Das Blockchain-Netz

In Zukunft müssen Millionen von vernetzten Maschinen sicher kommunizieren und agieren. Ein vielversprechender Ansatz hierfür ist die Blockchain-Technologie der dritten Generation. Dabei wird auf eine verteilte, dezentrale Datenstruktur gesetzt, die Transaktionen transparent, chronologisch und unveränderbar in einem Netzwerk speichert.

Bild: pixabay / geralt

Daten werden infolge der zunehmenden Digitalisierung von Produktionsprozessen zum neuen Öl der Zukunft. Um jene zu ermitteln und weiterzuverarbeiten bietet die Vision Industrie 4.0 und das IoT ein bislang unausgeschöpftes Potenzial. Gleichzeitig stehen dieser Chance erhebliche Risiken hinsichtlich IT-Sicherheit und Datenschutz gegenüber. Denn die Kommunikation und Interaktion von Millionen oder gar Milliarden vernetzter Maschinen und Sensoren bietet auch eine enorme Angriffsfläche und unterschiedlichste Einfallstore für Hacker. Gefragt ist folglich eine sichere Basistechnologie, welche die Kommunikation verschiedenster IoT-Geräte regelt.

Das DAG-Prinzip

Als ein vielversprechender Ansatz gilt hierfür die Blockchain-Technologie der dritten Generation. Diese ist im eigentlichen Sinne gar keine Blockchain, sondern ein sogenannter gerichteter, azyklischer Graph (Directed Acyclic Graph, DAG), der sich lediglich die positiven Blockchain-Prinzipien zunutze macht. Dabei setzt das DAG-Prinzip auf eine verteilte, dezentrale Datenstruktur, die Transaktionen transparent, chronologisch, unveränderbar und quantencomputerresistent in einem Netzwerk speichert.

Ausschlaggebend ist vor allem, dass der DAG im Gegensatz zu bisherigen Blockchain-Modellen ohne Transaktionsgebühren auskommt, partitionstolerant und theoretisch unbegrenzt skalierbar ist. IOTA

verfolgt hiermit den Ansatz, dass das Netzwerk (sämtliche Nodes weltweit) nicht die komplette Datenbank synchronisieren und abspeichern muss. Damit ist der ‚Aufbau' kleinerer, neben dem Main-DAG bestehenden, Side-DAGs möglich – und zwar auch ohne Internet-Anbindung.

Eine Synchronisierung mit dem Main-DAG erfolgt dann, sobald eine Verbindung mit dem Internet besteht. Die Gewährleistung der Skalierung wird mit der Durchführung von sogenannten Snap-Shots umgesetzt. Dabei handelt es sich um ein Verfahren, welches zu einem definierten Zeitpunkt die gesamte Historie des DAGs bereinigt und auf ihre Korrektheit prüft. Anschließend werden die getätigten Transaktionen sicher in sogenannten Permanodes abgelegt und die dezentralen Nodes geleert. Die Nodes müssen somit nicht mit einer Historie vom Zeitpunkt Null an agieren.

Im abgebildeten Diagramm (*Bild 1*) beispielsweise steht jedes Quadrat für eine gesendete Transaktion. Jedes Mal, wenn eine neue Transaktion gesendet wird, erfolgt eine automatische Bestätigung von zwei vorhergehenden Transaktionen im Netzwerk (siehe die zwei Pfeillinien, die sich von jeder Transaktion zu zwei anderen Transaktionen erstrecken). Die grauen Felder auf der rechten Seite stellen neue (nicht validierte) Transaktionen dar. Die blauen Kästchen symbolisieren mehrfach validierte Transaktionen. Transaktionen, die ausreichend oft validiert wurden, um von ihrem Empfänger als ‚bestätigt' akzeptiert zu werden, sind durch grüne Kästchen repräsentiert. Für die Bestätigung muss von jedem Node ein Proof of Work durchgeführt werden (einfach gesagt: ein mathematisches Problem gelöst werden). Das Proof of Work soll zusätzlich Spam und Sybil-Attacken verhindern.

Verglichen zu anderen Blockchain-Protokollen ist dieses Verfahren leichtfüßig und kann von sämtlichen Kleinstgeräten durchgeführt werden. Anders als bei der Blockchain ist der User gleichzeitig der Validator (häufig auch Miner genannt). Dies ermöglicht das Wegfallen des rechenintensiven Mining-Prinzips sowie die derzeit bestehende Zentralisierung der Validierung in Mining-Pools (wenige, aber sehr große Mining-Farmen). Durch das Wegfallen von Minern kommt das DAG-Protokoll auch ohne Transaktionsgebühren aus.

Interoperabilität bietet Chancen für die Industrie

Da IOTA – wie seine Vorgänger Bitcoin und Ethereum – auch eine Kryptowährung ist, wird sie als solche von Skeptikern verpönt. Doch Sicherheitsexperten wie etwa Accessec warnen vor einer schnellen Verurteilung und sehen hierin insbesondere auch für die Industrie einen möglichen, sicheren Ansatz für den Weg in das Internet-der-Dinge. Denn IOTA ist mehr als nur ein Bezahlsystem. Unternehmen, die DAG-Technologie adaptieren, sind vielmehr in der Lage, ihre IoT-Visionen zu unterstützen und umzusetzen.

Einer der größten Vorteile birgt die Interoperabilität des Protokolls. Tatsächlich kann IOTA unterschiedliche IoT-Geräte und -Produkte miteinander verknüpfen. Die Kommunikation des IOTA-Protokolls ist nicht auf UDP und TCP beschränkt, sondern kann offen erfolgen, zum Beispiel via Bluetooth oder ZigBee. Auch Interoperabilität hinsichtlich anderer Payment-Systeme und Blockchain-Protokolle (etwa Ethereum, RSK, Qtum und Hyperledger) strebt die IOTA Foundation mittels 2nd-Layer-Lösungen an. Mit der Umsetzung der nachfolgend beschriebenen Lösungen sind ebenso Verknüpfungen zu anderen standardisierten Industrieprotokollen, wie etwa OPC UA, möglich und vergleichsweise einfach umzusetzen.

IOTA bietet in Summe große und sicherheitsrelevante Vorteile. Daten und Transaktionen können übertragen und auf dem DAG direkt gespeichert werden. Nicht nur unterschiedliche Anwendungsfälle lassen sich auf diese Weise abbilden, sondern auch unterschiedliche Funktionen durch Erweiterungen des Protokolls selbst.

So ist gerade eine Erweiterung namens ‚Qubic' in der Umsetzung. Diese soll in naher Zukunft ‚Smart Contracts', ‚Oracles' und ‚Outsourced Computing' ermöglichen. Im Fall von Smart Contracts spricht man zum Beispiel von programmierbaren Bedingungen, die an eine Transaktion geknüpft sind. Oracles hingegen sollen Informationen für Smart Contracts von außerhalb des DAG bereitstellen. Mit einem ‚Quorum Consensus-Prozess' soll sichergestellt werden, dass diesen aus Fremdquellen stammenden Informationen vertraut werden kann, ohne dass hierfür zentrale Instanzen zu deren Kontrolle herangezogen werden müssen. Zudem soll Outsourced Computing die Auslagerung von Rechenkapazität ermöglichen, welche mit IoT-Geräten nicht lokal abgearbeitet werden kann. Mehr noch: Künftig soll hierüber der Zukauf von Rechenkapazität möglich sein.

Schon jetzt steht hierfür das sogenannte Masked Authenticated Messaging (MAM) zur Verfügung, mit dem Datenströme – beispielsweise von Sensoren – verschlüsselt an den DAG gesandt und gespeichert werden können. Der Datenzugriff ist über einen Schlüssel steuerbar. Somit ermöglicht MAM Integrität, Datenschutz und Datenzugriffsmanagement in der Verwendung (siehe *Bild 2*).

Diese Funktion ist daneben zeitgleich die Grundlage für den IOTA-Datenmarktplatz, an dem sich weltweit bereits

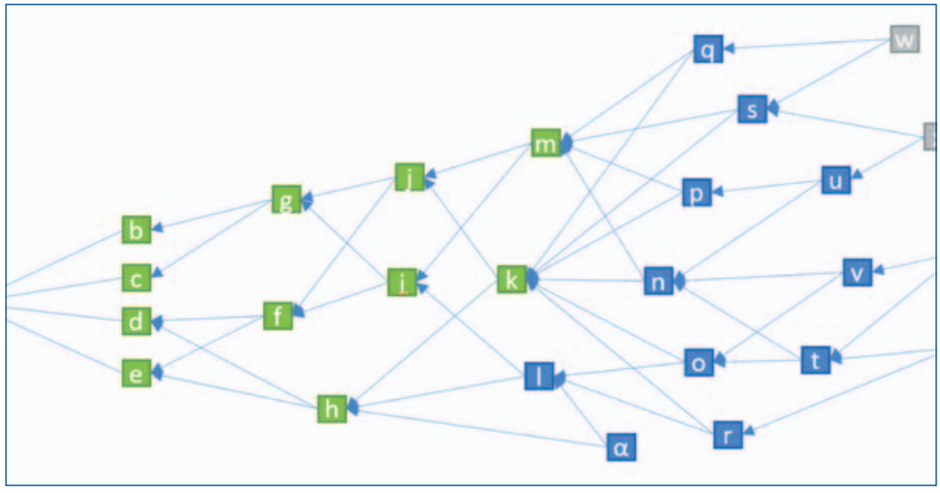

Bild 1. Im Gegensatz zur Blockchain handelt es sich beim DAG-Prinzip vielmehr um ein Netz als um eine Kette.

Bilder: Accessec

69 namhafte Unternehmen und Institutionen, vorrangig aus dem Umfeld Industrie, Kommunikation und IT, beteiligen. Der Marktplatz stellt sicher, dass die Daten durch ihre Unverfälschbarkeit und End-to-End-Datenüberprüfbarkeit wertvoll und weiter nutzbar bleiben. Die Integration von MAM sorgt darüber hinaus für die Einhaltung der EU-Datenschutz-Grundverordnung. Die Plattform schafft eine Alternative zur bisherigen Gangart, die überwältigende Mehrheit von Daten (auch aufgrund von Sicherheitsbedenken) in sogenannten Datensilos einzuschließen und ungenutzt zu lassen, und steht jedem offen, der Sensordaten und neue datengesteuerte Anwendungen bereitstellen und nutzen möchte.

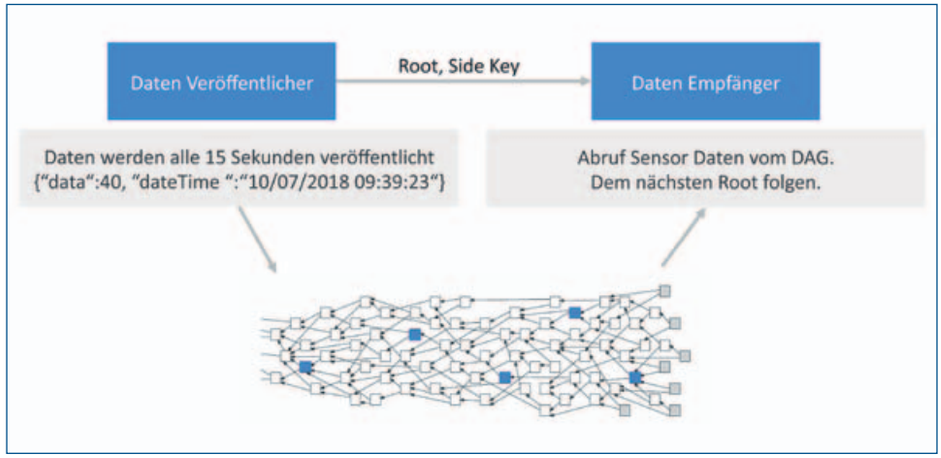

Bild 2. Beim MAM-Prinzip für verschlüsselte Datenströme können nur autorisierte Parteien den gesamten Datenstrom lesen und rekonstruieren. Anwender können ihre Empfänger bestimmen, indem sie diesen einen Schlüssel übergeben (Side Key). Der Root dient dabei der Identifikation von Nachrichten, welche der Empfänger benötigt, um eine Nachricht beziehungsweise den Datenstrom im DAG zu finden.

Industrielle Anwendungsfälle

Die Anwendungsfälle für die Industrie sind schier unbegrenzt. Momentan ist vor allem auch eine potenzielle Adaption und ein starkes Interesse im Bereich von autonom betriebenen (elektrischen) Autos, Produktionsdaten und den Lieferketten zu beobachten. So stellte beispielsweise Fujitsu einen Industrie-4.0-Proof-of-Concept für Fertigungsstraßen vor, die stellvertretend für smarte Fabriken stehen. Bestandteil des Konzepts ist ein Anwendungsfall für Audit-Trails und Transaktionen, mit dem ein Anwender in der Lage ist, Produktionsdaten zu erheben, zu verarbeiten und komplett zu visualisieren. Im Wesentlichen ist hierdurch die Fertigungskontrolle sowie Mikrotransaktionen zwischen Produktionen möglich, um die Überwachung von Maschinen und der Produktion gewähr-leisten zu können. Dabei ist jede einzelne Komponente detailliert nachverfolgbar. Zusätzliche Mittel für eine Kontrolle und Überwachung von Maschinen sind folglich obsolet. Jederzeit könnten die erhobenen Daten von einem Dashboard angezeigt werden. Dieser Case verdeutlich, dass IOTA die Arbeit von Maschinen überwachen und durch den kostenlosen Transfer von monetären Einheiten auch automatisch für eine Zusammenarbeit und den Austausch von Ressourcen zwischen Firmen sorgen kann.

Das Unternehmen Fujitsu arbeitet aktuell an der Integration von IOTA in seine IoT-Suite ‚IntelliEdge'. Zudem wirbt es wiederholt für sein Authentifizierungssystem ‚PalmSecure', das mittels biometrischer Handvenen-Daten und IOTA Anwendung finden soll. Fujitsu zielt damit auf eine benutzerfreundliche und hygienische Möglichkeit zur Überprüfung der Identität. Dies könnte künftig vor allem in medizinischen Bereichen und Laboren Anwendung finden, aber auch in sämtlichen Gebieten, wo eine schnelle und eindeutige Identität erforderlich ist.

Auch die RWTH Aachen zeigte die Vorteile kürzlich in einem IOTA-Proof-of-Concept auf. Die Universität nutzte IOTA bei der Problemlösung physikalischer Materialschwankungen und Prozessunsicherheiten, die physisch und statistisch gesehen immer vorhanden sind. Obwohl alle Komponenten in einem industriellen Umfeld die gleichen Anforderungen erfüllen müssen, sind feinste Abweichungen nicht auszumerzen. Diese individuellen Informationen und Abweichungen konnte die RWTH Aachen bereits in ersten Versuchen mit Hilfe digitaler Zwillinge der Komponenten öffentlich verfügbar machen. Hierfür wurden Produktionsdaten von Feinschneidteilen aus der Maschinensteuerung in Echtzeit extrahiert, verschlüsselt und im Gewirr gespeichert. Daten, wie die Stanzkraft, der Pressenhub oder der Materialname, sind so jederzeit über einen MAM-Kanal abrufbar. Auf diese Weise wären potenzielle Zulieferer in der Lage, Komponenten nach ihren Eigenschaften nachgelagert anzupassen und das Vertrauen der Endkunden zu erhöhen.

Aber nicht nur Unternehmen, sondern auch Institutionen wie die UN oder Kommunen sind an IOTA interessiert. So wird Taipe den IOTA-DAG als Grundlage für die intelligente Stadt der Zukunft nutzen. Unter anderem soll es eine DAG-basierte ID-Karte geben, mit welcher Identitätsdiebstahl und Wahlbetrug verhindern werden soll. Außerdem wird damit das Nachvollziehen der medizinischen Historie und anderer Daten für Regierungsdienste möglich.

Das Potenzial ist unverkennbar, auch wenn es momentan noch Chancen und Risiken abzuwägen gilt. Und obwohl sich der DAG derzeit noch weitestgehend in der Beta-Phase befindet, widerlegen erste Use Cases, es handele sich hierbei lediglich um eine ‚Mode-Erscheinung'. Insbesondere im industriellen Umfeld besteht die Möglichkeit, die Produktion schneller, billiger und sicherer zu gestalten. *ld*

SEBASTIAN ROHR
ist CEO bei Accessec.

MARKUS SOPPA
ist Research Consultant bei Accessec.