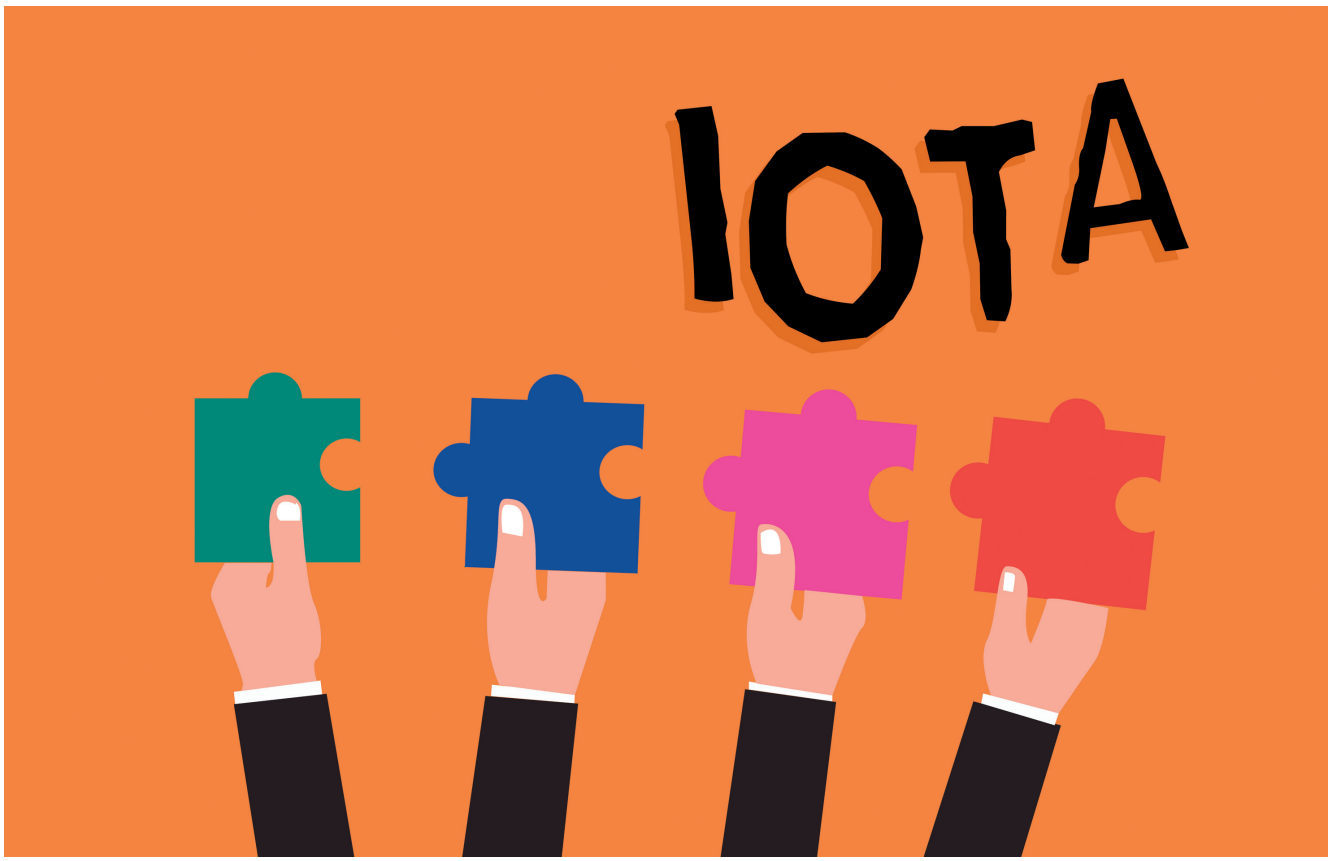


Bild: Shutterstock / Artur Szczybylo

VERTEILTES DATENBANKSYSTEM

IOTA für das IoT

Ein Peer-to-Peer-Datenbanksystem für die sichere und vollständig skalierbare Kommunikation vernetzter Geräte im Internet of Things.

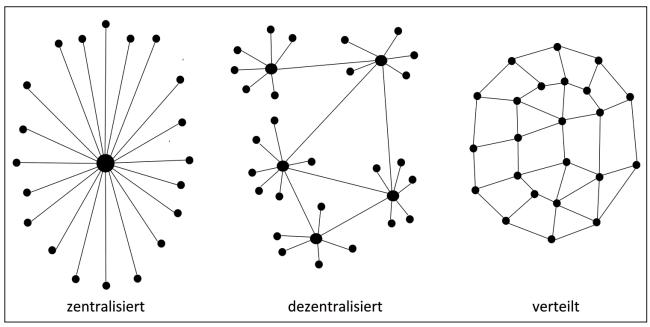
Die globale Vernetzung von Geräten nimmt rasant zu. Dabei ist von der Thematik das geschäftliche Umfeld im gleichen Maßstab betroffen wie der private Sektor. Über beide Bereiche gesehen gab es im Jahr 2014 bereits vier Milliarden vernetzte Geräte. Laut Prognosen ist bis Ende 2020 mit einem Zuwachs von mehr als 500 Prozent und damit mit einem Anstieg auf fast 21 Milliarden Geräte zu rechnen [1]. Egal ob vernetzte TVs, smarte Homecomputer-Anlagen, ein Kühlschrank, bei dem von unterwegs das Innere begutachtet werden kann, oder aber industrielle Fertigungsstraßen, die in Echtzeit jeden Prozess aufzeichnen und intelligente IoT-Features (Internet of Things) besitzen: Grundbedingung für diese Art von vernetzten IoT-Prozessen ist, dass die Geräte untereinander schnell und sicher kommunizieren. Schwierigkeiten stellen hier die Skalierbarkeit des Datenstroms und die dabei zu erhaltende Sicherheit dar.

Eine Möglichkeit für ein standardisiertes IoT-Protokoll, das diese Faktoren priorisiert, ist IOTA, ein völlig verteiltes Datenbanksystem, das der sicheren und vollständig skalierbaren Kommunikation dient [2].

Zentrale, dezentrale und verteilte Datenbanken

Eine reguläre einfache Client-Server-Datenbankarchitektur ist zentralisiert (vergleiche Bild 1). Sie besitzt also viele Clients, die alle mit einem Server kommunizieren. Dieser übernimmt die Übertragung und die damit verbundene Arbeit.

Der erste Schritt in Richtung IOTA-Architektur wäre die Dezentralisierung. Das bedeutet, dass jeder Teilnehmer entscheiden kann, ob er einen Server beziehungsweise einen Knotenpunkt darstellt. Ein Beispiel hierfür wäre eine Blockchain mit dem bekannten Vertreter Bitcoin [3]. Hier können Nutzer ihre Rechenleistung zur Verfügung stellen, um die Sicherheit der Übertragung zu gewährleisten, und erhalten im Gegenzug eine kleine Vergütung. Diese Vergütung wird über eine Gebühr bereitgestellt, die für eine Wertübermittlung eines Nutzers im Netzwerk fällig wird [4].



Darstellung eines zentralisierten, eines dezentralisierten und eines verteilten Systems (Bild 1)

IOTA ist ein verteiltes Datenbanksystem, das mit einem Peer-to-Peer-Netzwerk arbeitet und als Basis ein Konsens- und Validierungssystem verwendet. Da diese Eigenschaften einer Blockchain sehr ähnlich sind, fällt es aus technologischer Sicht auch in die Rubrik Kryptowährung und wird deshalb oft Blockchain 3.0 genannt [2]. Anstelle einer Blockchain findet bei IOTA der Tangle (deutsch: Gewirr) Anwendung. Dieser Tangle ist ein vollständig verteiltes Netzwerk, bei dem Daten auf den Transaktionen selbst gespeichert werden und diese die Knotenpunkte darstellen. Die Transaktionen sind wiederum sogenannten Seeds zugeordnet [5].

Funktionsweise des Tangle

Betrachtet man die Funktionsweise des Tangle, handelt es sich hierbei um eine sehr komplexe Blockchain. Eine Blockchain ist nichts anderes als eine lange Verkettung von Blöcken und stellt eine besondere Art des Hash-Baums dar (siehe Bild 2).

Dabei wird aus den Informationen einer Transaktion anhand eines Hash-Algorithmus ein Hash-Wert erzeugt. Ein Hash ist nichts anderes als eine digitale Signatur, die zu jeder Datenart berechnet werden kann. Das heißt, dass digitale Signaturen zu Filmen, Bildern, Texten und zu jeder weiteren Form von Daten existieren.

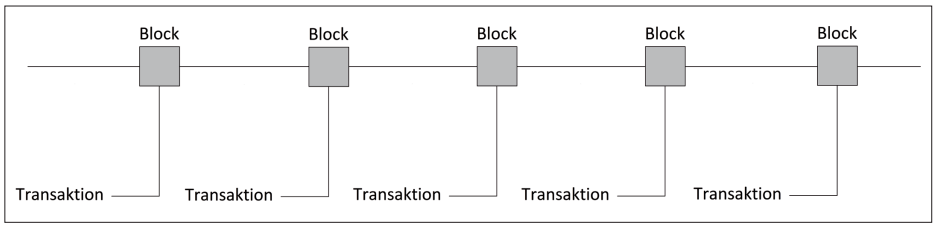
Wenn nun eine Transaktion stattfindet, wird daraus die digitale Signatur gewonnen, die einen Block darstellt. Die nächste Wertübermittlung erzeugt aus den eigenen Informationen und dem Hash-Wert des vorangehenden Blocks eine neue digitale Signatur und somit einen neuen Block.

Jeder Teilnehmer, der Übertragungen bestätigt, besitzt automatisch auch die vollständige Verkettung der Blöcke und wirkt an deren Berechnung mit. Die Blockchain befindet sich somit synchron auf verschiedenen Geräten. Dies unterbindet eine Datenmanipulation in diesem Konstrukt, da jede nachträgliche digitale Signatur im Fall einer Manipulation völlig unterschiedlich wäre [6]. Das tiefere Problem dieser Architektur ist die Skalierbarkeit, da es sich um eine einzelne Kette handelt, an die Informationen angehängt werden.

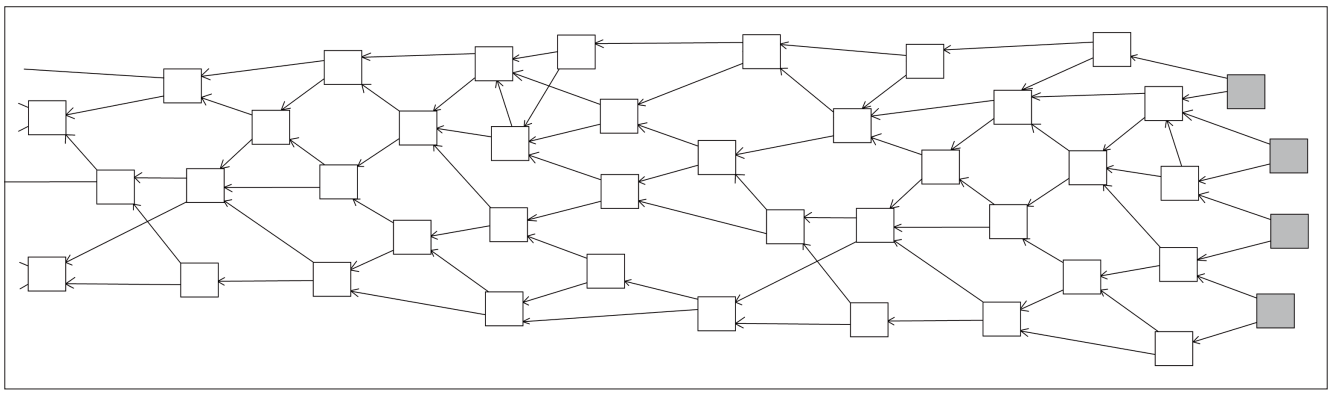
Aus diesem Grund verwendet IOTA als Sicherheitskonzept den Tangle, der ein gerichteter azyklischer Graph (DAG) nach Bild 3 ist. Anstelle von Blöcken existieren Transaktionen, die nicht ausschließlich der Reihe nach angeordnet sind, sondern ein Gewirr an Datenströmen ergeben und somit auch parallel Übermittlungen stattfinden lassen können.

Betrachtet man den Graphen in Bild 3, so lässt sich erkennen, dass jeder, der im Netzwerk Informationen austauschen möchte, gleichzeitig die Aufgabe der Validierung übernimmt. Die Aufgabe der Blockchain wird somit von einem Netzwerk gegenseitiger Transaktionsbeglaubigungen durchgeführt.

Ein Algorithmus sieht vor, dass für jede Transaktion zwei vorhergehende Transaktionen bestätigt und überprüft werden müssen [5]. Folglich wird bei einer steigenden Anzahl an Übermittlungen das Netzwerk nicht etwa verlangsamt, sondern beschleunigt. Ebenso wirkt sich dieser Prozess positiv auf die Sicherheit aus, da der Informationsaustausch bei steigender Netznutzung immer häufiger überprüft wird. ▶



Die Blockchain, visualisiert (Bild 2)



Der Tangle, visualisiert (Bild 3)

Die Zahlung für eine Transaktion findet durch die bereitgestellte Rechenleistung statt, die für den Prozess des sicheren Informationsaustauschs benötigt wird. Mehr Teilnehmer wirken sich also positiv auf das Netzwerk aus, wodurch sich IOTA als weltweit kostenloses und standardisiertes Netzwerkprotokoll eignet.

Vorteile von IOTA

Welche Gründe gibt es aber konkret, ein vollständig verteiltes Datenbanksystem, wie es das IOTA-Protokoll bereitstellt, zu verwenden? Schließlich könnte man bei der herkömmlichen zentralen Variante verbleiben oder zu einem dezentralen System wie der Blockchain wechseln.

Ein wichtiger Faktor für eine Welt der Maschinen ist der umfassende Austausch an Informationen. Da bei einer Blockchain jeder Block an den letzten angefügt wird und Blöcke Verkettungen von Hash-Werten darstellen, bietet dieses Modell keine Skalierungsmöglichkeiten. Es ist sogar so, dass eine länger werdende Blockchain das Netzwerk immer weiter verlangsamt und die benötigte Rechenleistung weiter ansteigt. Demgegenüber besitzt IOTA folgende Vorteile:

- Sicherheit und Transparenz,
- völlig verteilter Angriffspunkt,
- Gerätemanagement,
- gleichbleibend geringe Rechenleistung erforderlich,
- Skalierung; den Transaktionen pro Sekunde (TPS) sind keine Grenzen gesetzt,
- Kostenfreiheit,
- Quantencomputer-sicher,
- keine Mittelsmänner notwendig.

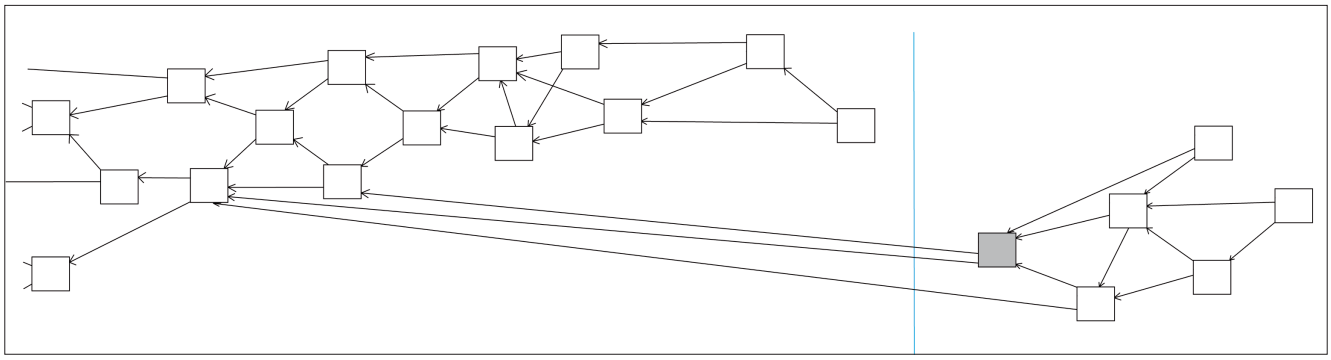
Jeder Teilnehmer stellt für eine Datenübertragung Rechenleistung zur Verfügung, um zwei andere Transaktionen zu verifizieren. Ein manipulierter Datensatz würde schnell erkannt werden und anschließend als unbestätigt gelten.

Betrachtet man die Architektur, so besitzt jeder Teilnehmer des Netzwerks einen eindeutigen Schlüssel, wodurch ein eindeutiges Gerätemanagement gewährleistet wird [7]. Da die Teilnehmer die Aufgabe der Validierung anhand gegenseitiger Transaktionsbeglaubigung übernehmen und der Prozess dahinter vorsieht, zwei Transaktionen zu validieren, erhöht sich bei steigender Netznutzung die Geschwindigkeit der TPS, während die benötigte Rechenleistung immer gleichbleibend gering ist. Außerdem entstehen durch diesen Validierungsprozess keine Kosten, da die Arbeit über die Nutzung selbst gezahlt wird. Dadurch eignet sich das Softwareprotokoll ideal für Services, da selbst kleinste Informationseinheiten in unbegrenzter Menge sicher, schnell und kostenlos verarbeitet werden.

Weiterhin ist IOTA quantensicher, ein Sicherheitsproblem, das sich in der Zukunft noch entwickeln kann und worauf das Softwareprotokoll bereits vorbereitet ist. Bei einer regulären Blockchain existieren pro Teilnehmer ein privater Schlüssel zur Identifikation und ein öffentlicher Schlüssel als Zieladresse bei Datenversand, ähnlich einer PKI-Struktur. Bei ausreichender Rechenleistung, die in der Zukunft beispielsweise von einem Quantenrechner bereitgestellt werden könnte, ließe sich über den Public Key der Private Key auslesen [8]. Allerdings wird die Sicherheit im Tangle über ein spezielles Signatur-Schema gewährleistet, das Winternetz-one-time-signature Scheme (WOTS) [9]. Hier ist das Auslesen des privaten Schlüssels nicht möglich, da sich die Schlüssel, die IOTA verwendet, aufgrund des verwendeten Signatur-Schemas anders verhalten. Aus diesem Grund gibt es keinen privaten Schlüssel mit einem zugeordneten öffentlichen Schlüssel, sondern Seeds mit einer zugehörigen exorbitant großen Anzahl an Adressen [7]. Dabei nimmt der Seed die Rolle des Private Keys ein, während jede Adresse als Public Key fungiert. Mithilfe der aufgezählten Vorteile dieser Technologie könnte wiederum eine sichere Handelsumgebung ohne Mittelsmänner garantiert werden, um Verträge sicherzustellen und vor Betrug zu schützen.

Konkrete Anwendungsfälle

Insbesondere im IoT-Bereich ist eine kostenlose, aber sichere und schnelle Variante des Informationsaustauschs notwendig. Deshalb gewinnt das Open-Source-Protokoll zunehmend an Aufmerksamkeit und kooperiert mit zahlreichen Unternehmen, unter anderem mit bekannten Konzernen wie Bosch, Fujitsu und Volkswagen [10]. Insbesondere Volkwagen präsentierte bei der Cebit 2018 in Hannover ein gemeinsames Konzept, an dem derzeit noch gearbeitet wird. Dabei handelt es sich um einen digitalen CarPass, wodurch jedes Fahrzeug über einen IOTA-Schlüssel eindeutig zu identifizieren ist. Ziel des Projekts ist es, zuverlässig Daten von Fahrzeugen aufzuzeichnen, um die Performance zu steigern. Vo-



Potenzielle Sicherheitslücke durch einen Seitenzweig (Bild 4)

raussichtlich 2019 könnten bereits die ersten Fahrzeuge mit IOTA-Technologie im Markt erhältlich sein. Der digitale Car-Pass stellt allerdings nur einen zentralen Bestandteil der Zusammenarbeit dar. Das VW-Tochterunternehmen Porsche etwa verfolgt den Ansatz, über den Tangle mehreren Einzelpersonen den Zugriff auf ein Fahrzeug zu gewährleisten [11].

Einfacher Einstieg dank Open Source und Community

Da es sich bei IOTA und der dahinterstehenden Technologie um Open-Source-Technologie handelt, ist der Einstieg für jeden leicht möglich. Um einen ersten Kontakt mit dem Projekt und dem dahinterliegenden Code herzustellen, gibt es ein über GitHub zugängliches Repository. Zusätzlich wurde speziell für Entwickler am 1. Mai 2018 der Start des IOTA Ecosystems verkündet, bei dem es sich um eine Plattform für Entwickler handelt. Die Idee ist, Interessenten den Einstieg zu erleichtern und eine Umgebung zu erschaffen, in der sich die Community austauschen kann. Erreicht werden soll dies über Lernmaterialien, Entwicklerressourcen, Artikel, Blogs, Organisationen und Start-ups im Kontext IOTA und Events. Weiter wurde ein Ecosystem Development Fund ins Leben gerufen, der sich auf Spenden von der Community selbst gründet. Bisher wurden circa zehn Millionen Dollar gesammelt, um Forschung, Weiterentwicklung und Projekte, die im Zusammenhang mit IOTA stehen, finanziell zu unterstützen [12].

Aktuelle Schwierigkeiten von IOTA

In der Theorie klingt IOTA nach einem bereits voll funktionsfähigen System – in der Realität weist die Technologie jedoch noch eine große Schwäche auf. Da derzeit zu wenige Transaktionen stattfinden, bietet das Netzwerk keinen ausreichenden Schutz und ist sehr langsam.

Die gegenseitige Transaktionsbeglaubigung verwendet einen Tip-Selektions-Prozess, wodurch Transaktionen bei ausreichender Beglaubigung anderer Transaktionen als bestätigt gelten. Bei einem kleinen Netzwerk könnte ein Angreifer einen eigenen Zweig am Tangle anfügen (siehe Bild 4), der größer als der eigentliche Tangle selbst ist. Dadurch würden über den Tip-Selektions-Prozess die Transaktionen am ursprünglichen Zweig als unbestätigt gelten [13].

Aus diesem Grund betreibt die IOTA Foundation einen sogenannten Koordinator, der in kurzen Zeitabständen Transaktionen durchführt, die als Milestones bezeichnet werden. Der gesamte Informationsaustausch nach einem Milestone ist direkt oder indirekt mit diesem verbunden. Der Koordinator stellt sicher, dass der Tangle in eine Richtung wächst, und hilft bei der Validierung mit. Wenn sich ein Zweig anfügt, der gefälschte Transaktionen beinhaltet, werden diese erkannt und gelten als unbestätigt [13]. Obwohl IOTA theoretisch als verteilt gilt, ist das Netzwerk somit momentan dezentral, was für viele ein nachvollziehbarer Kritikpunkt ist [14].

Zukunftsperspektiven

IOTA ist eine zukunftsorientierte Softwarelösung für die immer größer werdende Bedrohung durch Cyberkriminalität. Wird davon ausgegangen, dass das Protokoll weitreichende standardisierte Verwendung findet, ermöglicht IOTA kostenlose, sichere und schnelle Datenübertragung. Jeder Teilnehmer besitzt eine eindeutig zugeordnete ID, der Daten zugewiesen werden können. Dies ermöglicht ein völlig verteiltes Datenbanknetz, das eine große Anzahl an Vorteilen für eine Maschinenwelt ermöglicht. Da das gemeinnützige Protokoll über Maßnahmen für Projektförderung und eine starke Community verfügt, ist der Einstieg entsprechend einfach, wodurch eine weitreichende Verwendung realisiert wird.

Weiterhin beachtet IOTA bereits Risiken, die auf der Grundlage immer besser werdender Hardware Realität werden können. IOTA ist damit eine Technologie der Zukunft. Die Softwarelösung hat großes Potenzial, das Backbone des IoT-Zeitalters zu werden und den Datenverkehr auch bei immer größerem Durchsatz sicher zu gewährleisten. ■

[1] Jennifer Lapp, Was ist das Internet der Dinge und was hat es mit Marketing zu tun? www.dotnetpro.de/SL1902IOTA1

[2] Jannik Hüls, Tangle – Eine Einführung, www.dotnetpro.de/SL1902IOTA2

[3] Hagengraf, Zentrale, dezentrale und verteilte Systeme, www.dotnetpro.de/SL1902IOTA3

[4] Bitcoin Wiki, Transaktionsgebühren, www.dotnetpro.de/SL1902IOTA4

[5] Selim Baykara, Was ist IOTA und Tangle? Wir erklären die Kryptowährung, www.dotnetpro.de/SL1902IOTA5

[6] Schiller, Merkle Tree – Eine Basis der Blockchain, www.dotnetpro.de/SL1902IOTA6

[7] IOTA Guide, Seeds, Private Keys and Addresses, www.dotnetpro.de/SL1902IOTA7

[8] Sjoerd Langkemper, Breaking cryptography using quantum computers, www.dotnetpro.de/SL1902IOTA8

[9] Cryptowolf, Was ist IOTA? www.dotnetpro.de/SL1902IOTA9

[10] Christian Zink, Partner der Kryptowährung IOTA, www.dotnetpro.de/SL1902IOTA10

[11] Patrik Eberle, IOTA und VW werden 2019 Blockchain-fähige Autos auf den Markt bringen, www.dotnetpro.de/SL1902IOTA11

[12] Moritz Sattler, Das IOTA Ecosystem vorgestellt, www.dotnetpro.de/SL1902IOTA12

[13] Jelle Millenaar, IOTA Deepdive #1: Consensus on the Tangle, www.dotnetpro.de/SL1902IOTA13

[14] Limo, The Tech Behind IOTA Explained, www.dotnetpro.de/SL1902IOTA14

Moritz Diener
ist als Microsoft Trainee im CRM-Bereich bei der adesso AG am Standort Nürnberg tätig. Zu seinen Leidenschaften gehören Datenbanksysteme und moderne Technologien im IoT-Kontext.
moritz.diener@adesso.de

dnpCode A1902IOTA