicht noch etwa 100 bis 300 TEUR im Idealfall oder aber viel mehr im Jahr, was je nach Produkt, Compliance und Reputationsrisiken in vielen Fällen als gering bezeichnet werden kann.

" Jeder Mietvertrag in Malta wird registriert. Das System, mit dem wir die Verträge registrieren werden, ist die Blockchain - Distributed Ledger Technologie... Wir werden den Menschen jetzt den Mehrwert dieser Technologie zeigen, indem wir sie auf etwas anwenden, das sie in ihrem täglichen Leben nutzen werden."
– Joseph Muscat, Premierminister von Malta (Juni 2019)

COMPETENCE CIRCLE **TECHNOLOGIE, INNOVATION & MANAGEMENT #CCTIM** DMV Whitepaper **Nr. 01 | Januar 2020**

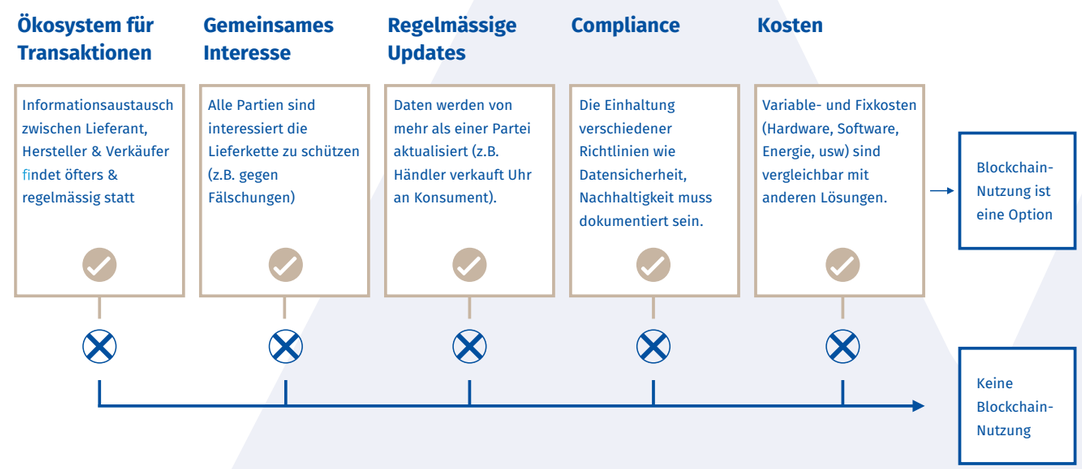
5. Anwendungsmöglichkeiten für Blockchain-Lösungen

Es gibt sicherlich Geschäftsbereiche, in denen die Anwendung von Blockchain mehr Sinn macht, als im Marketing oder im Verkauf. Nichtdestotrotz, Firmen müssen ihre Daten als Anlagegut verwalten, um z.B. Vertrauen, Transparenz und Sicherheit der Lieferkette zu optimieren. Die Stärkung der Unternehmensreputation und die Garantie der Lieferkettensicherheit sind sicherlich auch eine Priorität für Marketing und Vertrieb.

Blockchain-Projekte wie z.B. Ethereum, IOTA, Hyperledger oder andere sind vergleichbar mit Software wie z.B. Salesforce oder SAP. Welche Blockchain Plattform oder Software für das Unternehmen die beste ist, kann erst beurteilt werden, wenn das Unternehmen genau festgelegt hat, welches Problem damit gelöst werden soll.

Blockchain ist ein Lösungsmodell für ein sehr spezifisches Problem. Zentrale Instanzen innerhalb einer Datenbank sollen abgeschafft werden. Die Frage, die ich mir als Unternehmen also stellen muss, ist: Inwiefern ist diese Blockchain-Lösung für mein aktuelles Problem die passende?

Wie funktioniert Kryptographie? Ein Beispiel:



Grafik 4. Erfolgreiche Blockchain-Technologie: vier der fünf Bedingungen gilt es zu erfüllen

Vier der unten aufgeführten fünf Bedingungen sollten erfüllt sein (siehe auch Grafik 4 oben), damit sich eine Blockchain-Lösung empfiehlt.

1. Ökosystem für Transaktionen ist vorhanden: Als Basis brauchen wir ein Ökosystem, in dem grundsätzlich Transaktionen oder ein Informationsaustausch zwischen den Beteiligten stattfindet (z.B. Kunden, Lieferanten, usw.).

2. Gemeinsames Interesse: Es muss sich ein Sachverhalt finden lassen, der alle der möglichen Beteiligten interessiert z.B. die Lieferkette für das Produkt gegen Fakes schützen.

3. Veränderungen finden statt: Um im Netzwerk Aktivitäten zu haben ist es notwendig, dass die Teilnehmer den Zustand des Sachverhalts aktiv verändern (z.B. Das Kaufen und Verkaufen von Produkten). Ein Mehrwert entsteht dabei, wenn es allen Teilnehmenden wichtig ist, darauf vertrauen zu können, dass der Zustand innerhalb des Netzwerks korrekt ist.

4. Compliance: Müssen bestimmte Regularien von allen interessierten Parteien erfüllt werden, wie beispielsweise die Datenschutzgrundverordnung (DSGVO)?

5. Kosten: Eine Kostenkalkulation muss vorgenommen werden. Diese ermöglicht anhand der Werte der Produkte und Dienstleistungen, die über die Blockchain abgewickelt werden, zu entscheiden, ob dies eine finanziell praktikable Lösung darstellt.

Um die Problematik wie oben angedeutet besser veranschaulichen zu können, haben wir unten zwei Beispiele aus der Unternehmenspraxis aufgeführt.

5.1 Beispiel Rohstoffe und Compliance

2017 wurde auf EU-Ebene die Konfliktmineralienverordnung [Infos dazu gibt es hier: https://ec.europa.eu/trade/policy/in-focus/conflict-minerals-regulation/regulation-explained/index_de.htm] verabschiedet. Am 1. Januar 2021 wird in der EU die Verordnung über Konfliktmineralien in Kraft treten. Diese legt besondere menschenrechtliche Sorgfaltspflichten fest, wenn Gold, Tantal, Zinn und Wolfram (3TG) aus Konflikt- und Hochrisikogebieten eingeführt werden.

Hier können wir eine Lösung finden, die es ermöglicht, vom Abbau bis zum Kunden nachvollziehen zu können, ob die Mineralien aus einem Konfliktgebiet stammen oder nicht. Die Schwierigkeit liegt darin, dass entschieden werden muss, wer die Kontrolle durchführt und wo diese anfängt. In der Demokratischen Republik (DR) Kongo werden die Erze von ca. 500.000 “selbstständigen“ Minenarbeitern in Tausenden einzelner Abbaustellen gefördert, die unmöglich alle überwacht werden können. Aber nur eine Rund-um-die-Uhr-Überwachung würde garantieren, dass die Rohstoffe tatsächlich konfliktfrei abgebaut und gehandelt werden.

Es gilt in den Herkunftsländern das Angebot an zertifizierten Rohstoffen schrittweise zu erhöhen. Das dies schwierig ist, beschreibt Intel. Das Unternehmen brauchte über vier Jahre, um die Lieferkette für die Produktion von Chips von Konfliktmaterial (conflict mineral nennt es die US Securities und Exchange Commission) zu befreien [Hier erklärt Intel diese Problematik im Detail https://www.intel.com/content/www/us/en/corporate-responsibility/conflict-free-minerals.html].

5.2 Beispiel Produktpiraterie und Compliance für die Lieferkette

Die RL 2014/33/EU über Aufzüge und Sicherheitsbauteile regelt die Anforderungen im Europäischen Wirtschaftsraum [Siehe https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014L0033]. Ein Sicherheitsbauteil für einen Aufzug kann z.B. eine Verriegelungseinrichtung der Fahrschachttüren oder ein Geschwindigkeitsbegrenzer sein. Auch elektrische Sicherheitseinrichtungen in Form von Sicherheitsschaltungen mit elektronischen Bauelementen für Aufzüge sind durch diese Regulierung betroffen.

Entscheidend ist hier, wie das Unternehmen sicherstellen kann, das ein Originalteil, das vom Zulieferer garantiert ist, auch in dem für das Sicherheitsteil vorgesehenen Fahrstuhl eingebaut wird. Hier kann die halb-private Blockchain Abhilfe schaffen und anhand der Daten genau aufzeigen, wann z.B. ein Originalteil vom Hersteller fertiggestellt war und von A nach B transportiert wurde. Wenn es dann auf einem anderen Kontinent auftaucht, weiß der Monteur mit der Hilfe von einem Codesystem (rot, orange und grün), dass das vor ihm liegende Teil eine Fälschung ist. Es gibt hier verschiedene Möglichkeiten von der App, bis zur Überprüfung der Legierung, usw. Wichtig ist, dass diese Sicherheitsmechanismen genau geplant sind. Nur dann ist es möglich, in die Lieferkette mehrere Kontrollpunkte einzubauen. Diese helfen, das Risiko für den Service-Techniker und den Kunden zu minimieren, dass ein Falschteil eingebaut wird.

6. Fazit und Schlussfolgerungen

Blockketten sind manipulationssichere und manipulationsgeschützte digitale Ledger, die dezentral (d.h. ohne zentrales Repository) und in der Regel ohne zentrale Behörde (d.h. Bank, Unternehmen oder Regierung) implementiert werden. Auf ihrer grundlegenden Ebene ermöglichen sie es einer Gemeinschaft von Benutzern, Transaktionen in einem gemeinsamen Ledger innerhalb dieser Gemeinschaft zu erfassen, so dass unter normalen Betrieb des Blockchain-Netzwerks keine Transaktion nach ihrer Veröffentlichung geändert werden kann.

Die beeindruckenden Ergebnisse zeigen, dass Blockketten verwendet werden, um Informationen zu speichern, Intermediäre auszuschalten und eine bessere Koordination zwischen Unternehmen zu ermöglichen, z.B. in Bezug auf Datenstandards.

Wenn Journalisten Studien zitieren, in denen Umfrageteilnehmer von deutschen Unternehmen (Konzerne, usw.) zu über 90% angeben, in 2019 Blockchain-Lösungen an den Start zu bringen, lässt dies aufhorchen. Dies wäre aber nur möglich gewesen, wenn alle diese Unternehmen

1. Die Technologie inklusive der Herausforderungen in Sachen Skalierbarkeit, Energieverbrauch, usw. verstehen würden, und

2. ein genau definiertes Problem haben, das mit Hilfe der Blockchain besser gelöst werden kann, als mit einer anderen Technologie (siehe auch Grafik 4 oben).

Wenn die beiden obigen Voraussetzungen erfüllt werden, kann mit der Umsetzung begonnen werden. Es gilt, ein Minimum-Viable-Product (MVP) zu bauen. Mit der MVP-Blockchain kann dann ausprobiert werden, inwiefern sich die Pläne haben realisieren lassen und welche Verbesserungen noch nötig sind.

Blockchain: Die drkpi® Methodik in 4 Schritten

1. Analyse

SWOT Potential für neue Produkte in Marktnischen

2. Projektierung

Messbahre Prioritäten für die nächsten 3 Jahre setzen.

3. Umsetzung

Bau einer Minimum Viable Blockchain (MVB) in 4-8 Monaten

4. Kontrolle

Auswertung der Kennzahlen zur Bewertung der umgesetzten Massnahmen

Grafik 5. Vier Schritte für die erfolgreiche Umsetzung einer Blockchain

Vier der unten aufgeführten fünf Bedingungen sollten erfüllt sein (siehe auch Grafik 4 oben), damit sich eine Blockchain-Lösung empfiehlt.

1. Ökosystem für Transaktionen ist vorhanden: Als Basis brauchen wir ein Ökosystem, in dem grundsätzlich Transaktionen oder ein Informationsaustausch zwischen den Beteiligten stattfindet (z.B. Kunden, Lieferanten, usw.).

2. Gemeinsames Interesse: Es muss sich ein Sachverhalt finden lassen, der alle der möglichen Beteiligten interessiert z.B. die Lieferkette für das Produkt gegen Fakes schützen.

3. Veränderungen finden statt: Um im Netzwerk Aktivitäten zu haben ist es notwendig, dass die Teilnehmer den Zustand des Sachverhalts aktiv verändern (z.B. Das Kaufen und Verkaufen von Produkten). Ein Mehrwert entsteht dabei, wenn es allen Teilnehmenden wichtig ist, darauf vertrauen zu können, dass der Zustand innerhalb des Netzwerks korrekt ist.

4. Compliance: Müssen bestimmte Regularien von allen interessierten Parteien erfüllt werden, wie beispielsweise die Datenschutzgrundverordnung (DSGVO)?

5. Kosten: Eine Kostenkalkulation muss vorgenommen werden. Diese ermöglicht anhand der Werte der Produkte und Dienstleistungen, die über die Blockchain abgewickelt werden, zu entscheiden, ob dies eine finanziell praktikable Lösung darstellt.

Um die Problematik wie oben angedeutet besser veranschaulichen zu können, haben wir unten zwei Beispiele aus der Unternehmenspraxis aufgeführt.

6.1 Metriken und schlüsselrelevante Kennzahlen

Wichtig im Zusammenhang mit der Blockchain ist ebenfalls, dass sich das Unternehmen damit auseinandersetzt, was die schlüsselrelevanten Kennzahlen betrifft. Zum Beispiel hat sich Telefonica kürzlich entschieden E-plus, Genion und weitere Marken, die sie in Deutschland besitzt, zu verkaufen. Doch es ist schwierig zu entscheiden, welche Metrik genutzt wird, um die Brand Equity (Markenwert) von solchen Marken zu messen.

Genau die gleiche Problematik haben wir auch bei der Blockchain. Ohne eine Metrik ist es nicht möglich zu entscheiden, ob das eine Blockchain-System besser ist als das andere. Deshalb müssen wir mehr Energie darauf verwenden, die wichtigsten Leistungsindikatoren zu erstellen und diese genau zu messen, anstatt uns über den Aufwand für diese kritische Arbeit zu beschweren.

Die richtigen Metriken und/oder die schlüsselrelevanten Kennzahlen zu entwickeln, um die Effektivität und Effizienz der Blockchain zu verfolgen, ist keineswegs einfach.

Unser Ansatz nutzt steuerungsrelevante Kennzahlen. Diese ordnen wir unter der Gruppe SMART Metrics ein. SMART steht dabei für Specific, Manageable, Actionable, Relevant, Trending Metrics oder auf deutsch so etwa: Spezifisch, handhabbar, umsetzbar, relevant, zeitvergleichend.

Wir wollen konkrete schlüsselrelevante Kennzahlen (KPIs), die wir relativ schnell über die Blockchain erheben können. Ebenfalls müssen diese umsetzbar sein. Das impliziert wiederum, dass es Konsequenzen haben wird, ob wir über oder unter einem definierten Budget sind. Es sind nur die KPIs relevant, die helfen, die Dinge weiter zu optimieren. Es ist zu empfehlen, darauf zu achten, dass die KPIs auch vom Top Management als relevant betrachtet werden.

SMART Metrics beinhalten immer Kennzahlen, die relevant für das Controlling sind, wie beispielsweise Kosten. Zu guter Letzt wollen wir natürlich die Kennzahlen über mehrere Perioden vergleichen. Damit können wir sehen, ob der Trend in die richtige Richtung zeigt.

Hier ein paar Beispiele von SMART Metrics, die wir in unserem Business im Blockchain-Bereich einsetzen:

1. Kosten pro Transaktion: Mehrere Faktoren beeinflussen diese Kosten, wie was ein Teilnehmer in der Blockchain bekommt, der gewillt ist, den Ledger zu ändern.

2. Fixkosten: Beispielsweise Hardware, Software, Server und bauliche Maßnahmen, um die Blockchain starten zu können.

3. Variable Kosten: Ein Beispiel ist der Energieverbrauch, der wiederum vom Transaktionsvolumen abhängig ist; d.h. desto mehr Transaktionen desto höher der Energieverbrauch für die Blockchain-Teilnehmer oder Nodes.

4. Komplexität der Transaktion: Smart Contracts können Prozesse vereinfachen, jedoch vergrößern diese die Datensätze, was wiederum Kosten nach sich zieht.

5. Anzahl der Teilnehmer: Mehrere Teilnehmer wie z.B. Anzahl der Organisationen, die in einer halbprivaten Blockchain einen Node betreuen, erhöhen die Kosten.

6. Verwahrungs- und Depotkosten: Custody-Funktionen, d.h. wenn Wertpapiere oder Dokumente wie Urkunden usw. auf der Blockchain aufbewahrt werden, kostet dies ebenfalls. Ob die Höhe dieser Kosten vergleichbar sind mit Bank Depots, muss ausgerechnet werden.

Die oben aufgeführten Kennzahlen sind nur ein Anfang, um ein Rahmen für ein effektives und logisches Kostenmodell für eine Blockchain entwickeln zu können. Aber ein effektives Projektmanagement für ein Minimum Viable Product (MVP) in Sachen Blockchain muss eine solche Kalkulation beinhalten, um die nächsten realistischen Schritte in die Wege leiten zu können.

Arbeitet die Blockchain korrekt? Ein Audit ist Pflichtprogramm

Grafik 6.

6.2 Audit der Blockchain ist Pflichtprogramm

Wie immer muss auch eine Blockchain überprüft werden. Beispielsweise meldete ABI (Association of British Insurers) im September 2019 (ABI, nicht datiert), dass der durchschnittliche Versicherungsbetrug die Summe von 12.000 britischen Pfund pro aufgedeckten Fall ausmacht. Täglich werden rund 1.300 Versicherungsbetrugsfälle aufgedeckt. Hier können Smart Contracts helfen, solche Betrugsversuche aufzudecken und die nicht betrügerischen Fälle schneller auszahlen zu können. Doch muss kontrolliert werden, ob die gemachten Rückschlüsse und Entscheidungen solcher programmierten Kontrakte auch den wirklichen Tatsachen entsprechen. Fehler können hier viel Ärger auslösen, die Reputation der Versicherung beschädigen und unnötige Kosten verursachen.

6.3 Kann die Blockchain unsere Lieferkette und die Dating-Kultur revolutionieren?

Was das Management der Lieferkette oder das Life-Cycle Management für ein Produkt betrifft, haben unsere Beispiele hier gezeigt, dass einige Änderungen in der Umsetzung sind. Sowohl für Start-ups als auch für Mittelständler können verteilte Ledger-Technologien neue Geschäfts- und Betriebsmodelle ermöglichen. Auf der Blockchain kann jede Transaktion nachverfolgt werden. Die Sequenz der Ereignisse ist fest definiert und für immer im Blockchain-Netzwerk gespeichert.

Um Mehrwert zu schaffen, müssen Unternehmen die Blockchain-Technologie systematisch mit ihrer Strategie und ihren Fähigkeiten verknüpfen.

Der Schlüssel zur besseren Datenverantwortung und Datensicherheit ist natürlich ein ganzheitlicher, verteidigungsorientierter Ansatz. Dieser muss sich auf die Prävention, Erkennung, Eindämmung und Wiederherstellung von Sicherheitsvorfällen konzentrieren. Die Blockchain hilft bei der Prävention wie auch bei der Erkennung und Eindämmung von Sicherheitsvorfällen mit z.B. gefälschten Produkten, die als Originale verkauft werden.

Bei der Eindämmung von unautorisiertem Nutzen von Daten hilft z.B. die Blockchain. Beispielsweise werden die PII (Personally Identifiable Information) Daten verschlüsselt aufbewahrt. Ebenfalls werden diese PII wie Angaben zum Alter, Geschlecht und Kundenadressen nicht auf der Blockchain aufbewahrt. Wir generieren eindeutige Identifizierungsmerkmale oder Identifikatoren mit einer Applikation. Diese Identifizierungsmerkmale werden auf der Blockchain aufbewahrt. Sie zeigen, wer die Transaktion veranlasst hat (Alice verkauft an Urs), können aber nur in der von der Blockchain getrennt gehaltenen Datenbanktabelle eingesehen werden (siehe Teil 3.1 oben für weitere Erklärungen).

Ebenfalls gilt es mit Hilfe von Network Segmentation (z.B. verschiedene Blockchain für unterschiedliche Lieferketten und deren Produkte), das Risiko besser zu verteilen. Dabei ist ein Key (Schlüssel) Management der privaten oder öffentlichen Schlüssel ebenfalls wichtig (Pal, 2019).

Was wir nicht außer Acht lassen dürfen, ist das Blockchain, wie oben erläutert, nicht immer der beste Ansatz ist. Unabhängig vom dem sind Distributed Computing und Asymmetrische Kryptografie beides Technologien, die eine wichtige Rolle spielen. Sie finden aber auch außerhalb der Blockchain regen Zuspruch und werden immer mehr genutzt, um die Sicherheit von Daten wie auch das Supply-Chain Management zu verbessern.

Ob die Blockchain-Technologie die Dating Kultur verändert und vielleicht die Suche nach einem Lebenspartner mit der Möglichkeit lebenslanger Kompatibilität vereinfacht, ist noch nicht ganz klar. Selbstverständlich gibt es auch hier schon Bewegungen mit Hilfe der Blockchain die Dinge zu verbessern. Das Luna Dating Network versucht, Blockchain-Technologie zu nutzen. Interessant ist dabei, dass einige Aktivitäten außerhalb der Blockchain passieren, sodass PII Daten (Personally Identifiable Information), wie beispielsweise sensible Daten (wie Alter, Geschlecht und Adresse) nicht in der Blockchain gespeichert werden (Ornish, Gupta, Martin & Buchanan, 2017-10-24). Dies wiederum ermöglicht dem Luna Dating Network in Sachen Datenschutz Grundverordnung (DSGVO) sowie dem California Consumer Privacy Act (CCPA), der Juli 2020 in Kraft tritt, compliant zu sein.

Zu guter Letzt, wenn Ihr Unternehmen einen zentralisierten Ledger benötigt, der alle Änderungen von Anwendungsdaten aufzeichnet und eine unveränderliche Aufzeichnung dieser Änderungen pflegt, kann mit Hilfe einer Blockchain eine Ledger-Datenbank bereitgestellt werden. Diese Datenbank ist idealerweise leistungsstark, natürlich unveränderlich und kryptographisch überprüfbar. Dann müssen keine komplexen Prüfungstabellen oder Blockchain-Netzwerke erstellt werden.

Wenn die Funktionen der Unveränderlichkeit und Überprüfbarkeit von einem Ledger bereitgestellt werden sollen und Ihr Unternehmen außerdem mehreren Parteien die Möglichkeit geben möchte, Geschäfte ohne eine vertrauenswürdige, zentralisierte Instanz abzuschließen, kann es von Vorteil sein, eine skalierbare Blockchain zu nutzen.

Im Gegensatz zu Bitcoin ist Lira nicht spekulativ und ein Versuch, mit Hilfe hinterlegter Werte eine stabile Kryptowährung zu lancieren. Doch die regulatorischen Hürden in den USA und EU sind hoch. Deshalb erscheint dessen laut Facebook geplante Lancierung im Dezember 2020 als eher unwahrscheinlich. Trotzdem ist die Blockchain die Technologie, die es erlaubt, Transaktionen zurückzuverfolgen. Dadurch sind Transparenz, Sicherheit und Unveränderlichkeit dieser Transaktionen oder beispielsweise der Einbau von Ersatzteilen gewährleistet. Im internationalen Zahlungsverkehr, Energie- und Kunsthandel sowie Supply-Chain Management, kommt die Blockchain bereits wirkungsvoll zum Einsatz. Da es etwa drei Jahrzehnte dauerte, bis das Internet vom Arpanet zum World Wide Web wechselte, sind wir mit der Blockchain also noch im Zeitplan.

Referenzliste

ABI (not dated, 2017). Fraud. London, UK: Association of British Insurers (ABI). Retrieved 2018-11-10 from https://www.abi.org.uk/products-and-issues/topics-and-issues/fraud/ siehe auch 2019-09 https://www.abi.org.uk/news/news-articles/2019/08/detected-insurance-frauds-in-2018/

Commission Nationale de l'Informatique et des Libertés" (CNIL) (2018-09). Premiers éléments d'analyse de la CNIL. Blockchain. Aufgerufen am 1. September 2019 auf https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf . Siehe auch https://www.mll-news.com/cnil-veroeffentlicht-leitfaden-zum-datenschutz-bei-blockchain-technologien/

de Vries, Alex (nicht datiert). Bitcoin energy consumption index. Digiconomist Webseite. Aufgerufen am 4. Sept. 2019 auf https://digiconomist.net/bitcoin-energy-consumption und https://digiconomist.net/ethereum-energy-consumption. Die Annahmen für diese Kalkulationen können hier eingesehen werden: https://digiconomist.net/bitcoin-energy-consumption#assumptions

de Vries, Alex (2018-03). Bitcoin's growing energy problem. Joule, 2(5), pp. 801-805. DOI: DOI: https://doi.org/10.1016/j.joule.2018.04.016 Summary retrieved 2018-11-08 from https://digiconomist.net/bitcoins-growing-energy-problem

EU Blockchain Observatory and Forum (2018-10). Blockchain and the GDPR. A thematic report prepared by the European Union Blockchain Observatory and Forum. Aufgerufen am 15 Juli, 2019 von https://www.eublockchainforum.eu/reports

EUIPO 2019 Status report on IPR Infringement. Why IP rights are important, IPR infringement and the fight against counterfeiting and piracy. Brüssel: European Union Intellectual Property Office. Aufgerufen 2019-09-17 auf https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/docs/2019_Status_Report_on_IPR_infringement/2019_Status_Report_on_IPR_infringement_en.pdf

EU Commission Taxation and Customs Union (2019-09). Report on the EU customs enforcement of intellectual property rights: Results at the EU border, 2018. Luxemburg: European Union. Aufgerufen am 2019-09-20 auf https://ec.europa.eu/taxation_customs/sites/taxation/files/2019-ipr-report.pdf

Eurostat (nicht datiert). Energy consumption in households. Aufgerufen am 1. September 2019 auf https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_consumption_in_households

EY (2019-04) Total cost of ownership for blockchain solutions. Ernst & Young. Aufgerufen am 2019-08-31 auf https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf

Gattiker, Urs E.; Temmen, Taina; Sinistra, Patrizia (2019-01). Künstliche Intelligenz: Roboter Lisa räumt die Küche auf und jobbt als Wirtschaftsprüfer. Whitepaper. Duesseldorf: Deutscher Marketing Verband e.V. (DMV). Aufgerufen am 2019-01-04 auf https://MCLago.com/download/30/

Gattiker, Urs E., Temmen, Taina, Sinistra, Patrizia (2018-04, 2. rev. Auflage). EU-Datenschutzgrundverordnung (DSGVO): Was ist Sache für Marketing Manager, Geschäftsleitung und Vorstand? Whitepaper. Düsseldorf: Deutscher Marketing Verband e.V. (DMV). Aufgerufen am 2019-08-31 auf https://MCLago.com/download/13/

Higginson, Matt, Nadeau, Marie-Claude and Rajgopal, Kausik (January 2019). Blockchain's Occam problem. McKinsey Blog. Retrieved 2019-01-21 from https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem

Lex (2019-03-30/31). Second-hand luxury: thrift shift. Financial Times, S. 22.

Noonan, Laura (2019-04-21). JPMorgan to widen use of blockchain system. Platform aimed at tackling compliance issues to be used to validate payments. Financial Timels. Retrieved, August 30, 2019 from https://www.ft.com/content/87ae3010-61ec-11e9-b285-3acd5d43599e

Ornish, Andree, Gupta, Vinay, Martin, Aella, & Buchanan, Aeron (2017-10-24). Luna. Draft 1. Aufgerufen am 15 September, 2019 auf https://drkpi.com/download/5

Pal, Monica (2019-08-29). Hacked! Neil Daswani on security lessons from big name breaches. 4iQ Blog. Aufgerufen am 30. August 2019 auf https://4iq.com/hacked-neil-daswani-on-security-lessons-from-big-name-breaches/

Tortermvasana, Komsan (2019-08-29). Blockchain easing customs process. Thailand second in Asean to use system. Bangkok Post. Aufgerufen am 30. August, 2019 auf https://www.bangkokpost.com/tech/1738611/

Uhlmann, Sacha (2017) Reducing counterfeit products with blockchains. Master thesis, University of Zurich, Dept. of Informatics. Retrieved June 1, 2019 from https://www.merlin.uzh.ch/contributionDocument/download/10024

Wanger-Baumann, Cindy (August 2019). Blockchain smart contracts for reimbursement of special medications in Switzerland - A pilot process innovation project to demonstrate the barriers and success factors for introduction of disruptive innovation in the Swiss healthcare system. Master thesis, Department of Management, Technology and Economics, ETH Zurich.

Yaga, Dylan, Mell, Peter, Roby, Nik, & Scarfone, Karen (October 2018). Blockchain Technology Overview (NISTIR 8202). National Institute of Standards and Technology. Aufgerufen September 1, 2019 auf https://csrc.nist.gov/publications/detail/nistir/8202/final

Yang, Fan, Choi, You-Jang, Misch, Antonia, Yang, Xing, & Dunham, Yarrow (2018). In definse of the commons: Young children negatively evaluate and scanction free riders. Psychological Science, 29(10), 1598-1611. Aufgerufen am 1. September 2019 auf DOI: https://doi.org/10.1177/0956797618779061

https://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:32014L0033

COMPETENCE CIRCLE **TECHNOLOGIE, INNOVATION & MANAGEMENT #CCTIM** DMV Whitepaper **Nr. 01 | Januar 2020**

Interessante Ressourcen

Zusätzliche weiterführende Ressourcen in Form von Checklisten, Tools und Tipps gibt es zum Thema Blockchain auch hier:

- Marketing Club Lago: https://mclago.com/tag/blockchain
- DrKPI: https://drkpi.com/tag/blockchain/

Hansen, Patrick, Britze, Nils, Wingelmann, Martin und weitere Autoren (2019). Evaluierung und Implementierung von Blockchain Use Cases. Leitfaden. Berlin: Bitkom. Aufgerufen 2019-09-18 auf https://www.bitkom.org/sites/default/files/2019-09/leitfaden_evaluierungundimplementierungvonblockchainusecases_190917.pdf

Kuzmanovic, Aleksandar (May 2019). Net neutrality: Unexpected solution to blockchain scaling. Communications of the ACM, 62(6) , pp. 32-34. Aufgerufen am 30. August, 2019 auf DOI: https://doi.org/10.1145/3319422

Murphy, Hannah (December 20, 2018). Bitcoin miners see to crack survival code. Financial Times, Companies, p. 14. Retrieved 2018-12-21 from https://www.ft.com/content/98d52c50-fd37-11e8-aebf-99e208d3e521

Pasquier, Thomas Eyers,David & Bacon, Jean. (May 2019). Personal data and the internet of things. Communications of the ACM 62(6), pp. 32-34. Aufgerufen am 30. August, 2019 auf DOI: https://doi.org/10.1145/3322933

Saydiari, Sami, O. (Mai 2019). Engineering trustworthy systems: a principled approach to cybersecurity. Communications of the ACM, 62(6), pp. 63-69. Aufgerufen am 30. August, 2019 auf DOI: https://doi.org/10.1145/3282487

Regularien – Zwei Leaders

Liechtensteins Regierung hat am 7. Mai 2019 als erstes Land der Welt ein Blockchain-Gesetz verabschiedet, das am 1. Januar 2020 in Kraft trat. Das Land wird als globaler Blockchain-Vorreiter eingestuft. Das Gesetz bietet branchenneutrale Rechtssicherheit und dient auch der Industrie und weiteren Dienstleistungsanbietern.

Die Eidgenössischen Finanzmarktaufsicht Finma hat am 26. August 2019 weltweit erstmalig zwei Blockchain-Finanzdienstleistern eine Bankenbewilligung erteilt. Dabei handelt es sich um die in Zug ansässige Seba Crypto AG Zug und die Sygnum AG mit Sitz in Zürich.
Die Finma erteilte den zwei neuen Blockchain-Finanzdienstleistern je eine Bank- und Effektenhändlerbewilligung,

Um die Geldwäscherei zu bekämpfen, müssen die beiden Finanzinstitute - wie bei einer herkömmlichen Banküberweisung - auch bei Transaktionen von Kryptowährungen zwingend Angaben zum Auftraggeber und zum Begünstigten übermittelt werden. Nur so können die Beteiligten einer Überweisung mit Sanktionslisten abgeglichen werden. Mehr unter: Kryptofinanzplatz Schweiz und Blockchain -- CH-Banken handeln mit Bitcoin: https://drkpi.com/faq-semi-private-und-federated-blockchain/

Glossar

Bitcoin
Wenn man heute das Wort Blockchain hört, denken viele zuerst einmal an die digitale Kryptowährung Bitcoin. Bitcoin ist eine digitale Währung, die elektronisch hergestellt, gehandelt und verwahrt wird. Blockchain als Protokoll und im Sinne einer verteilten Datenbank entstand 2008, als Satoshi Nakamoto dieses im Whitepaper zu Bitcoin beschrieb. 2009 wurde von ihm die erste Implementierung der Software Bitcoin veröffentlicht. Dies war der Startschuss für die Blockchain-Technologie.

Blockchain
Wortwörtlich aus dem Englischen übersetzt, bedeutet Blockchain („chain" = Kette) soviel wie "Blockkette" – in diesem Fall eine Kette aus Transaktionsblöcken. Man könnte die Blockchain als ein digitales Register betrachten, das Transaktionen zwischen einem Verbraucher und einem Lieferanten verzeichnet.

Vereinfacht erklärt können wir uns eine Blockchain wie ein Kassenbuch vorstellen. Wenn Absender und Empfänger eine Datentransaktion auslösen, wird in das Kassenbuch eine neue Position eingetragen. Viele weitere Computer haben das gleiche Kassenbuch und die neue Transaktion wird auch überall dort angezeigt. Erst nachdem die Transaktion von allen Computern mit einer Kopie dieses Kassenbuches authentifiziert wurde, ist die Transaktion gültig. Diese Zeile oder Position kann, nachdem sie bestätigt wurde, nicht mehr verändert werden. Das macht eine Blockchain so gut wie fälschungssicher.

Bei einer "public" (=öffentlich) oder „permissionless" (=erlaubnislos) Blockchain wie z.B. Bitcoin, kann jeder mitmachen, solange er die Software auf seinem Server laufen lässt.

Bei einer privaten oder „permissioned" (=erlaubten) Blockchain braucht der Interessent die Erlaubnis vom Besitzer oder dem Konsortium, das er mitmachen kann (für mehr Detail; siehe das Whitepaper, Sektionen 1.1 - 1.4).

Kryptowährungen
2011, zwei Jahre nach der Einführung des Bitcoins, kam mit Litecoin (2011) eine weitere Kryptowährung, gefolgt von Bytecoin (2012), Ripple (2013), Dogecoin (2013) usw. auf den Markt. Bis zum Jahre 2014 gab es kaum mehr als zehn digitale Währungen. Seit 2015 sind jedoch viele Kryptowährungen kreiert worden. Einige sind seitdem bereits auch schon wieder verschwunden.

Die Schweizerische Nationalbank (SNB) ist der Meinung, dass die dezentral verteilte Technologie (DLT) - oder kurz Blockchain - künftig mit konventionellen Lösungen zusammenspielen sollte. Doch findet die SNB, dass herkömmliche Systeme im Zahlungsverkehr vorläufig den DLT-Blockchain-Lösungen überlegen sind (Fischer, 2019-03-19, S. 31). Trotzdem hinderte dies die Eidgenössische Finanzmarktaufsicht (FINMA) nicht daran, am 26. August 2019 zwei Blockchain-Dienstleistern die Banklizenz erteilen. Dies ist laut FINMA weltweit der erste Fall, in dem sich ein Regulator zu diesem Schritt entschied.

Bitcoin läuft auf einer Public Blockchain, d.h. jeder kann mitmachen, solange er die Software auf seinem Server installiert hat und diese läuft. Das heißt, niemand muss gefragt werden, ob man mitmachen kann. Dies macht es aber wiederum schwierig, die Richtlinien zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung einhalten zu können, da man seinen Transaktionspartner weder kennt, noch weiß, wie er die Mittel bekommen hat (z.B. legal und versteuert, siehe auch Libra).

Glossar

Distributed Ledger
Oftmals wird der Überbegriff "Distributed Ledger" synonym für das Wort Blockchain verwendet. Jedoch nicht jeder Distributed Ledger verwendet unbedingt eine Blockkette.

Libra
Was ist eine Libra? Facebook sagt, dass Libra eine „globale Währungs- und Finanzinfrastruktur" ist. Mit anderen Worten, es handelt sich um digitales Vermögen oder eine Kryptowährung, die von Facebook erstellt wurde. Dazu will das Projekt eine von Facebook erstellte Version der Blockchain nutzen (genau gesagt eine Permissioned Blockchain).
Wenn die Kryptowährung wie geplant Ende 2020 startet, können Benutzer Calibra herunterladen. Calibra ist eine digitale Brieftasche, die es dem Nutzer ermöglicht, die Kryptowährung an jeden Smartphone-Besitzer zu senden. Es soll auch in WhatsApp und als eigenständige App verfügbar sein.
Die Europäische Kommission ist besorgt über die möglichen Auswirkungen des Libra-Projekts. Aus diesem Grunde versandte die EU-Kommission Anfang Oktober 2019 einen Fragebogen an das Libra-Projekt. In einer Reihe von Fragen will die EU-Kommission wissen, welche möglichen Auswirkungen und Risiken das Libra-Projekt darstellt, was Finanzstabilität, Geldwäsche und Datenschutz betrifft.

Diese Angaben werden in die Überarbeitung der Regulierung digitaler Währungen einfließen, an denen die EU-Kommission zur Zeit arbeitet. Regulatoren wollen sicher gehen das Libra und ähnliche digitale Währungen weder das Finanzsystem destabilisieren, noch die regulatorischen Arbeiten von Regierungen und Zentralbanken zunichtemachen. So ließ PayPal, einer der Gründerfirmen des Libra-Projektes, am 4. Oktober 2019 verlauten, dass es sich aus Libra zurückziehen wird. PayPal führte als Argument für diesen Schritt die Tatsache an, dass Facebook nicht genug getan hatte, um die regulatorische Gegenreaktion gegen das Projekt in der Planung von Libra zu berücksichtigen. Frankreich will z.B. wegen diesen regulatorischen Fragen nicht, dass Libra in der EU genutzt werden kann. Singapore's Notenbank Präsident Ravi Menon warnte im September 2019, dass Libra die Makro-Stabilität gefährden könnten. Verschiedene Notenbankchefs sind der Meinung, dass Libra durch Notenbanken überwacht werden müsse. Ebenfalls sollen die gleichen regulatorischen Vorschriften gelten wie für klassische Finanzinstitute.
Durch diesen regulatorischen Widerstand aus Europa und den USA haben z.B. die Libra-Partner Mastercard und Visa kalte Füße bekommen und sind ebenfalls noch im Oktober 2019 aus dem Projekt verabschiedet.

Was unterscheidet Libra von Bitcoin? Private Distributed Ledger Technologien oder DLTs werden auch „permissioned" Blockchains genannt, d.h. Blockketten fungieren als geschlossene Ökosysteme, in diesem Falle Facebook. Als Facebook-Nutzer mit der digitalen Calibra-Geldbörse kann der Benutzer nur mitmachen, wenn die Libra Vereinigung ihn teilnehmen lässt. Die Transaktionen verifizieren können nur Libra-Mitglieder, meist große Konzerne wie Facebook, usw..

Bei einer „permissionless" (oder public) Blockchain wie Bitcoin kann jeder ohne notwendige Autorisierung auf der Blockchain lesen und schreiben.

Sicherheit
Jeder Datensatz in der dezentralen Datenbank (d.h. Blockchain) wird durch die Speicherung des Hashwertes des vorangehenden Datensatzes gesichert. Der Hashwert ist eine Art virtueller Daumenabdruck des Datensatzes (siehe auch Grafik 3).

Bevor eine Transaktion stattfinden kann, muss diese von jedem Rechner aus bestätigt werden. Selbstverständlich verschlüsselt, um die Sicherheit der Transaktion gewährleisten zu können. Dann fügt sich alles zu einer Kette zusammen und wird dann in einen Computer-Code umgewandelt.

Smart Contract
Smart Contracts sorgen dafür, dass einzelne Schritte automatisch ausgelöst werden, falls die vordefinierten Bedingungen erfüllt sind. Wenn beispielsweise von dritter Seite die Bestätigung vorliegt, dass ein Exporteur die vereinbarte Ware in der vereinbarten Menge und Qualität and den Kunden geliefert hat, wird die Zahlung ausgelöst.

Stablecoin
Libra basiert wie Bitcoin, Ethereum & Co. auf der Blockchain, im Gegensatz zu diesen soll Facebooks Kryptowährung im Wert stabil sein: Libra wurde als sogenannter Stablecoin konzipiert und ist durch einen Reservefonds gedeckt. Der Reservefonds soll aus verschiedenen Währungen bestehen. Doch die finanziellen Risiken, die diese nationalen Währungen mit sich bringen, müssen noch abgeklärt werden (siehe auch Libra oben).

Anhang 1 - Kostentypen für eine Blockchain

Vier Inputs beeinflussen vor allem die Kosten für öffentliche und private Blockchain-Lösungen. Diese Inputs hängen zu fast 100% vom Anwendungsfall und den Zielen ab, die ein Unternehmen oder eine Gruppe von Unternehmen erreichen will.
Wir haben unten die vier wichtigsten Kostenfaktoren aufgeführt:

Transaktionsvolumen
Dies ist die Menge der Transaktionen, die durchgeführt werden und beeinflusst die Skalierbarkeit einer Blockchain-Lösung.
In vielen Fällen fallen Blockketten unter 365.000 jährliche Transaktionsmarken (EY, 2019).

Transaktionsgröße
Die Transaktionsgröße bezieht sich auf den Speicherbedarf für eine im Netzwerk getätigte Werteinheit. Die Eingabe hängt von der Menge und Komplexität der für jede Transaktion benötigten Daten ab. Darüber hinaus wirken sich alle On-Chain- und Off-Chain-Datenspeicherprozeduren auf diese Kennzahl aus.

Zur Veranschaulichung: Anwendungen, die den Einsatz von Smart Contracts zur Ausführung von Vereinbarungen auf der Grundlage programmierbarer Bedingungen erfordern, vergrößern die Transaktionsgröße. Bei Anwendungen, wie beispielsweise Zahlungen oder der Übertragung von Wertpapieren, ist die Transaktionsgröße kleiner.

Knoten-Hosting-Verfahren
Dies bezieht sich auf das gewählte Verfahren zur Speicherung einer Blockchain-Plattform und alle damit verbundenen technologischen Zusatzanforderungen. Die drei gängigsten Stand-Alone-Methoden sind:

COMPETENCE CIRCLE **TECHNOLOGIE, INNOVATION & MANAGEMENT #CCTIM** DMV Whitepaper **Nr. 01 | Januar 2020**

(1) vor Ort, d.h. Investitionen in neue Systeme für die Blockchain,

(2) vor Ort, aber unter Verwendung vorhandener Technologien und Servers sowie

(3) cloud-basiert.

Wenn Hersteller A (Zulieferer) und Hersteller B (Werkzeugmaschinen) eine Konsortium Blockchain aufbauen wollen, haben sie höhere Knoten-Hosting-Verfahrenskosten als vielleicht ein „einfacher" Teilnehmer. Ein Beispiel hierfür ist das auf Blockchain-Technologie basierte Interbank Information Network (IIN, welches JPMorgan Chase, die australischen ANZ-Bank und die Royal Bank of Canada gegründet haben. Die restlichen über 200 Banken müssen sich an diesen Kosten beteiligen. Dies kann als Teil eines Fixums oder aber genau berechnete Fixanteile für die verursachten Transaktionskosten sein. Die bereitgestellte Infrastruktur muss von allen Teilnehmern bezahlt werden.

Konsensusprotokoll
Dies bezieht sich auf die Methode zur Überprüfung der Rechtmäßigkeit von Transaktionsblöcken. Es gibt vier Arten von Protokollen, die von öffentlichen und privaten Blockketten verwendet werden:

1. Nachweis der Arbeiten: Dies verbraucht eine große Menge an Rechenleistung, um Blöcke und Transaktionen abzubauen. Beispielsweise für Bitcoin heißt dies, der Stromverbrauch für eine Transaktion entspricht der gleichen täglichen Menge, die 20 US-Haushalte an einem Tag verbrauchen (de Vries, nicht datiert).
2. Nachweis der Beteiligung: Hier werden finanzielle Vermögenswerte verwendet, um Parteien zu motivieren, Blöcke mit Integrität zu bauen.
3. Autoritätsnachweis: Hier wird die Verantwortung für die Überprüfung von Blöcken auf bestimmte Teilnehmer verteilt.
4. Byzantinische Fehlertoleranz: Diese verwendet ein Abstimmungssystem, normalerweise innerhalb privater Blockketten, durch das der Konsens erreicht wird, sobald identische Antworten von vertrauenswürdigen Knoten empfangen werden.

Der Nachweis der Arbeit ist ein intensives Konsensusprotokoll (siehe Bitcoin). Daher sind die damit verbundenen Stromkosten und Hardwareausgaben höher sowie Zeiten für ausgeführte Transaktionen länger, als wenn beispielsweise der Nachweis der Autorität als Konsensusprotokoll verwendet wird (siehe Nr. 3 oben). Ein Beispiel ist Libra, wo die Partner die Verantwortung für die Überprüfung der Blöcke übernehmen.

Anhang 2: Wie läuft eine Transaktion in der Blockchain ab?

1. Definition einer Blockchain Transaktion
Der „Sender" erstellt eine Transaktion und überträgt sie an das Netzwerk. Die Transaktionsmeldung enthält Details über die öffentliche Adresse des Empfängers, den Wert der Transaktion und eine kryptografische digitale Signatur, die die Authentizität der Transaktion belegt.

2. Authentifizierung der Transaktion
Die Knoten (Computer/Benutzer) des Netzwerks empfangen die Nachricht und authentifizieren die Gültigkeit der Nachricht durch Entschlüsselung der digitalen Signatur. Die authentifizierte Transaktion wird in einen „Pool" von noch nicht erledigten Transaktionen gestellt.

3. Erschaffung des Blockes
Diese schwebenden oder noch nicht erledigten Geschäfte werden von einem der Knoten im Netzwerk in einer aktualisierten Version des Ledgers, dem sogenannten Block, zusammengefasst. In einem bestimmten Zeitintervall sendet der Knoten den Block zur Überprüfung an das Netzwerk.

4. Validierung vom Block
Die Prüferknoten des Netzwerks erhalten den vorgeschlagenen Block und arbeiten durch einen iterativen Prozess, der einen Konsens der Mehrheit des Netzwerks erfordert, ihn darin zu validieren. Verschiedene Blockchain-Netzwerke verwenden unterschiedliche Validierungstechniken. Bitcoin's Blockkette verwendet eine Technik namens „proof-of-work", Ripple verwendet „Distributed Consensus" und Ethereum verwendet einen „Proof-of-Stake". Die verschiedenen Techniken haben unterschiedliche Vor- und Nachteile. Der gemeinsame Nenner ist, dass sie sicherstellen, dass jede Transaktion gültig ist, und dass sie betrügerische Transaktionen unmöglich machen.

5. Blockverkettung
Wenn alle Transaktionen validiert sind, wird der neue Block in die Blockkette „eingekettet" und der neue aktuelle Zustand des Ledgers in das Netzwerk übertragen. Neben der guten Internetverbindung beeinflusst auch die Rechenkapazität der einzelnen Server, wie lange dieser Prozess dauert.
Dieser ganze Prozess - d.h. Ablauf einer Transaktion - sollte in der Regel in ca. 3 bis 10 Sekunden abgeschlossen sein.

Fazit

Wenn Alice ein Bitcoin an Urs verkauft, wird für diese Transaktion soviel Strom verbraucht, wie dies 20,87 US-amerikanische Haushalte im Schnitt pro Tag tun.
Ethereum schafft es, mit dem Tagesverbrauch von Strom von 0,94 US Haushalten, eine Transaktion abzuschließen.
Rund 24% vom totalen Energieverbrauch in einem Haushalt ist die Elektrizität, neben z.B. Erdgas oder Heizöl (Eurostat, nicht datiert).

Bei einem Firmenfahrzeug oder einem Industriebau wie einer Lagerhalle, werden die späteren Betriebskosten am Anfang in den Investitionsentscheid mit einbezogen. Dies hat auch bei einer Blockchain zu geschehen.

Headlines Anhänge und Fazit wie Glossar?
Fond durchziehen?

Im Inhaltsverzeichnis seperat mit aufnehmen - oder ab Referenzliste als „Anhang"?

Autor und Leiter des CoCi:
Professor Urs E. Gattiker Ph.D.
CyTRAP Labs GmbH

Autorin und Leiterin des CoCi:
Taina Temmen
Vorstand DMV
Content
& Social Media

" Es gibt einige wirklich gute Technologien in Bezug auf die gemeinsame Nutzung von Datenbanken und die Überprüfung von Transaktionen, die als Blockchain bezeichnet werden. Das ist eine gute Sache. Bitcoin und ICO sind eines der verrückteren spekulativen Dinge. Es handelt sich weder um eine Anlageklasse, noch produzieren sie etwas... "
– Bill Gates, Microsoft-Gründer (Mai 2018)

Kontakt DMV-Geschäftsstelle
Telefon: 0211.864 06-0
competence@marketingverband.de

Kontakt Competence Circle
Taina Temmen
temmen@marketingverband.de

Urs E. Gattiker
gattiker@marketingverband.de

Competence Circle

Die neun Competence Circle bilden eine inhaltliche Themen- und Kompetenz-Plattform für den DMV und sorgen mit ihrer Expertise u.a. durch die Erstellung der Whitepapers für einen Know-how Transfer auf allen Ebenen des Deutschen Marketing Verbands. Die einzelnen Gruppen stehen für folgende neun Themen:

1 **Bewegtbild**
2 **Customer Excellence**
3 **Data Driven Marketing & Decision Support Pricing**
4 **Employer Branding**
5 **Markenmanagement**
6 **Marketingplanung und -optimierung**
7 **Pricing & Market Strategy**
8 **Sponsoring**
9 **Technologie, Innovation & Management #ccTIM**

Impressum

Herausgeber
Deutscher Marketing Verband e.V. (DMV)
Sternstrasse 58, D-40479 Düsseldorf
Fon +49 (0) 211.864 06-0
info@marketingverband.de
marketingverband.de

Bildrechte: iStock, Adobe Stock

ISSN (Print) 2512-5842
ISSN (Online) 2512-5656