# Blockchain: Potenzial und Gefahr zugleich

*Derzeit braucht man nur das Buzzword Blockchain in einer Runde fallen zu lassen, um die volle Aufmerksamkeit zu bekommen. Doch was hat es mit dieser Technologie auf sich? Nur ein Hype? Oder – wie mehrfach prophezeit – der Beginn eines neuen Finanzzeitalters? Um beim Small Talk mit Expertenwissen zu punkten, gibt Sophos einen kompakten Über- und Ausblick über Funktion und Potenzial von Blockchain.*

**Wiesbaden, 07. April 2017.** Die Blockchain-Technologie ist auf dem Vormarsch. Acht Jahre nach dem Aufkommen der Original Bitcoin Blockchain, gibt es viele Bemühungen, mit den Sicherheitsvorteilen der Technologie in zahlreiche Industriezweige vorzustoßen. Doch welche Vorteile bringt diese den Usern, wie den Unternehmen? Und welche neuen Herausforderungen ergeben sich dadurch? Stichwort: Security Next Generation.

Zunächst einmal: Eine Blockchain lässt sich als Datenbank verstehen, welche die technische Grundlage für eine Kryptowährung bereithält. Bekanntestes Beispiel einer Blockchain ist das Zahlungsmittel Bitcoin.

**Vorteil 1: Direkte Transaktion ohne Mittelsmann**
Der größte Vorteil besteht in der direkten Transaktion von Parteien. Es gibt keinen Dritten im Bunde, der wie ein Schiedsrichter, zum Beispiel eine Bank, oder Treuhänder, wie der Bezahldienst Paypal, die Verlässlichkeit der Akteure prüft.
Doch warum sollte man das bewährte Treuhänder-Modell umgehen wollen? Der Mittelsmann nimmt einem ja gerade die Arbeit ab, das Gegenüber auf Herz und Niere zu prüfen. Aber: Kann man denn dem Schiedsrichter trauen? Auch große Banken sind vor Manipulationen nicht sicher, wie zahlreiche Berichte in der Vergangenheit gezeigt haben.

**Vorteil 2: Nachträgliche Änderungen ausgeschlossen**
Die Parteien können ihren Deal selbst regeln und versiegeln, so dass die Transaktion zwar sicht- aber unveränderbar bleibt. Dieses Prinzip fordert quasi ehrliches Verhalten der Akteure ein.
Das „Einfrieren“ der Transaktionen erfordert eine andere Technologie als bisher: Bitcoin zum Beispiel hält die Rechenkapazität einer Kleinstadt vor, um seine Transaktionen in digitalem Herz zu verwahren. Andere Technologien nutzen einen Proof-of-stake-Algorithmus. Jedes Prinzip hat seine eigenen technischen und ökonomischen Konsequenzen. Kein Wunder also, dass gerade im Hinblick auf den Sicherheitsaspekt viel mit der Blockchain Technologie experimentiert wird. Dänische und australische Parteien hoffen auf eine Nutzung bei Online-Wahlen. Es gibt Angebote zur notariellen Beurkundung von Dokumenten und sogar die Überlegung, Krankenakten via Blockchain Technologie zu sichern.

**Problem 1: Blockwashing**
Eine der größten Herausforderungen im Umgang mit der Blockchain Technologie wird blockwashing sein: entwickelt sich eine vielversprechende Technologie, soll diese als Heilsbringer in den unterschiedlichsten Bereichen fungieren. Die Hals-über-Kopf-Methode, um aus der neuen Technologie Kapital zu schlagen, befeuert die frühe Kurve des Gartner Hpye-Zyklus‘ (http://www.gartner.com/newsroom/id/3412017). Diese führt aber auch zu einem unausweichlichen Zusammenbruch, wenn die Technologie den Erwartungen nicht gerecht wird – wie bereits gemutmaßt wird. Galt Dezentralisierung als wichtige Charakteristik der original Blockchain, muss man sich fragen, was der Einzug der Technologie in Cloud-Strukturen (u.a. bei Microsoft und IBM) für die Sicherheitsleistung bedeuten wird. Zwar ist alles kryptografisch gesichert, aber betrieben wiederum von einer einzigen Partei. Der

ursprüngliche Charakter der Blockchain wird damit ausgehöhlt. Mehr noch: Microsofts Marketing spielt bereits mit dem unvermeidlichem Spitznamen „Blockchain as a Service“ und negiert damit offen die gesamte Idee des dezentralen und unabhängigen Netzwerks.

**Problem 2: Fehlende Standardisierung**
Mit dem Thema Standardisierung wird man sich ebenfalls in Zukunft auseinandersetzen müssen. Es gibt zahlreiche Vorschläge und Lösungsansätze für die Blockchain Technologie. Jede mit ihren Vor- und Nachteilen. Zusammenarbeit kann hier nur die richtige Vorgehensweise sein, um allgemein gültige Standards zu definieren. Die Internationale Organisation für Normung (ISO) hat bereits ein Komitee gebildet, das erste Bemühungen in diese Richtung prüft.

**Problem 3: Gute Konzepte, schlechter Code**
Eine weiteres kritisches Thema dreht sich um die Sicherheit. Denn nur weil das Blockchain-Konzept Security bietet, bedeutet das noch lange nicht, dass auch die Implementierungen sicher ist. China beispielsweise – interessiert an einer eigenen Kryptowährung – analysierte kürzlich 25 der Top Blockchain-bezogenen Software Projekte und fand signifikante Sicherheits-Schwachstellen: Stichwort Input Validation.

**Fazit: Erst sicherer programmieren, dann nutzen**
Die hier dargestellten Probleme sind nicht nur theoretisch. Vielmehr stehen sie den Zielen vieler Blockchain-Projekte diametral entgegen. Bugs in Blockchain Implementierungen sind ernst zu nehmen und führen zu massiven Sicherheitslücken und finanziellen Verlusten, wie der Diebstahl von Zcoins im Wert von 400.000 US Dollar letzten Monat veranschaulicht.
Mit der Weiterentwicklung von Blockchain Software vergrößern sich auch deren Angriffsflächen. Ein Schlüsselfaktor werden hier klug ausgetüftelte Verträge sein. Während die Orginal Bitcoin Blockchain nur Protokolle der digitalen Transaktionen bereithält, könnten neuere Abkommen in Wirklichkeit Programme sein, die auf der Blockchain laufen: Man stelle sich einen legalen Vertrag vor, der durch ein Computerprogramm ersetzt wird. Statt einen Anwalt zu bezahlen, der den Vertrag regelt, könnten alle teilnehmenden Parteien das selbstständig organisieren. Die Blockchain sorgt für unveränderbaren und transparenten Programm Output. Das Programm selbst analysiert die externen Bedingungen und führt seine Klauseln ordnungsgemäß aus. Dennoch: Computer-Programme werden immer Schwachstellen haben. Insofern kann die Lösung für eine sichere Blockchain-Technologie nur darin liegen, unter Berücksichtigung von Sicherheitskonzepten zu programmieren und so zum Beispiel die Schwachstellen bei Input und Output Validierung zu korrigieren. Und zwar bevor man diese Technologie weiten Teilen der Wirtschaft anvertraut oder sie ausgiebig dafür nutzt, um beispielsweise das Internet der Dinge zu organisieren.
Blockchain hält seine Versprechen. Aber es sollte Gartners Hype-Zyklus durchlaufen bevor es zum Hauptthema in der Sicherheitsindustrie wird. Und wir werden unsere Code-Praxis mit Hilfe von Security-Audits und Code-Scans ebenfalls überdenken müssen. Die Blockchain ist heute das, was das Internet 1994 war. Zwei Jahrzehnte später ist das Web wie der Justin Bieber der Technologie: unlängst erwachsen geworden, wahnsinnig erfolgreich, aber auch faul und angeschlagen durch den etwas außer Kontrolle geratenen Siegeszug. Es ist ein schöner aber verrückter Ort, im Stich gelassen durch einen Mix aus fragwürdigem Javascript und steil ansteigender Cyberkriminalität. Beherrscht von Monolithen, welche die Privatsphäre ihrer Nutzer zum Frühstück verspeisen. Zugegeben, etwas pessimistisch, aber wäre es nicht sinnvoll, aus den Fehlern der Vergangenheit zu lernen während wir uns mit Blockchain beschäftigen?

Sophos Naked Security http://bit.ly/2ml8jKN

**Über Sophos**
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

**Pressekontakt:**

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de