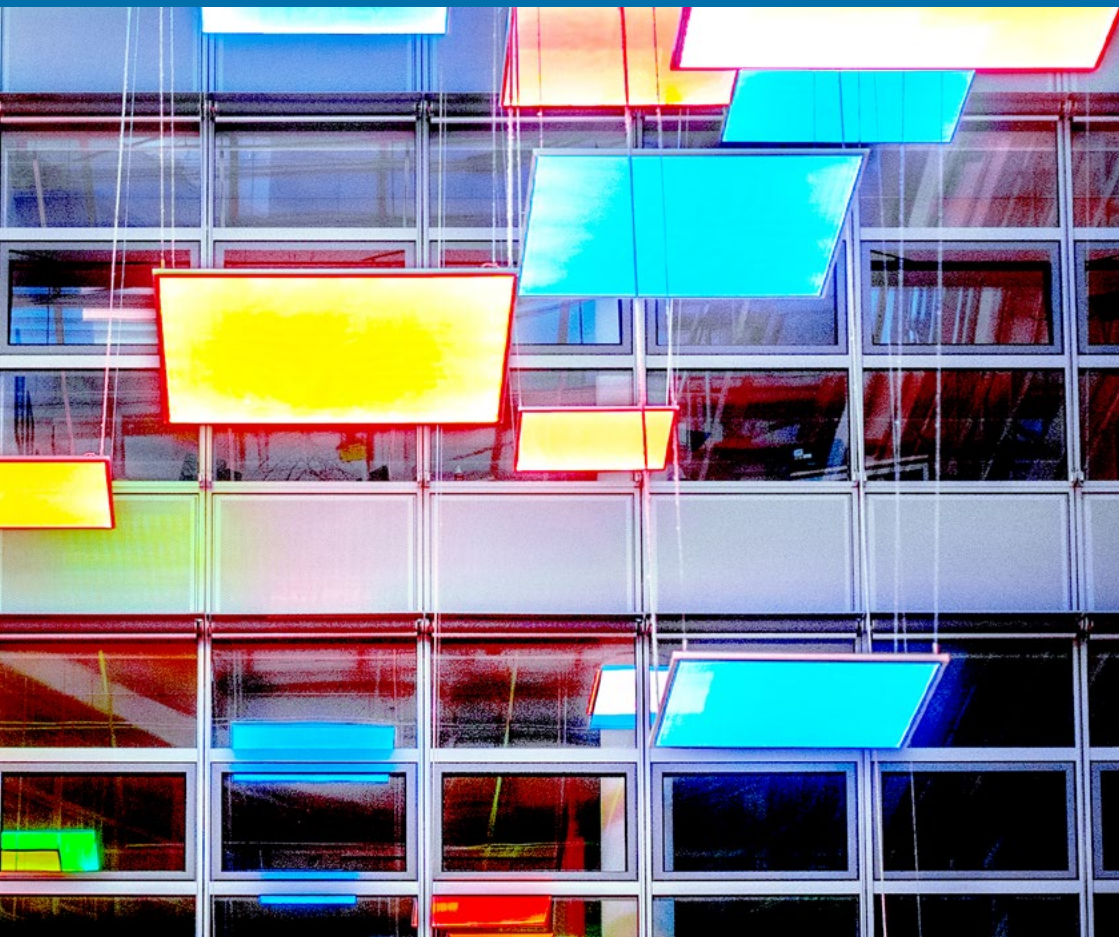
Fraunhofer

BLOCKCHAIN KOMPETENZEN UND SCHWERPUNKTE



INHALT

BLOCKCHAIN-POTENZIALE GEWINNBRINGEND NUTZEN

Prof. Dr. techn. Dieter W. Fellner,
Vorsitzender Fraunhofer-Verbund IUK-Technologie

Die Blockchain-Technologie durchlief in ihren ersten zehn Lebensjahren verschiedene Phasen zwischen Euphorie und Skepsis. Eine klassische Trendkurve zeichnete sich zunächst ab, die nach einem steilen Aufstieg immer weiteren Auftrieb durch neue Implementierungen und so genannte »Killer-Applikationen« erfuhr und schließlich im Status einer »Schlüsseltechnologie« mündete. Aktuell stagnieren jedoch die Erfolgsmeldungen rund um Blockchains. Grund dafür sind Hürden praktischer und psychologischer Natur, die den bewussten Einsatz von Blockchains in der Industrie als Ergänzung für etablierte IT-Prozesse verhindern. Dazu gehören unter anderen die hohen Erwartungen, die mit der Technologie verbunden werden und noch nicht eingelöst wurden, die vermeintliche Komplexität, aber auch negative Schlagzeilen über Kryptobörsen und eine wahrgenommene rechtliche Unsicherheit beim Einsatz von Smart Contracts. Unternehmen – vor allem Mittelständler – zögern daher, das Wagnis eines Innovationssprungs einzugehen. Dabei müssten gerade diese Firmen mehr in Innovation investieren, um ihre Wettbewerbsfähigkeit zu erhalten.

Doch seitens der Politik kommt Unterstützung: Mit der Blockchain-Strategie hat die Bundesregierung im September 2019 ein umfassendes Programm vorgelegt, mit dem die Potenziale für die digitale Transformation mobilisiert werden sollen.

Die Fraunhofer-Gesellschaft begrüßt dieses Vorhaben, da unsere Forscherinnen und Forscher ebenso davon überzeugt sind, dass Blockchains nicht nur viele IT-Prozesse effizienter machen, sondern auch für mehr Transparenz und Sicherheit für Anbieter und Anwender sorgen. Mehrere unserer Institute können wichtige Kompetenzen und Erfahrungen vorweisen, um die zunächst einmal abstrakte Technologie in reale Anwendungen zu überführen. Darüber hinaus besteht ein großer Vorrat an Wissen, um die Potenziale weiterer Digitalisierungstechnologien, auch in Verbindung mit Blockchains, zu entfalten.

Prof. Dr. Dieter Fellner

Um das Thema Blockchain ranken sich viele Mythen. Fraunhofer-Forscher haben diese nun einmal unter die Lupe genommen und nehmen Stellung zu Vorurteilen in Bezug auf die Technologie.

»Die Blockchain ist nur ein Hype.«

Die Blockchain hat auf jeden Fall einen Hype ausgelöst. Dieser ist vor allem auf Kryptowährungen zurückzuführen, welche viel Aufmerksamkeit auf das Thema gelenkt haben. Zum einen ist das natürlich positiv, zum anderen hat es auch viele überzogene Erwartungen geschürt. Insofern ist es ganz gut, dass der Hype jetzt langsam wieder abebbt, denn jetzt können andere Anwendungsfelder in den Blick genommen werden.
Wie sich das Thema weiterentwickeln wird, ist allerdings schwer vorherzusagen. Ich glaube, als Infrastruktur-Technologie wird Blockchain in Zukunft eher unsichtbarer werden. Das heißt, so einen Hype werden wir nicht noch einmal erleben, aber sie wird für viele andere Bereiche hoch interessant sein.
(Christian Welzel, Fraunhofer FOKUS)

»Die Blockchain wird Branchen und damit auch Arbeitsplätze abschaffen.«

Notare und Banken werden keinesfalls überflüssig. Über dieses Thema wurde zwar anfangs stark diskutiert, es hat sich jedoch relativ schnell herausgestellt, dass Banken, Notare und andere Intermediäre im Normalfall ein weites Aufgabenspektrum bearbeiten, welches weit über das hinausgeht, was eine Blockchain erfüllen kann. Natürlich kann die Technologie ansich dazu führen, dass sich die Arbeit verändert, weil Abläufe schneller, einfacher und günstiger funktionieren. Das bedeutet aber nicht, dass Arbeitsplätze verschwinden. Schon in der Vergangenheit und in Bezug auf die Industrialisierung hat sich gezeigt: Mit jeder Automatisierung hat die Arbeit keinesfalls abgenommen, die Arbeit ist stattdessen angenehmer und anders geworden.
(Prof. Dr. Gilbert Fridgen, Fraunhofer FIT)

Youtube-Playlist:
Blockchain-Mythen

»Der Energieverbrauch der Blockchain ist enorm hoch.«

Für bestimmte Blockchain-Anwendungen wie Bitcoin und Ethereum trifft dies zu. Diese verbrauchen Unmengen an Energie. Das liegt allerdings am Konsensverfahren, welches nicht für alle Anwendungen genutzt werden muss. Es gibt inzwischen zahlreiche Entwicklungen für andere Blockchain-Konsensverfahren in anderen Infrastrukturen. Mit diesen werden dann Anwendungen möglich, die sogar Energieeinsparungen oder ein besseres dezentrales Energiesystem ermöglichen. In vielerlei Hinsicht kann die Blockchain zudem nachhaltige Entwicklungen fördern. Durch Dokumentationsmöglichkeiten können beispielsweise Lieferketten besser gesteuert werden. Zusätzlich kann Transparenz vor allem in Hinblick auf ökologische und soziale Nachhaltigkeit geschaffen werden.

(Dr. Michael Kubach, Fraunhofer IAO)

»Im Vergleich mit KI ist Blockchain nur ein Nebenschauplatz.«

Das sind zwei unterschiedliche Technologien. Die KI ist hervorragend geeignet, um Daten zu interpretieren, das Unternehmen und die Unternehmensdaten zu digitalisieren und hier Schlüsse zu ziehen. Mit der Blockchain-Technologie ist man in der Lage, Netzwerke zu organisieren, Prozesse zu digitalisieren und das auf sichere Art und Weise. Wenn wir beides kombinieren, können wir auch anfangen, unsere Daten anderen vertrauensvoll zur Verfügung zu stellen. Wir können beide Technologien zusammenführen, um eine neue Datenökonomie zu schaffen. Aber dass man nur das eine oder das andere betrachten sollte, das ist nicht korrekt. Man muss eigentlich beide Trends aktuell sehr intensiv im Auge behalten.

(Prof. Dr. Wolfgang Prinz, Fraunhofer FIT)

Was ist Blockchain? Wichtige Begrifflichkeiten kurz erklärt

Blockchain-Technologie Blockchain-Technologie ist der Sammelbegriff für alle spezifischen Blockchain-Technologien, wie die Bitcoin- oder Ethereum-Blockchain-Technologie. Für den allgemeinen Begriff gibt es weder Code noch Bibliotheken. Vielmehr bezeichnet der Begriff die gängigen Konzepte, die in typischen spezifischen Blockchain-Technologien realisiert werden, wie das Speichern von Transaktionen in verteilter Form, Kommunikationsprotokolle für den Transport und die Validierung von Transaktionen.

Dezentrale Autonome Organisation (DAO) Eine DAO ist eine Blockchain-basierte, autonome, dezentral strukturierte Organisationseinheit, die auf der Basis eines Algorithmus selbstständig Entscheidungen trifft.

Distributed Ledger Ein Distributed Ledger ist ein öffentliches, dezentral geführtes Journal, in dem üblicherweise alle Geschäftsfälle eines Unternehmens chronologisch erfasst werden.

Hard Fork Eine irreversible Spaltung einer Blockchain in zwei inkompatible Fortsetzungen.

Hashfunktion/-wert/-baum Bei der Generierung neuer Blöcke einer Blockchain verwendete Abbildungsverfahren, die die Blöcke manipulationssicher machen.

Intermediär Vermittler bei Transaktionsgeschäften, der die Korrektheit des Ablaufs garantiert und dem die beteiligten Partner vertrauen.

Knoten Knoten bilden ein individuelles System innerhalb des Blockchain-Netzwerks. (Netzwerk-)Knoten bezeichnen den Verbindungspunkt für Datenübertragungen im Zusammenspiel mit weiteren Teilnehmern (Knoten) des Netzwerkes.

Kryptoagilität Die Möglichkeit in einem verschlüsselnden System kryptografische Verfahren, die unsicher geworden sind, durch neue, weithin sichere zu ersetzen.

Kryptowährungen Virtuelle, digitale Währung, die Blockchains als Transaktionsprotokoll einsetzt und kryptographische Verfahren zur Manipulationssicherheit einsetzt. Es gibt derzeit 2776 Kryptowährungen mit einer Marktkapitalisierung von insgesamt 227 Mrd. Dollar *(Quelle: investing.com, Stand September 2019)*. Darunter fallen neben dem Bitcoin z. B. Ethereum, Ripple, Litecoin, Ethereum Classic, NEM, Dash, IOTA, Bitshares, Monero, um nur einige zu nennen.

Mining Bezeichnet das Verfahren zur Lösung eines Kryptorätsels innerhalb eines Proof-of-Work Konsensmodells.

Nonce *(Abkürzung für: used only once oder number used once)*
In der Kryptographie wurde die Bezeichnung Nonce genutzt, um eine Zahlen- oder Buchstabenkombination zu bezeichnen, die nur ein einziges Mal in dem jeweiligen Kontext verwendet wird.

Payment Channel Networks Dies sind Konzepte für ein parallel zur Blockchain bestehendes Netz für den Zahlungsverkehr, das keine Transaktionsgebühren bedingt und maximale Vertraulichkeit er-

möglicht. Sie befinden sich derzeit in der Phase der experimentellen Implementierung.

Proof-of-Work Hierbei handelt es sich um ein Modell, bei dem ein Knoten das Recht erhält, den nächsten Block zu veröffentlichen, indem er Zeit, Energie und Rechenzyklen aufwendet, um ein schwer zu lösendes, aber leicht zu verifizierendes Problem zu entschlüsseln.

Pruning Pruning bezeichnet eine Möglichkeit, unnötige Daten über Transaktionen zu entfernen, die vollständig abgearbeitet sind.

Public und private Blockchains Public Blockchains sind öffentliche Systeme, auf die jeder, der eine Kopie besitzt, zugreifen kann. Das ist nicht gleichbedeutend mit dem automatischen Lesen und Schreiben auf einer Blockchain.
Private Blockchains beschreiben Systeme, die nur für ein abgeschlossenes Konsortium z. B. von Organisationen verfügbar sind. Der Öffentlichkeitscharakter ist von der Frage nach den Zugriffsrechten zu unterscheiden.
Public Blockchains sind häufig genehmigungsfrei. Bei Privaten Blockchains werden Zugriffsrechte in der Regel administriert bzw. auf ein Konsortium beschränkt.

Sharding Einzelne Rechner »verwalten« lokal lediglich verschiedene Partitionen der Blockchain.

Smart Contracts Computerbasierte Verträge, die nach bestimmten Regeln automatisch ausgeführt und z. B. in Blockchains protokolliert werden.

Smart Oracle Der Begriff Smart Oracle hat sich etabliert, wenn es darum geht, einen Zustand in der »realen Welt« zu bestimmen, der Einfluss auf die Ausführung eines Smart Contracts in einer Blockchain hat.

Transaktion Transaktionen sind Aufzeichnungen von Ereignissen, wie z. B. die Übertragung von Vermögenswerten (digitale Währung, Lagerbestände usw.) zwischen Parteien oder die Erstellung neuer Vermögenswerte.

Verteilte Konsensbildung Verfahren, das die Validität einer Transaktion über einen verteilten Beurteilungsprozess herstellt. Hierfür ist je nach eingesetztem Verfahren beispielsweise ein kryptographisches Rätsel von einem oder mehreren Teilnehmern der Blockchain zu lösen. Erst wenn die anderen Teilnehmer die Korrektheit der Lösung bestätigt haben, kann die Transaktion der Blockchain hinzugefügt werden.

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE INFORMATIONSTECHNIK FIT

Fraunhofer Blockchain-Labor
Das Fraunhofer Blockchain-Labor ist eine multidisziplinäre Einrichtung zur Konzeption, Entwicklung und Evaluation von Blockchain-Lösungen. Ein Arbeitsschwerpunkt liegt auf Entwicklungsmethoden für Blockchain-basierte Anwendungen, die die Digitalisierung in Unternehmensnetzwerken ermöglichen und unterstützen. Distributed-Ledger-Technologien (DLT) helfen, Unternehmensprozesse zu automatisieren, aber auch zu dezentralisieren. Das Blockchain-Labor überführt aktuelle wissenschaftliche Erkenntnisse aus dem Forschungsfeld DLT in praxistaugliche Anwendungen. Dabei unterstützt es Unternehmen und Organisationen bei der Identifikation von Innovationen und Effizienzsteigerungspotenzialen durch Blockchain und begleitet deren Realisierung.
In einem Pilotprojekt mit dem Bundesamt für Migration und Flüchtlinge wurde eine Blockchain-Lösung entwickelt, durch die die behördenübergreifende Zusammenarbeit im Rahmen des Asylprozesses erleichtert wird. Für die fälschungssichere Verwaltung von Zeugnissen und Sachkunde- sowie Herkunftsnachweisen wurde die Blockchain-for-Education-Lösung entwickelt. Für das Bundesministerium für Verkehr und digitale Infrastruktur wurde das »Grundgutachten Blockchain« erarbeitet, welches die Chancen und Herausforderungen von Blockchain in Bezug auf Mobilität und Logistik untersucht. Mit der Entwicklung zahlreicher Prototypen und Minimal Viable Products (MVP) unterstützt das Lab die Exploration verschiedener Blockchain-Anwendungen für die Industrie und konnte so eine breite Basis an Werkzeugen und Bibliotheken, z. B. für die immer wiederkehrende Aufgabe des Clearings in Kooperationsprozessen zwischen Geschäftspartnern, aufbauen, mit denen agil neue Use Cases umgesetzt werden können. Beispiele dafür

Das Fraunhofer
Blockchain-Labor

sind eine sichere Lebensmittelkette, eine Konsistenzsicherung für Informationsflüsse im Containertransport und eine Plattform für Mikrotransaktionen im Bereich Platooning. Das Blockchain-Labor hat verschiedene Methoden entwickelt, die eine systematische Untersuchung von Geschäftsprozessen und deren Überführung in ein Digitalisierungskonzept ermöglichen. Im Ergebnis konnten mit der Blockchain-Technologie nicht nur übergreifende Prozesse umgesetzt, sondern auch innovative Erweiterungen des Geschäftsportfolios ermöglicht werden. Zur Realisierung der identifizierten Blockchain-Innovationen bietet das Fraunhofer Blockchain-Labor Implementierungsleistungen von der Geschäfts- und Anforderungsanalyse über das prozessuale Design bis hin zum »Proof of Concept« oder MVPs. Durch individuelle Lösungen mit Hilfe unterschiedlicher Blockchain-basierter Konzepte sind die Anwendungsmöglichkeiten breit gestreut.

Ansprechpartner

Prof. Dr. Gilbert Fridgen
Projektgruppe Wirtschaftsinformatik
gilbert.fridgen@fit.fraunhofer.de
Telefon: +49 921 55-4711

Prof. Wolfgang Prinz, PhD
Leiter Kooperationssysteme
wolfgang.prinz@fit.fraunhofer.de
Telefon: +49 2241 14-2730

Prof. Dr. Thomas Rose
Leiter Risikomanagement
thomas.rose@fit.fraunhofer.de
Telefon: +49 2241 14-2798

Prof. Dr. Nils Urbach
Projektgruppe Wirtschaftsinformatik
nils.urbach@fit.fraunhofer.de
Telefon: +49 921 554-712

blockchain@fit.fraunhofer.de

FRAUNHOFER-INSTITUT FÜR ARBEITSWIRTSCHAFT UND ORGANISATION IAO

Das Fraunhofer IAO gestaltet das Zusammenspiel von Mensch, Technik und Organisation ganzheitlich und kundenindividuell. Im Team Identity Management untersuchen wir, wie sich Blockchain- und Distributed-Ledger-Technologien in der praktischen Anwendung schlagen, wo ihre Grenzen liegen und an welchen Stellen sich perspektivisch Entwicklungspotenziale ergeben. Anstatt einer rein technischen Betrachtung orientiert sich unsere Herangehensweise auch an den Marktbedürfnissen und Nutzerwünschen. Dabei liegt der Fokus unserer Projekte auf Anwendungen im Bereich Identitätsmanagement, Vertrauensinfrastrukturen, IT-Sicherheit und Datenschutz.

Derzeit in Entwicklung befindliche Blockchain-basierte Identitätsmanagement- und Vertrauensinfrastrukturen versprechen, zahlreiche gegenwärtige Herausforderungen zu adressieren. Wir betrachten etwa, wie sich hiermit Datensouveränität in einer Plattformökonomie ermöglicht oder die hochvernetzen Wertschöpfungsketten der Industrie 4.0 effizienter und datenschutzfreundlicher gestalten lassen könnten. Bei unseren diesbezüglichen Forschungen sind wir jedoch nicht auf die Blockchain-Technologie festgelegt, sondern nutzen je nach Herausforderung auch etablierte Technologien. Somit bieten wir eine fundierte, technologie- und anbieterunabhängige Analyse von Blockchain-Use-Cases, wobei wir nicht nur technische, sondern insbesondere auch Aspekte der User-Experience, mentale Modelle und sozioökonomische Faktoren in Betracht ziehen.

Hierauf aufbauend begleiten wir ebenso die praktische Umsetzung von Blockchain-Projekten von der mit dem Kunden erarbeiteten Anforderungsdefinition und Auswahl eines Technologie-Providers über die Steuerung der Implementierung bis hin zur Evaluation der Ergebnisse. Beispiels-

Blockchain-Projekte des Fraunhofer IAO

weise unterstützen wir eine große international agierende NGO bei der Durchführung eines Pilotprojektes zum Blockchain-basierten Identitätsmanagement. Unser Wissen über Blockchain-Use-Cases und deren sozioökonomische Wechselwirkungen floss zudem in eine von einem Industrieverband beauftragte Studie zu den potenziellen Auswirkungen der Technologie auf die ökonomische Entwicklung ein.

Ansprechpartner

Dr. Heiko Roßnagel
Leiter Team Identity Management
heiko.rossnagel@iao.fraunhofer.de
Telefon: +49 711 970-2145

Dr. Michael Kubach
Team Identity Management |
Sozioökonomische Aspekte
michael.kubach@iao.fraunhofer.de
Telefon: +49 711 970-2428

Rachelle Sellung
Team Identity Management |
Vertrauensinfrastrukturen
rachelle.sellung@iao.fraunhofer.de
Telefon: +49 711 970-2403

Stephanie Weinhardt
Team Identity Management |
User Experience
stephanie.weinhardt@iao.fraunhofer.de
Telefon: +49 711 970-2389

FRAUNHOFER-INSTITUT FÜR OFFENE KOMMUNIKATIONSSYSTEME FOKUS

Fraunhofer FOKUS erforscht und entwickelt die vernetzte Welt – sicher, zuverlässig und vertrauenswürdig. Dazu zählen beispielsweise der effiziente Zugang zu Informationen, der nachhaltige und wirtschaftliche Umgang mit Ressourcen, vernetzte Mobilität oder eine moderne öffentliche Verwaltung.

Seit 2017 betreibt FOKUS die Blockchain-Werkstatt in Berlin. In Kooperation mit der öffentlichen Hand, Unternehmen, Software-Herstellern, Standardisierungsorganisationen, Start-ups und Universitäten wird der Einsatz der Blockchain-Technologie in unterschiedlichen Anwendungsfeldern erforscht und erprobt. Zu den Schwerpunktthemen der Blockchain-Werkstatt zählen der Energiesektor, digitale Verwaltung, Open Data, Open Science, Qualitätssicherung, Identitätsmanagement und das Internet of Things.

Wir unterstützen Sie mit folgenden Leistungen:

- Hilfe bei der Erstellung oder Bewertung von Use Cases
- Analyse bestehender Anwendungen bzgl. Blockchain-Erweiterungen: Ist eine Blockchain für diesen Anwendungsfall geeignet, nachhaltig und wirtschaftlich?
- Unterstützung bei der Auswahl und Konzeption geeigneter Blockchain-Technologien oder verwandter dezentralen Technologien, bspw. durch Machbarkeitsstudien
- Erstellung von Demonstratoren und Pilotanwendungen
- Wissenschaftliche, fachliche und technische Begleitung bei der Umsetzung von Blockchain-Anwendungen

Die Blockchain-Werkstatt
des Fraunhofer FOKUS

Ansprechpartner

Prof. Dr. Manfred Hauswirth
Institutsleiter
manfred.hauswirth@fokus.fraunhofer.de
Telefon: +49 30 3463-7204

Christian Welzel
Geschäftsbereich DPS – Digital Public Services
christian.welzel@fokus.fraunhofer.de
Telefon: +49 30 3463-7377

Philipp Lämmel
Geschäftsbereich SQC – Quality Engineering
philipp.laemmel@fokus.fraunhofer.de
Telefon: +49 30 3463-7256

Fabian Kirstein
Geschäftsbereich DPS – Digital Public Services
fabian.kirstein@fokus.fraunhofer.de
Telefon: +49 30 3463-7718

FRAUNHOFER-INSTITUT FÜR EXPERIMENTELLES SOFTWARE ENGINEERING IESE

Ingenieursmäßige Entwicklung von Software-intensiven Systemen: Dafür steht das Fraunhofer IESE.

Systeme, die auf Blockchain-Technologie basieren, sind besonders anspruchsvoll in der Entwicklung. Unter anderem wegen der inhärent massiven Verteilung der Systeme, der komplexen und relativ neuen eingesetzten Technologien und der hohen Anforderungen an Sicherheit. Damit ist klar, dass methodische Unterstützung bei der Entwicklung Blockchain-basierter Applikationen für Software-Ingenieure sehr sinnvoll ist.

Das Fraunhofer IESE unterstützt Kunden mit passenden Methoden und aktiver Mitarbeit bei den ersten Schritten zu Blockchain-basierten Applikationen und bei deren systematischer Entwicklung.

Wir unterstützen Sie z. B. in folgenden konkreten Aspekten der Entwicklung:

- Etablierung eines gemeinsamen Verständnisses und Verwendung einer einheitlichen Terminologie rund um Blockchain, um häufige Missverständnisse direkt zu vermeiden

- Beurteilung der Eignung von Blockchain-Technologie für ein zu entwickelndes System:
  Ist es sinnvoll, auf Blockchain-Technologie zu setzen? Deuten die geforderten Qualitätseigenschaften in Richtung der Verwendung von Blockchain-Technologie?

- Treffen und Dokumentieren von zentralen Architekturentscheidungen für eine Blockchain-basierte Applikation: Was sind mögliche und nötige Entscheidungen und wie wirken sie sich aus?

Der Blockchain-Blog des Fraunhofer IESE

– Welche Auswirkungen hat die Verwendung von Blockchain-Technologie auf die User-Experience einer Applikation und welche Gestaltungsmöglichkeiten gibt es?

Ansprechpartner
Dr. Matthias Naab
Abteilung Architecture-Centric Engineering
matthias.naab@iese.fraunhofer.de
Telefon: +49 631 6800-2249

FRAUNHOFER-INSTITUT FÜR MATERIALFLUSS UND LOGISTIK IML

Das Fraunhofer-Institut für Materialfluss und Logistik IML gilt als erste Adresse in der ganzheitlichen Logistikforschung und arbeitet in den zentralen Bereichen Technologie, Unternehmenslogistik und Mobilität. Diese Forschung umfasst Themen wie z. B. Automation, Auto-ID, Transport, Lagerung, Verpackung, Bestand- und Risikomanagement sowie Planung und Finanzen in Supply Chains unter Verwendung innovativer Technologien wie KI, Blockchain, VR, AR und IoT. Das Institut kann dabei auf jahrelange Erfahrung aus zahlreichen Logistik- und IT Projekten in unterschiedlichen Branchen bauen und verfügt über eine hohe Kompetenz in der Planung, Realisierung und Pilotierung von Industrie 4.0-Lösungen.

Die Forschungsarbeiten im Bereich Blockchain und Smart Contracts fokussieren sich auf Anwendungen im Bereich der physischen und finanziellen Supply Chain und der Verknüpfung mit anderen Zukunftstechnologien wie IoT und künstlicher Intelligenz. Dies findet u.a. Berücksichtigung in aktuellen Forschungsprojekten, wie dem Industrie 4.0 Recht-Testbed (BMWi und Plattform Industrie 4.0) und dem Blockchain Reallabor im Rheinischen Revier. Diese Forschungsarbeiten werden durch eine Vielzahl praxisnaher Entwicklungsprojekte mit Kooperationspartnern aus unterschiedlichen Branchen komplettiert. So werden z. B. in den Enterprise Labs am Fraunhofer IML Lösungen für Anwendungsfälle mit hohem Praxisbezug gemeinsam mit Partnern aus der Industrie, oder der Dienstleistungsbranche entwickelt. Weiterhin können im Rahmen sogenannter Cross Lab Initiativen Synergien entlang von Wertschöpfungsketten erzeugt und genutzt werden, welche nur im Forschungsumfeld des Fraunhofer IML entstehen.

Homepage des
Fraunhofer IML

Das Leistungsspektrum im Bereich Blockchain umfasst die Identifizierung konkreter Use Cases für die Entwicklung von Smart Contracts zum Einsatz in Wertschöpfungsnetzwerken. Dabei werden individuelle Anforderungen der Partner aus Industrie, Handel und Finanzwirtschaft, die bereits bei der Auswahl geeigneter Technologien begleitet werden, berücksichtigt. Darüber hinaus werden am Fraunhofer IML Machbarkeits- sowie Kosten-Nutzen-Bewertungen durchgeführt und die Software für maßgeschneiderte Blockchain Anwendungen konzipiert und entwickelt. Im Rahmen diverser Pilotprojekte (z. B. Piel Technischer Großhandel, Commerzbank, Claas, Diebold Nixdorf) werden schließlich Blockchain-basierte Geschäftsprozesse entwickelt und direkt an Anwendungsfällen aus der Praxis validiert.

Ansprechpartner

Univ.-Prof. Dr. Michael Henke
Institutsleiter (Unternehmenslogistik)
michael.henke@iml.fraunhofer.de
Telefon: +49 231 9743-100

Dr. Axel T. Schulte
Abteilungsleiter Einkauf und Finanzen im Supply Chain Management
axel.t.schulte@iml.fraunhofer.de
Telefon: +49 231 9743-298

Dr.-Ing. Philipp Sprenger
Wiss. Mitarbeiter Einkauf & Finanzen im Supply Chain Management
philipp.sprenger@iml.fraunhofer.de
Telefon: +49 231 9743-167

Dipl.-Inf. Dominik Sparer
Wiss. Einkauf & Finanzen im Supply Chain Management
dominik.sparer@iml.fraunhofer.de
Telefon: +49 231 9743-296

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE UND INTEGRIERTE SICHERHEIT AISEC

Im Kontext von Blockchain liegt der Forschungsschwerpunkt des Fraunhofer AISEC auf dem Bereich IT-Sicherheit. Der Fokus liegt auf der Entwicklung vertrauenswürdiger Blockchain-Anwendungen. Außerdem beschäftigen sich die Forschenden mit der Analyse der Sicherheitseigenschaften bereits existierender Plattformen.

Obwohl Anwendungen auf Blockchain-Basis häufig als »Secure-by-Design« beworben werden, verfügen sie häufig nur über wenige Sicherheitsmerkmale. Vielmehr bestehen sie aus komplexen, aufeinander aufbauenden Software-Schichten, deren Sicherheitseigenschaften auch für Experten schwer zu beurteilen sind.

Ein Sicherheitsrisiko sind z. B. fehlerhafte Smart Contracts: Diese speziellen Anwendungen werden in der Blockchain veröffentlicht und unveränderlich gespeichert. Einmal eingebracht lassen sie sich nicht mehr entfernen, mögliche Programmierfehler und Sicherheitslücken bleiben dauerhaft im System. Die Entwicklung von Smart Contracts ist keineswegs einfacher als die von traditionellen Anwendungen – im Gegenteil: Durch das Modell der verteilten Ausführung schleichen sich schneller Fehler ein. Um Entwickler zu unterstützen, erarbeitet das Fraunhofer AISEC Werkzeuge wie »Annotary«, um Fehler schon im Entwicklungsprozess zu vermeiden.

Hemmnisse für die breite Nutzung von Blockchain-Technologien resultieren oft aus den Bedenken von Nutzern und Unternehmen, ihre sensiblen Daten öffentlichen Systemen anzuvertrauen. Hinzu kommt, dass gerade diese Technologien darauf beruhen, dass Daten auch im Nachhinein nicht gelöscht werden können.

Blockchain-Projekte des
Fraunhofer AISEC

Aus diesem Grund entwickelt das Fraunhofer AISEC Lösungen, um Blockchain-Anwendungen in Einklang mit Sicherheitsanforderungen von Unternehmen zu bringen. Innovative kryptografische Verfahren, wie beispielsweise *Attribute-based Encryption*, ermöglichen nur einem autorisierten Benutzerkreis Zugriff auf die verschlüsselten Daten – trotz öffentlicher, dauerhafter Speicherung. Anwendung findet dies in der »TrackChain«, einer Lösung zur Nachverfolgung von Ereignissen in Logistik-Ketten. So lassen sich Paketsendungen über Unternehmens- und Ländergrenzen hinweg verfolgen, um Verluste von Paketen zu minimieren und die Transparenz zu erhöhen.

Ansprechpartner
Dr. Julian Schütte
Abteilungsleitung
Service & Application Security
julian.schuette@aisec.fraunhofer.de
Telefon: +49 89 3229986-173

Christian Banse
Abteilungsleitung
Service & Application Security
christian.banse@aisec.fraunhofer.de
Telefon: +49 89 3229986-119

Martin Schanzenbach
Service & Application Security
martin.schanzenbach@aisec.fraunhofer.de
Telefon: +49 89 3229986-193

Mark Gall
Service & Application Security
mark.gall@aisec.fraunhofer.de
Telefon: +49 89 3229986-124

Impressum

Herausgeber
Fraunhofer-Verbund IUK-Technologie
Anna-Louisa-Karsch-Straße 2
10178 Berlin
pr@iuk.fraunhofer.de
www.iuk.fraunhofer.de

Redaktion
Henning Köhler, Carolin Steinert

Gestaltung, Layout
Carolin Steinert

Bildquellen
Cover und Rückseite: Henning Köhler,
Fraunhofer-Verbund IUK-Technologie

Seite 3: Fraunhofer-Institut für
Graphische Datenverarbeitung IGD

Weitere Informationen
www.iuk.fraunhofer.de/blockchain

Twitter
twitter.com/Fraunhofer_IUK
Youtube
youtube.com/fraunhofer-innovisions
Soundcloud
soundcloud.com/fraunhofer-innovisions

Erschienen im September 2019