BLOCKCHAIN-REIFE

IM WINDSCHATTEN DER DIGITALISIERUNG.

Wieder einmal zeigt sich, dass die Technik dem Menschen oft einen Schritt voraus ist: Seit knapp zehn Jahren gibt es bereits die Blockchain-Technologie, aber erst in den letzten Jahren hat sie an Relevanz und Bekanntheit exponentiell zugenommen. Jetzt, zu einem Zeitpunkt, an dem es konkrete Anwendungsbereiche und Einsatzszenarien für die Blockchain gibt, kann sie ihre volle Kraft entfalten. Umso wichtiger ist es, dass jetzt auch die Verantwortlichen in den Führungsetagen der Unternehmen die Mehrwerte der Technologie und deren sinnvollen Einsatz erkennen.

Aber was macht die Blockchain so einzigartig? Aufgrund ihrer Vernetzung und des kryptographischen Speicherns von Datenblöcken erzeugt die Blockchain einerseits eine bisher nicht dagewesene Durchsichtigkeit und sorgt auf der anderen Seite für ein Maximum an Sicherheit. Die Blockchain-Technologie reduziert die Komplexität von Prozessen und erhöht die Transparenz und Unveränderbarkeit von Dokumenten. Dadurch bietet sie eine geradezu optimale Plattform für den direkten, transparenten und vertrauensvollen Datenaustausch zwischen Business- oder Projektpartnern.

Das kann die Blockchain

Das Besondere an der Blockchain ist ihre Struktur, mit der sie automatisch ein wesentlich höheres Sicherheitsniveau gewährleistet als andere Technologien – ein Vorteil, der im Zuge der zunehmenden Digitalisierung nicht hoch genug eingeschätzt werden kann.

Wie funktioniert das? Eine Blockchain ist im Grunde nichts anderes als ein verteiltes Register, in dem Daten, etwa statische Aufzeichnungen, dynamische Bewegungsdaten oder kritische personenbezogene Daten zunächst nach einem konsens-basierten Mechanismus überprüft werden. Erst danach werden die Daten zur Transaktion freigegeben. Dieser Vorgang basiert auf vier grundlegenden Eigenschaften.

1. Dezentrale Validierung

Neue Daten werden zunächst in Blöcke gepackt und erst dann einer Blockkette hinzugefügt, wenn ein Konsens über die Gültigkeit der Aktion erreicht ist.

2. Redundanz

Mehrere Blockchain-Nodes halten die Daten vor, so dass es keinen Single-Point-of-Failure gibt.

3. Unveränderliche Speicherung

Gespeicherte Daten werden durch eine Verkettung von Blöcken unveränderbar, dadurch entsteht vollständige Transparenz über die gesamte Transaktion.

4. Verschlüsselung

Digitale Signaturen, die auf kryptografischen Schlüsseln basieren, versetzen die Netzwerkteilnehmer in die Lage, zu authentifizieren, welcher Teilnehmer eine Transaktion initiiert, ein Asset besitzt, einen Smart Contract (Vertrag auf Software-Basis) bereitstellt oder Daten in die Blockchain geschrieben hat.

Aufgrund der maximal dezentralen Peer-to-Peer-Struktur bietet die Blockchain-Technologie Sicherheit, verbesserte Netzwerkflexibilität und reduzierte Transaktionskosten. Besonders aber ist, dass die Blockchain die Abhängigkeit von Vermittlern zwischen den Strukturen reduziert. Das ist zugleich auch das Revolutionäre an dieser Technologie und ihr Mehrwert für ihren Einsatz im Digitalisierungszeitalter. So stellt sie unter anderem das etablierte Prinzip von Web-Konzepten auf den Kopf: Bisher waren und sind die Protokollregeln bei Web-Modellen bewusst einfach gehalten, damit Anwendungsentwickler die Möglichkeit haben, diese Regeln entsprechend einzurichten. Im Blockchain-Modell dagegen sind die Regeln direkt im Protokoll eingebaut, so dass die Daten unveränderbar sind. Gleichzeitig sind diese Protokolle für alle transparent und nutzbar.

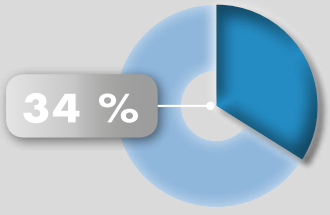
Nachholbedarf in Sachen Blockchain

Doch trotz dieses Potenzials steckt die Blockchain in Deutschland noch in den Kinderschuhen. Zwar nehmen ihre Nutzung und Akzeptanz nach und nach zu, aber noch ist der Einsatz der Blockchain in Deutschland überschaubar. Das zeigt nicht zuletzt eine Studie der Bitkom, die diese 2019 durchgeführt hat. Demnach

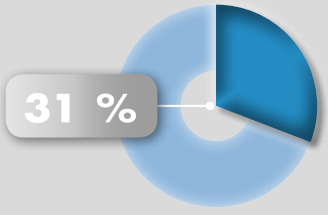
BLOCKCHAIN IM FACTORING

Die Fakturierung ist ein beispielhafter Bereich für die Mehrwerte der Blockchain. Beim Factoring verkauft ein Unternehmen seine Forderungen aus Lieferungen und Leistungen an ein Factoringinstitut und erhält damit sofort Liquidität. Der Austausch von Daten und das Vertrauen zwischen den beteiligten Parteien ist von großer Bedeutung. Erfolgt der gesamte Datenaustausch über die Blockchain innerhalb eines Ökosystems über die verteilte Ledger-Technologie, wird Vertrauen gebildet. Wichtig ist, bei der Fakturierung zwischen einer öffentlichen und einer privaten Blockchain zu unterscheiden, denn die Regulierungsbehörden, die einerseits private Blockchains einsetzen, hindern andererseits andere Parteien daran teilzunehmen – sie gestatten nur bestimmte Transaktionen. Empfehlenswert sind deshalb Rechnungsregister, die auf Basis einer Public Blockchain mit darin gespeicherten Hash-Tools, funktionieren.

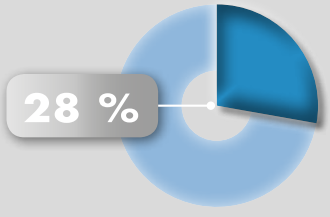
ZIELE DES BLOCKCHAIN-EINSATZES.



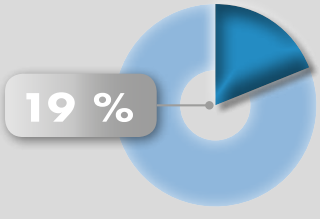
Blockchain ist für unser Unternehmen eine Technologie, die Sicherheit in unternehmensübergreifende Prozesse bringt.



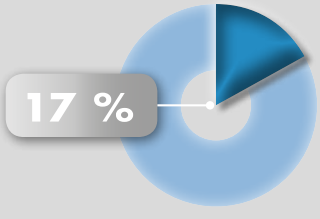
Blockchain ist für unser Unternehmen eine Technologie zur Effizienzsteigerung.



Mithilfe der Blockchain-Technologie können wir die Informationssicherheit verbessern.



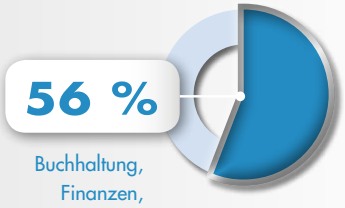
Mithilfe der Blockchain-Technologie können wir Transaktionskosten minimieren.



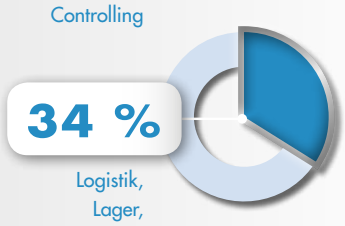
Blockchain ist in unserem Unternehmen für Prozesse wichtig, in denen es um die Zusammenarbeit mit Organisationen geht und das Vertrauen fehlt.

Quelle: Bitkom Research 2018

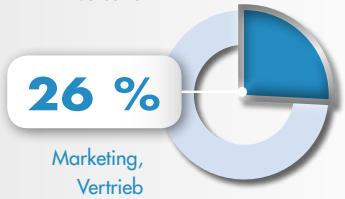
BLOCKCHAIN-EINSATZ NACH UNTERNEHMENSBEREICHEN.



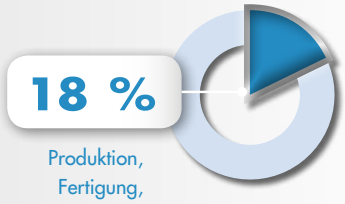
Buchhaltung, Finanzen, Controlling



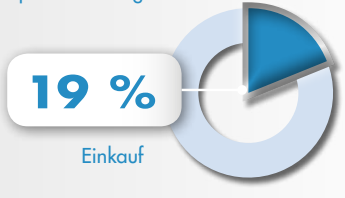
Logistik, Lager, Versand



Marketing, Vertrieb

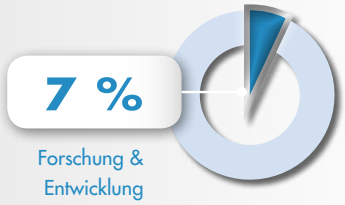


Produktion, Fertigung, Projektabwicklung



Einkauf

Human Resources



Forschung & Entwicklung

Quelle: Bitkom Research 2018

gibt jedes zehnte befragte Unternehmen an, dass die deutsche Wirtschaft verglichen mit anderen Ländern bei der Blockchain derzeit abgeschlagen sei. Etwa jedes zweite Unternehmen ordnet Deutschland sogar als Nachzügler ein. Etwa 40 Prozent sehen Deutschland im Mittelfeld. Signifikant aber ist, dass keines der befragten Unternehmen Deutschland als führend empfindet oder gar der Spitzengruppe zuordnen würde.

> AUFGRUND DER MAXIMAL DEZENTRALEN PEER-TO-PEER-STRUKTUR BIETET DIE BLOCKCHAIN-TECHNOLOGIE SICHERHEIT, VERBESSERTE NETZWERKFLEXIBILITÄT UND REDUZIERTE TRANSAKTIONSKOSTEN. BESONDERS ABER IST, DASS DIE BLOCKCHAIN DIE ABHÄNGIGKEIT VON VERMITTLERN ZWISCHEN DEN STRUKTUREN REDUZIERT."
>
> Lumir Boureanu, CEO, compacer GmbH, www.compacer.com

Spannend ist diese Momentaufnahme vor allem vor dem Hintergrund, dass die Bitkom-Studie auch noch ganz andere Einschätzungen einfangen konnte. Demnach sehen die Unternehmen in der Blockchain-Technologie ein ebenso enormes Potenzial wie in der künstlichen Intelligenz (KI) und dem Internet of Things (IoT). 15 Prozent aller von der Bitkom befragten Unternehmen gehen sogar davon aus, dass Blockchain die Gesellschaft und Wirtschaft genauso stark verändern wird, wie ehemals das Internet. Bei Unternehmen mit mehr als 500 Mitarbeitern teilen sogar 36 Prozent der IT-Spezialisten diese Einschätzung.

Kryptowährungen – Blockchain Best Practice

Gleichzeitig wird immer klarer, dass sich diese Technologie nicht für einen massenhaften Einsatz eignet, in speziellen Wirtschaftsbereichen aber unschlagbare Vorteile hat – beispielsweise bei Kryptowährungen. Auch wenn die Kryptowährungen sehr gehypt wurden und die Erwartungen überzogen waren, so ist dieser inzwischen abklingende Hype-Zyklus doch sehr typisch für neue Technologien und deren Markteinführung. Für die Glaubwürdigkeit und den Nutzen der Blockchain-Technologie hat dies jedoch keine negativen Folgen. Im Gegenteil.

Die unveränderliche Datenbankstruktur, welche Transaktionen mit einem oder mehreren Parteien vereinfacht und gleichzeitig sicherer gestaltet, macht die Blockchain einzigartig. Durch das Dezentralisierungskonzept entsteht eine sichere Plattform, die automatisch das Vertrauen aller beteiligten Parteien genießt. Basierend auf diesem Prinzip, lassen sich revolutionäre neue Anwendungen entwickeln, die unser Zusammenleben nachhaltig prägen werden – die Kryptowährungen sind nur der Anfang.

Ausblick

Doch unabhängig von diesen Ergebnissen lässt sich grundsätzlich festhalten, dass die Blockchain-Technologie mittlerweile in der Wirklichkeit angekommen ist. Problematisch bleibt aber, dass der Proof-of-Work basierende Konsensmechanismus der Blockchain-Technologie einen hohen Energieaufwand mit sich bringt und der Rechenzentrumsbedarf enorm ist. Insbesondere vor dem Hintergrund, dass die Arbeit von Kryptominern sehr energieaufwendig ist, sollten sich Unternehmen, die auf Blockchain setzen, der Folgen für den Klimawandel bewusst sein. Deshalb ist es wichtig, diese Kontroverse nicht unter den Tisch zu kehren, sondern sie als Ansporn für die Weiterentwicklung der Technologie zu sehen und hier weiterhin Innovationen voranzutreiben. Dann öffnet uns die Blockchain-Technologie Zukunftsoptionen, von denen heute noch niemand etwas ahnt.

Lumir Boureanu

ADVANCED MALWARE

HARTNÄCKIGE SCHÄDLINGE.

Advanced Malware, auch als Advanced Persistent Threats (APT) bezeichnet, sind Malware-Stämme, die mit erweiterten Funktionen für die Infektion, Kommunikation, Steuerung, Bewegung im Netzwerk oder Datenexfiltration- und Payload-Exekution ausgestattet sind. Dabei ist die Schadware darauf auslegt, möglichst unentdeckt und hartnäckig zu sein, und entgeht der Erkennung durch herkömmliche Antivirenlösungen. Aufgrund der ausgeklügelten Angriffsmöglichkeiten und der Geschwindigkeit, mit der Cyberkriminelle immer neue Malware-Versionen entwickeln, sind in den letzten Jahren die APT-Attacken deutlich gestiegen.

Das Vorgehen der Cyberkriminellen

Advanced Malware-Angriffe folgen in der Regel einer gemeinsamen Angriffsabfolge:

1. **Planung:** In dieser Phase wählen Cyberkriminelle ein Ziel aus und untersuchen dessen Infrastruktur, um festzustellen, wie die Malware eingeführt wird, welche Kommunikationsmethoden während des Angriffs verwendet und wie und wo Daten extrahiert werden sollen.

2. **Malware-Einführung:** In diesem Stadium wird Malware zur Erstinfektion an die Opfer abgegeben. Dies geschieht häufig über Spear-Phishing-E-Mails mit infizierten Anhängen oder über Drive-by-Angriffe durch eine verseuchte Website.

3. **Command and Control:** Advanced Malware kommuniziert mit dem Angreifer, um ihm erkannte Informationen zu senden und zusätzliche Befehle von ihm zu erhalten. Die Schadware sendet Benutzer-, Netzwerk- und Maschineninformationen an den Hacker und erhält von ihm neue Anweisungen, welche Identitäten oder Maschinen als nächstes infiziert werden sollen, wie man die Ziele identifiziert sowie Anweisungen zur Datenexfiltration.

4. **Ausweitung der Infizierung:** Advanced Malware verfügt oft über robuste Selbstvermehrungsfunktionen, um Ziele schnell zu identifizieren und zu infizieren. Angreifer werden solange wie möglich das Netzwerk erforschen und Malware verbreiten, bis sie diejenigen Computer oder Systeme infizieren, die Zugriff auf wertvolle Daten haben.

5. **Zielerkennung:** Sobald der Angreifer Fuß gefasst und das Netzwerk erkundet hat, werden die Ziele für die Endphase der Malware-Ausbreitung identifiziert. In diesem Stadium wird die Malware auf Computer oder Systeme verbreitet, die die gewünschten Daten enthalten.

6. **Exfiltration:** Nun wird die Malware-Payload ausgeführt. Bei einem Angriff, der sich auf Datendiebstahl konzentriert, ist dies die Phase, in der gezielte Daten gesammelt und an einen vom Angreifer kontrollierten Ort übertragen werden. Advanced Malware verwendet Verschleierungstechniken, um diese Exfiltration zu verbergen.

Rückzug: Nachdem ein Advanced Malware-Angriff abgeschlossen ist, zieht sich die Malware oft zurück und versteckt

7. sich in einem Computernetzwerk oder zerstört sich selbst, je nach Zielorganisation und der Wahrscheinlichkeit einer Entdeckung durch Sicherheitssysteme.

Um sensible Daten zu schützen, benötigen Unternehmen deshalb einen mehrschichten Security-Ansatz aus Mitarbeitertrainings und Technologien. Advanced Threat Detection-Tools sowie Sicherheitslösungen, die Data Loss Prevention (DLP), Endpoint Detection and Response (EDR) und die Überwachung von Anomalien im Nutzer- und Entitätsverhalten auf Basis von Machine Learning gewährleisten, können das Risiko von Datenexfiltration und Spionage durch Advanced Malware-Angriffe erheblich reduzieren.

https://digitalguardian.com