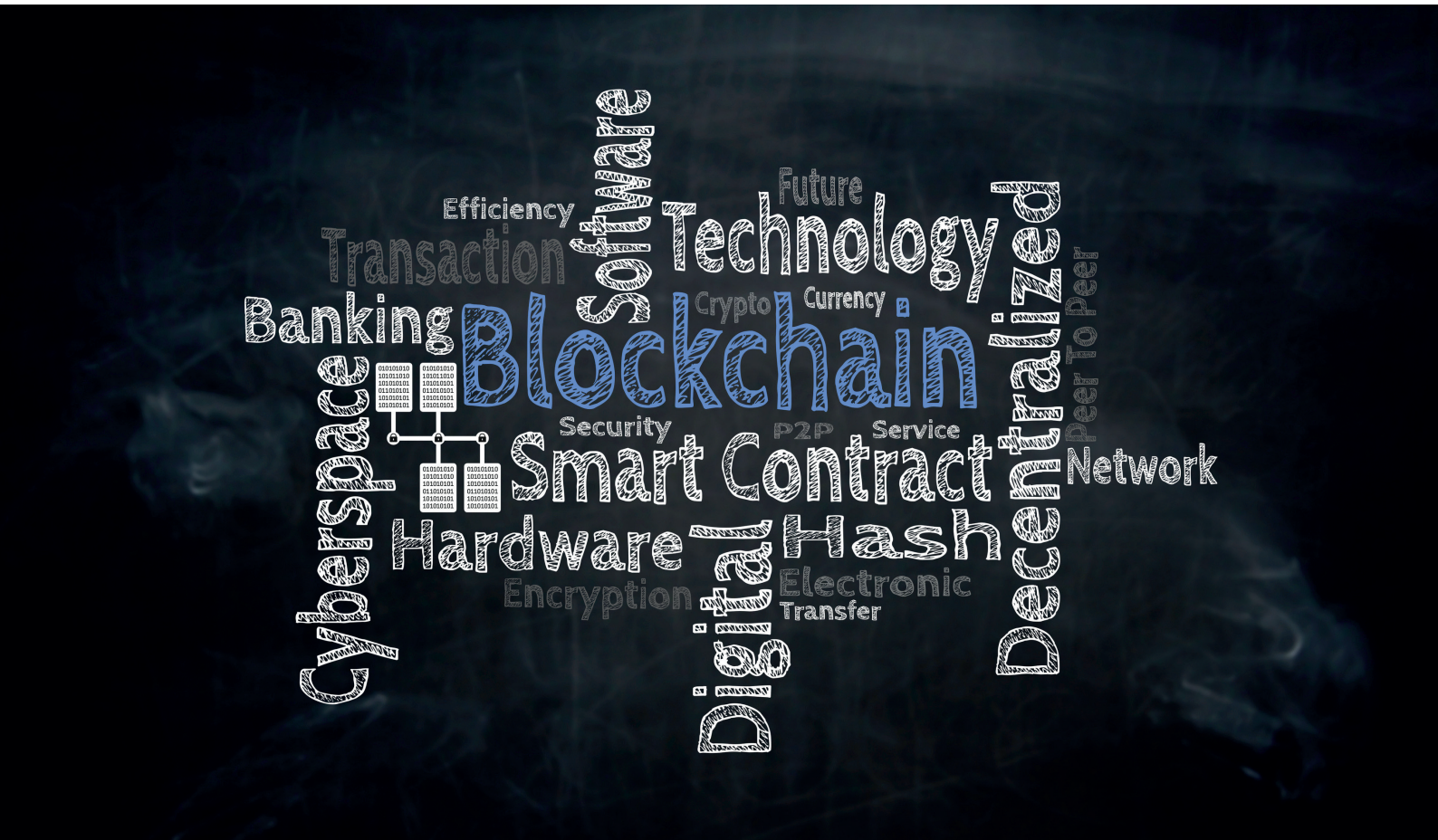
BLOCKCHAIN – mehr als eine Technologie für Kryptowährung

10 Jahre ist es her, dass ein unbekannter Autor unter dem Pseudonym Satoshi Nakamoto ein Paper veröffentlichte, in dem er eine Alternative zum Fiat-Währungssystem[1] beschrieb. Grundbaustein: die damals noch wenig bekannte Blockchain-Technologie. Gerade einmal ein Jahr später begann der kometenhafte Aufstieg dieser „Kryptowährung“: Der Bitcoin hangelt sich von einem Superlativ zum nächsten, inzwischen liegt die Marktkapitalisierung bei deutlich über 200 Mrd. US-Dollar. Doch das Fachpublikum hat längst bemerkt, dass der Bitcoin nur ein erster technischer Durchstich für etwas viel Größeres ist. Über 1000 verschiedene Kryptowährungen verzeichnet die Webseite coinmarketcap.com. Aber auch über die Anwendung als Währung hinaus tun sich enorme Potenziale auf und die Anzahl an wissenschaftlichen Veröffentlichungen nimmt jeden Monat zu. Gleichzeitig häufen sich die Vorbehalte, ob die Technologie halten kann, was diverse Berater und Start-ups versprechen; immer wieder wird die Technologie als Energiefresser verschrien. Und tatsächlich verbraucht das Bitcoin-Netz aktuell mehr Strom als beispielsweise ganz Irland.



An dieser Stelle wird schon ein grundsätzliches Problem deutlich: die mangelnde Differenzierung zwischen der Technologie (Blockchain) und der unbestreitbar führenden Anwendung derselben (Bitcoin). Was genau die Technologie auszeichnet und wann eine Anwendung noch als Blockchain-Applikation bezeichnet werden kann, ist in Zeiten von Tangle[2], Swirlds Hashgraph[3] und zentral gespeicherten Blockchains kaum noch zu beantworten. Forscher bemühen sich um Konsolidierung, doch die technische Entwicklung ist schneller.

Wir versuchen, einen kurzen Überblick zu geben, was nach allgemeinem Konsens (soweit man in diesem Feld davon sprechen darf) Eigenschaften einer Blockchain sind, und was das technisch bedeutet:

- **Eine Blockchain ist eine redundant und dezentral gespeicherte Datenbank.** Der vollständige Datenbestand der Blockchain liegt jedem Mitglied des betreibenden Netzwerkes vor. Bei besonders offenen Blockchain-Applikationen (wie beim Bitcoin) ist der Datenstand öffentlich für jeden einsehbar; er kann sogar kopiert und lokal gespeichert werden. Jeder Mensch mit Zugang zu einem Computer und dem Internet kann Teil des Netzwerks werden und dabei helfen, die Datenbank aufrechtzuerhalten, indem er sie mitverwaltet. Das bedeutet aber nicht, dass auch jeder sehen kann, wel-

[1]Der Begriff „Fiatgeld" oder „Fiatwährung" bezeichnet ein Zahlungsmittel, welches (von einer Regierung oder einem Staat) „künstlich erschaffe"» worden ist und keinen inneren Wert hat. Fiatgeld unterscheidet sich damit vom Warengeld (zum Beispiel Salz, Reis, Gold oder Silber), das zusätzlich zu seinem Tauschwert immer auch einen inneren Wert (in Form der Ware selber) hat. Manche Autoren bezeichnen mit dem Begriff „Fiatgeld" allgemein Zahlungsmittel, die nicht durch Gold gedeckt sind. (Quelle: https://www.moneyland.ch/de/fiatgeld-definition, zuletzt geprüft: 29.03.2018)

[2]Tangle ist eine von der verbreiteten Blockchain-Datenstruktur mit Blockketten abweichende Daten- und Validierungsanordnung. (Quelle: Popov, S.: The Tangle. https://iota.org/IOTA_Whitepaper.pdf, zuletzt geprüft: 29.03.2018)

[3]Der Swirld-Hashgraph-Konsensmechanismus ist eine alternative Form der Transaktionsvalidierung, bei der die Netzknoten nicht nach festen Blockintervallen eine vollständige Datensynchronität erreichen müssen. (Quelle: Baird, L.: The Swirlds Hashgraph Consensus Algorithm: Fair, fast, byzantine fault tolerance. https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf, zuletzt geprüft: 29.03.2018)

che Informationen die Rohdaten genau beinhalten. Durch die Verschlüsselung (Public-/Private-Key-Encryption) kann nur derjenige bestimmte Informationen sehen, der einen privaten Schlüssel zu der Adresse (öffentlicher Schlüssel) hat, auf welcher die jeweilige Information gespeichert wurde. Welche Teile der Daten verschlüsselt und welche offen sind, hängt auch hier von der Ausgestaltung der jeweiligen Applikation ab. Ein Problem dieser vollständigen Speicherung bei verschiedenen Teilnehmern wird sofort klar: Eine solche Speicherung ist bezüglich der Speichernutzung alles andere als effizient. Für Anwendungen wie den Bitcoin macht das wenig aus – alle mittlerweile über 290.000.000 Bitcoin-Transaktionen führen zu einer Gesamtgröße der Blockchain von gerade mal 150 GB (ungefährer Wert). Für speicherplatzintensive Anwendungen stellt dies aber natürlich ein Problem dar. Doch abweichend von der bis hierhin dargestellten Funktionsweise gibt es hierfür bereits Ansätze, Blockchains nur oder teilweise auf zentralen Servern zu speichern und nur die Prüfsummen im Netzwerk zu verteilen.

- **Blockchains sind transaktionsbasiert und die Transaktionen werden in Blöcken gespeichert.** Zumindest das ist eine Aussage, von der bisher kaum abgewichen wird. In Blockchains werden Daten nicht geändert, sondern nur hinzugefügt. Soll in einer Blockchain also eine Information über einen neuen Zustand gespeichert werden, wird die Änderung zum vorherigen Zustand aufgenommen. Bei Besitzverhältnissen ist dies denkbar einfach: Eine Übergabe von einem Besitzer an einen anderen nennt man Transaktion. Die Transaktionen wiederum werden zu Blöcken zusammengefasst. Dabei wird über alle Transaktionen, die zu einem Block gehören, eine „Prüfsumme" (auch „Hashwert") gebildet und im sogenannten „Blockkopf" (auch „Blockheader") gespeichert. Die kleinste Änderung einer Transaktion führt zu einer Änderung der zugehörigen Prüfsumme. Im Blockkopf werden zusätzlich einige andere blockchainspezifische Daten gespeichert, etwa die Nummer des Blocks oder die Uhrzeit der Entstehung desselben. Auf jeden Fall wird aber die Prüfsumme des Blockkopfs des vorangegangenen Blocks gespeichert. Dies führt dazu, dass, sollte irgendeine Transaktion in irgendeinem Block geändert werden, alle Blockköpfe ab diesem Block verändert werden. Es reicht also, wenn die Netzknoten die Prüfsumme des Blockkopfs ihres letzten Blocks abgleichen. Solange diese gleich sind, sind auch alle Daten gleich. Zeigt jedoch ein Netzknoten eine andere Prüfsumme, so sind die Daten an diesem Standort möglicherweise manipuliert. Die Fälschungssicherheit ist somit trotz Dezentralität gegeben.

- **Zur Prüfung vor der Aufnahme der Transaktionen wird ein gemeinsames Regelwerk vorgehalten.** Auch hier gilt: Für Kryptowährungen ist das recht einfach. Eine Transaktion ist nur dann gültig, wenn der Überweisende über Coins verfügen kann. Das Regelwerk muss dabei von den Netzknoten eingehalten werden – eine Abweichung würde zu einem anderen Datenstand führen, und der Datenstand des Netzknotens würde aufgrund seiner abweichenden Prüfsumme abgelehnt werden. Das Regelwerk dient also nicht nur der Vermeidung von nicht zulässigen, womöglich betrügerischen Transaktionen, sondern auch schlicht der Organisation der Daten. In anderen Anwendungsbereichen der Blockchain-Technologie sind wesentlich kompliziertere Regelwerke denkbar – soll etwa eine Lieferkette in einer Blockchain transparent gemacht werden, müsste das Regelwerk mit konvergenten und divergenten Materialflüssen umgehen können.

- **Konsensalgorithmen zur Prüfung der Transaktionen machen Demokratie im anonymen Internet möglich.** Es bleibt die Frage, wie sichergestellt wird, dass niemand sehr viele Accounts anlegt und dann das Regelwerk zu seinen Gunsten umgeht oder sich schlicht mit falschen Transaktionen selbst bereichert – und dafür mit seinen vielen Accounts die Zustimmung der Mehrheit des Netzwerks vorgibt (sogenannte Sybil-Attacke). Dagegen wurde beim Bitcoin der Konsensmechanismus „Proof-of-Work" eingeführt, welcher von bekannten Silicon-Valley-Entrepreneuren durchaus auch mal als „größte Erfindung seit dem Internet" (Marc Andreesen, Gründer u. a. von Netscape) bezeichnet oder auf eine Stufe mit der Erfindung von Dampfmaschine oder Verbrennungsmotor (Johann Palychata, BNP Paribas) gestellt wird. Die genaue Erklärung des Proof-of-Works würde hier den Rahmen sprengen, aber vereinfacht könnte man sagen: Durch diesen Konsensalgorithmus hat nicht jeder Beteiligte eine Stimme, sondern die Anzahl an Stimmen bemisst sich an der Rechenleistung, die er zur Verfügung stellt. Nur wenn es jemand schaffen würde, über 50 Prozent der Rechenleistung in einem solchen Netz zu erlangen, könnte er seine falschen Informationen glaubhaft machen (die Länge seiner kompromittierten Blockchain würde die Länge der korrekten Blockchain überholen). Ist das Netz jedoch groß genug, darf das ausgeschlossen werden. Für die Zurverfügungstellung der Rechenpower werden die sogenannten „Miner" mit Bitcoins belohnt. Dieser Konsensmechanismus allein ist der Grund, warum das Bitcoin-Netz so unglaublich viel Energie verschlingt. Weitere Konsensalgorithmen richten sich nach anderen Kriterien in der Gewichtung der Stimmen, zum Beispiel dem Anteil der gehaltenen Coins einer Währung („Proof-of-Stake"). So oder so gilt: Haben die Beteiligten keinen Grund, anonym sein zu müssen, ist auch kein energieintensiver Konsensalgorithmus notwendig – wie zum Beispiel bei einer Konsortialblockchain.

Vereinfacht gesagt:
Blockchains können überall dort sinnvoll sein, wo Daten hochverfügbar und fälschungssicher geteilt werden sollen, ohne dass zwischen den Parteien Vertrauen besteht und ohne dass ein vertrauensgebender Intermediär eingeschaltet werden soll.

Unter dem Leitsatz findet sich auch gleich die Antwort auf die Frage, warum der Bitcoin so einen Erfolg feiert: Es bestand und besteht offensichtlich ein Interesse an einer Möglichkeit, ohne Banken Geld auszutauschen.

Die spannende Frage, die sich anschließt: Wo gibt es weitere Anwendungsgebiete?
Für Verträge könnte die Blockchain klassische Notare ablösen. Patente könnten in einer Blockchain statt beim Patentamt angemeldet werden. Echtheitszertifikate könnten in eine Blockchain geschrieben werden, anstatt unter großem Aufwand für Fälschungssicherheit auf Papier.

Auch in der Logistik gibt es einige Anwendungsgebiete, die direkt vor uns liegen:
Mithilfe von Smart Contracts könnten Handelsvorgänge automatisiert werden – die Vertragsbedingungen und wichtige Dokumente (Rechnungen, Zustellbenachrichtigungen) können unfälschbar hinterlegt und automatisch hinsichtlich ihrer Konsequenzen (bspw. Bezahlung) verarbeitet werden. Die vollständige Historie eines Produkts kann nachvollziehbar gemacht werden, ohne dass eine Plattform „mitverdienen" möchte bzw. die Daten aus der Hand gegeben werden. Gerade in Zeiten, in denen für Endkunden verantwortungsbewusster Konsum immer wichtiger wird (Stichwort: Kobalt aus Kinderarbeit in E-Autos) und Lebensmittelskandale den Einzelhandel erschüttern (Stichwort: Skandal um mit Fipronil verseuchte Eier) ergibt sich ein wichtiger

Wettbewerbsvorteil. Bei einer End-to-End-transparenten Supply-Chain können problematische Produkte zielgerichtet identifiziert und zurückgerufen werden. Blockchain könnte hier zur Enablertechnologie werden, denn Plattformlösungen setzen sich mangels Akzeptanz kaum durch.

Wir hoffen, Ihnen damit einen kleinen Einblick in die Technologie gegeben zu haben. Wenn Sie das FIR schon länger begleiten, ahnen Sie sicher, wie und auf welche Weise wir uns aktuell in dem Thema positionieren.

Wir bearbeiten aktuell gleich mehrere Projekte, in denen wir:

- in einer Konsortialstudie unter der Leitung der KEX AG mit Industriepartnern zum Thema „Blockchain for Industrial Applications" Anwendungspotenziale der Blockchaintechnologie für Industrie-Unternehmen ableiten, konkret bewerten und Umsetzungswege aufzeigen,
- die Blockchaintechnologie mit anderen Technologien vergleichen im Versuch, betriebliche Anwendungssysteme zu vernetzen (Forschungsprojekt ‚myOpenSupplyChain'),
- ein Blockchain-Ökosystem für heterogene Industrie-4.0-Werkzeugmaschinen aufbauen (geplantes Forschungsprojekt BÖkos 4.0),
- in einem Konsortialprojekt unter Leitung des Centers Connected Industry eine Applikation zur Dokumentation der Produktion des e.GO Life, des Aachener Elektroautos der e.GO Mobile AG, gestalten,
- unsere Innovation-Labs mit einem Blockchain-Demonstrator ausstatten,
- Schnittstellen zwischen ERP-Systemen und Blockchains konzeptionieren, (Forschungsprojekt ‚ABChain'),
- Zulieferer durch Smart Contracts anbinden (Forschungsprojekt ‚BAPISCO'),
- eine Blockchain-Applikation für die Lebensmittelindustrie ausarbeiten (Forschungsprojekt ‚SafeFoodChain'),
- eine Umfrage bzgl. Akzeptanz und zukünftiger Einschätzung der Blockchain-Technologie für den deutschen Maschinenbau durchführen.

Mehr über unsere Blockchain-Aktivitäten finden Sie unter: **blockchain.fir.de**

Auch bei diesem spannenden Thema freuen wir uns über Zusammenarbeit, ob in bestehenden Projekten oder mit neuen Ideen. Melden Sie sich gern!

David Holtkemper, M.Sc.
Bereich Produktionsmanagement
Fachgruppe Supply-Chain-Management
Telefon: +49 241 47705-432
E-Mail: blockchain@fir.rwth-aachen.de

Blockchain