ÖFIT-Trendschau

Bibliographische Angaben

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 60

Smart Contracts

Herausgeber:

Kompetenzzentrum Öffentliche IT
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut FOKUS
Kaiserin-Augusta-Allee 31, D-10589 Berlin
Telefon: +49 30 3463 - 7173
Telefax: + 49 30 3463 - 99 - 7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

Autorinnen und Autoren der Gesamtausgabe: Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Nicole Opiela, Florian Friederici, Jan Gottschick, Jan Dennis Gumz, Fabian Manzke, Rudolf Roth, Dorian Grosch, Maximilian Gahntz, Hannes Wünsche, Simon Sebastian Hunt, Fabian Kirstein, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen: Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Autorinnen/Autoren: Fabian Kirstein

Bibliographische Angabe: Fabian Kirstein, Smart Contracts, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT,
https://www.oeffentliche-it.de/-/smart-contracts

Smart Contracts

Smarte Verträge versprechen, die Vorteile der Digitalisierung für die Vertragsgestaltung und -abwicklung nutzbar zu machen: Vertragssicherheit soll durch neue Formen der Vertrauensbildung und Nachvollziehbarkeit sowie durch kontinuierliche Überprüfung der Vertragseinhaltung auf eine neue Grundlage gestellt und automatisiert werden. Ergeben sich durch die digitale Abbildung von Verträgen neue Möglichkeiten im Hinblick auf Effizienz und Transparenz – oder lässt sich die Vielfalt der vertraglichen und juristischen Anforderungen durch starre Softwareprotokolle doch nicht hinreichend abbilden?

Was ist ein Smart Contract?

Ein Smart Contract ist ein Computerprogramm, das die Abbildung, Ausführung und Verifikation eines Vertrages ermöglicht. Die vertraglichen Vereinbarungen sind in Form eines Algorithmus fest kodiert. Der Begriff wurde bereits in den 1990er Jahren geprägt. Nutzbare Implementierungen sind allerdings erst auf Basis der **Blockchain**- bzw. Distributed-Ledger-Technologie entstanden, die die Anforderungen hinsichtlich der nötigen Vertrauenswürdigkeit, Nachvollziehbarkeit und Transparenz erfüllt. Aktuelle Smart Contracts nutzen also eine Blockchain als technische Grundlage, um vertragliche und vertragsähnliche Prozesse abzubilden.
Eine Blockchain ermöglicht eine fälschungssichere, dezentrale Speicherung und Überprüfung der Zulässigkeit von Transaktionen. Üblicherweise werden in den so abgesicherten Transaktionen Vermögenswerte (Digitale Assets) zwischen den Teilnehmenden nachvollziehbar ausgetauscht.

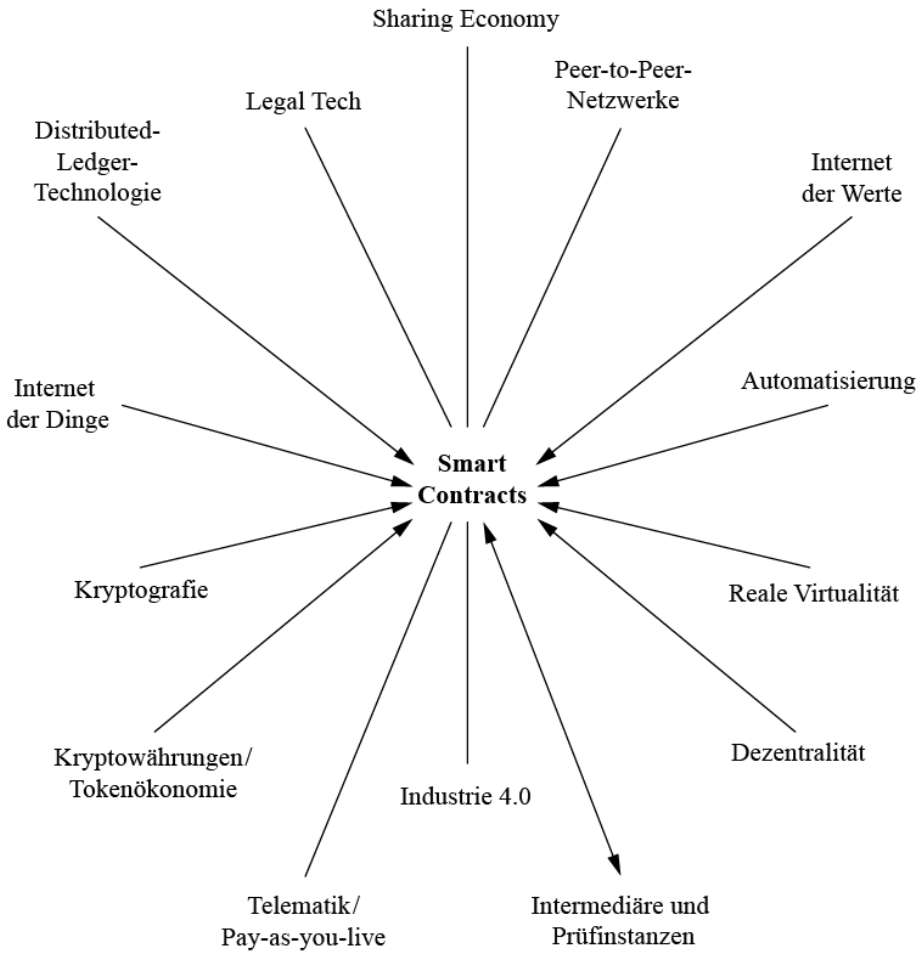
Bei **Kryptowährungen** werden etwa die entsprechenden Währungseinheiten übertragen. Dieser einfache Transfer wird bei Smart Contracts nun um die Ausführung eines Computerprogrammes erweitert. Bei einer Transaktion werden entsprechende Methoden des Vertrages ausgeführt. Ein Smart Contract wird dabei auf allen Teilnehmerknoten der Blockchain installiert und kann von allen Nutzer:innen gelesen und interpretiert werden. Analog zu Open-Source-Software können dadurch Fehler oder betrügerische Absichten entdeckt und kommuniziert werden. Darüber hinaus sind in einer Blockchain hinterlegte Smart Contracts unveränderbar und bleiben somit in ihrer Funktionsweise konstant. Mit rechtsgültigen Verträgen können sie dabei (noch) nicht gleichgesetzt werden.

Funktionsweise

Anders als der Name suggeriert, sind Smart Contracts nicht besonders »smart«. Vielmehr bezieht sich der Begriff auf die automatische Ausführung der Programmlogik ohne das Eingreifen von Dritten. Die Verträge bilden meistens nur einfache Wenn-Dann-Regeln ab. Auf diesem Weg werden Bedingungen und Ereignisse kodiert, deren Eintreten automatisch zuvor festgelegte Aktivitäten auslöst. Alle Teilnehmenden bzw. Vertragspartner:innen werden über ausgeführte Aktivitäten und Statusänderungen informiert. Theoretisch lassen sich auf Basis dieser einfachen Regeln auch sehr komplexe Vertragsverhältnisse und Bedingungen abbilden. An die Grenzen der Abbildbarkeit stoßen Smart Contracts allerdings immer dann, wenn der Vertragsgegenstand nicht in allen Punkten abschließend geregelt ist. Solche als unvollständig bezeichneten Verträge werden sowohl zwischen Privatpersonen als auch im B2B-Bereich geschlossen. Sie zeichnen sich oft durch eine lange Laufzeit und durch noch nicht bestimmbare Änderungen und Konkretisierungen während der Vertragslaufzeit aus, wie es etwa typischerweise bei Arbeitsverträgen der Fall ist. Eine wie auch immer geartete Flexibilität hinsichtlich der Veränderung vertragsrelevanter Rahmenbedingungen oder unerwarteter Ereignisse verbietet sich aufgrund des Determinismus' einfacher Regeln.

Smart Contracts werden im Zusammenhang mit Kyptowährungen als Übergang vom »Internet der Informationen« zum »Internet der Werte« diskutiert. Während die Kernfunktion des Internets in der Übertragung von Daten als Informationen besteht, werden mit Kryptowährungen direkt handelbare Zahlungsversprechen übermittelt. Smart Contracts können diese Übermittlung strukturieren, automatisieren und darüber hinaus die Übertragung anderer Wertgegenstände absichern. Als Beispiel wird oftmals ein Pkw-Leasingvertrag herangezogen. Dabei können nicht nur die Ratenzahlungen automatisiert werden, auch die Vertragseinhaltung lässt sich kontinuierlich überwachen. Bei kodifizierten Vertragsverstößen wird dann automatisch interveniert: Bei Ausbleiben einer Ratenzahlung oder Überschreitung der vereinbarten Fahrleistung kann der Pkw beispielsweise nicht mehr gestartet oder die zusätzlichen Kilometer automatisch abgerechnet werden (siehe auch **Pay-as-you-live**).

Begriffliche Verortung



Anwendungsfelder

In Smart Contracts werden große Potenziale für die Kooperation in B2B-Märkten und für den Legal-Tech-Sektor gesehen. Besonders für Handel und Logistik bieten sie interessante Anwendungsfelder. Sharing-Konzepte und Bezahl- oder Rechnungssysteme für verbundene Endgeräte sowie Peer-to-Peer-Marktplätze jeglicher Art können mit Smart Contracts realisiert werden. Der Ausschluss eines Intermediärs zwischen den Vertragsparteien erhöht die Effizienz der Kooperation etwa in Bereichen, in denen üblicherweise Banken, Notare, Clearingstellen oder andere Dritte benötigt werden.

Besonders weit in der Erprobung von Smart Contracts ist die Energiewirtschaft. Dort werden derzeit intensiv die potenziellen Anwendungsmöglichkeiten für den Handel mit kleinen Energiemengen zwischen dezentralen Produzenten und Netzbetreibern erforscht. Darüber hinaus können problemlos Kryptowährungen in die Verträge implementiert werden, um z. B. bei Vertragserfüllung unmittelbar zu bezahlen oder bei ausbleibender Zahlung die Lieferung zu stoppen.

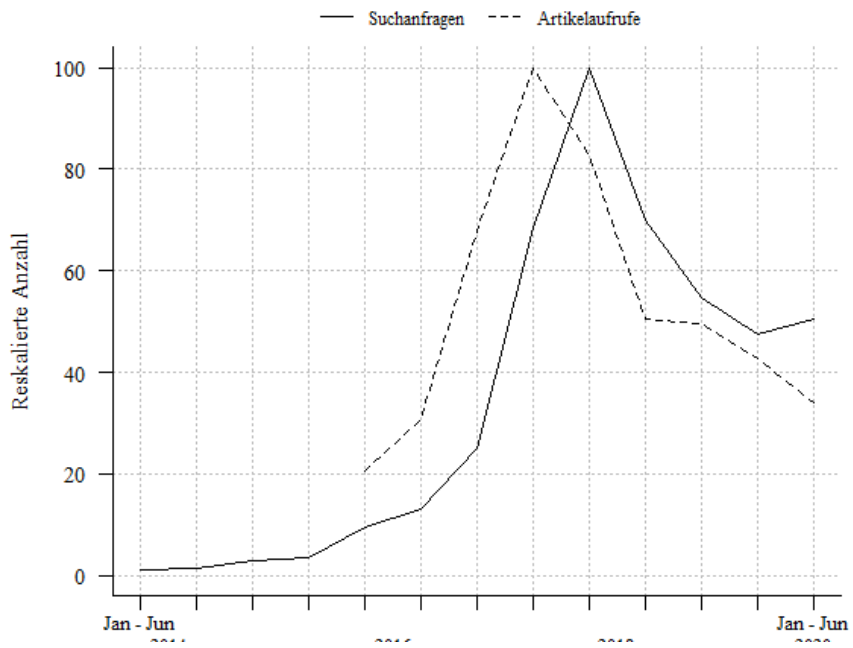
Insgesamt dienen Smart Contracts derzeit eher der Prozess- und Kommunikationsoptimierung, denn der vollständig digitalen Abbildung komplexer Verträge.

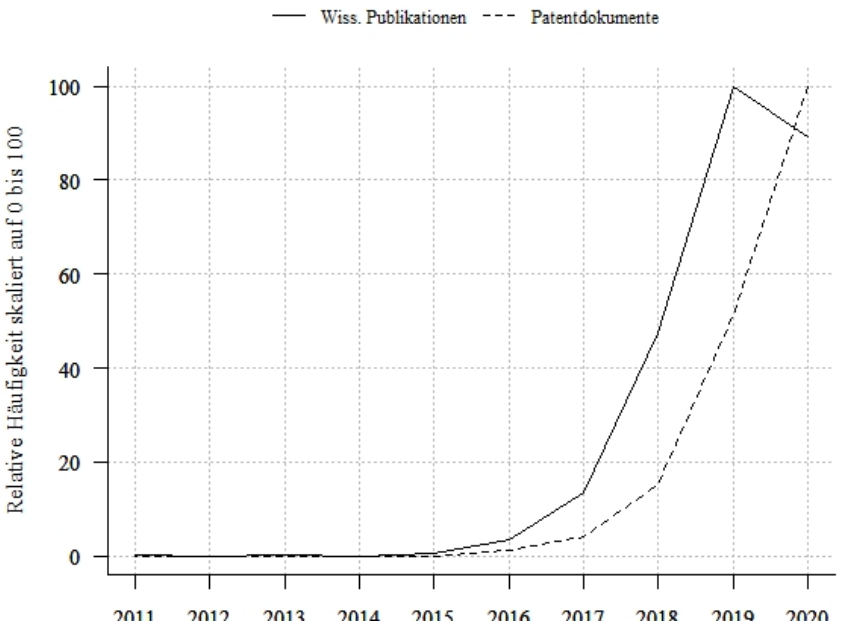
Vorzüge

Neben einer höheren Transparenz, Effizienz und der Möglichkeit der Automatisierung von Vertragsfolgen, bieten Smart Contracts gegenüber traditionellen Verträgen weitere Vorteile. Sie erreichen eine hohe Verlässlichkeit, da Parameter und Bedingungen eindeutig definiert sind und festen Regeln folgen. Durch kryptografische Verschlüsselungsverfahren ist eine Manipulation der Vertragsbedingungen nahezu ausgeschlossen und lässt sich auch bei geringem Vertragswert mit standardisierten Mitteln sicherstellen.

Zudem können Smart Contracts bei höheren Vertragswerten zu einer Vereinfachung des Vertragsabschlusses beitragen. Sie sind im Kern unabhängig von vertrauenswürdigen dritten Parteien, da der Vertrag unveränderlich ist und die Vertragsbedingungen autonom durchsetzt.

Themenkonjunkturen





Herausforderungen

Smart Contracts erben viele Herausforderungen ihrer Basistechnologie Blockchain. Dazu zählen insbesondere der Bedarf an enormen Rechenleistungen für einige der digitalen Verifikationsverfahren, die limitierte Skalierbarkeit und eine schwache Usability. Zudem gibt es bislang weder explizite Regeln, noch eine signifikante Rechtsprechung oder Standards und Zertifikate für die Umsetzung von Smart Contracts. Es besteht darüber hinaus kein Mechanismus zur (einseitigen) Korrektur fehlerhafter oder nichts rechtsgültiger Verträge bzw. ihrer Rückabwicklung.

Eine große Herausforderung liegt in der Programmierung der Smart Contracts. Die einzige wirkliche Absicherung der intendierten Vertragsausführung besteht darin, die gewünschten Vertragsinhalte angemessen zu spezifizieren und die Anwendungen ohne Fehler zu entwickeln. Fehlerfreiheit erweist sich jedoch schon bei mäßig komplexen Verträgen als kaum zu bewältigen. Daher müssen sich Smart Contracts auf einfache Algorithmen beschränken und zudem von erfahrenen Softwareentwickler:innen umgesetzt werden, was ihren Anwendungsbereich stark einschränkt. Es ist jedoch genauso gut vorstellbar, dass die Vorzüge von Smart Contracts auch auf die Vereinfachung von Verträgen zurückwirken.

Weitere Anwendungsfelder können Smart Contracts dann erschließen, wenn sie Vertragsgegenstände in der physischen Welt abbilden, bspw. eine ausgelieferte Ware oder ein gekauftes Auto. Hierbei entsteht unweigerlich ein Medienbruch, der überwunden werden muss. Ein digitales Asset kann durch die Ausführung eines Smart Contracts die Besitzenden wechseln, der Wechsel eines physischen Assets muss jedoch durch ergänzende Maßnahmen abgesichert werden. Eine solche Verifikation von Vorgängen in der physischen Welt bietet Einfallstore, Verträge auch bei perfektem Code zu korrumpieren.

Smart Contracts befinden sich noch in einem sehr frühen Stadium der Technologieentwicklung. Der Vielzahl an offenen Fragen und Herausforderungen wird mit zahlreichen Prototypen und Frameworks wie der Open Source Blockchain Ethereum zu begegnen versucht. Die Entwicklung dürfte auf mittlere Sicht dynamisch bleiben.

Folgenabschätzung

Möglichkeiten

- Hohe Verlässlichkeit durch formalisierte Parameter und Bedingungen
- Transparenz und Sicherheit durch den Einsatz einer Blockchain und kryptografischer Verfahren
- Effizienzsteigerungen durch automatisierte Umsetzung von Vertragsbedingungen
- Unabhängigkeit von Prüfinstanzen und Intermediären
- Demokratisierung der Vertragsgestaltung
- Rückwirkung auf die und Vereinfachung der Vertragsgestaltung im Allgemeinen

Wagnisse

- Verlust von (rechtlichen) Spielräumen und Interpretationsfreiräumen
- Herausfordernde Softwareentwicklung und fehlerhafter Quelltext
- Abbildbarkeit komplexer und unvollständiger Verträge
- Verifikation physischer Vorgänge
- Reifegrad und Entwicklung
- Korrektur und Rückabwicklung fehlerhafter Verträge
- Mangelnde Rechtssicherheit und Standardisierung
- Blockchain-typische Herausforderungen, wie DSGVO-Konformität, Usability, Energieverbrauch, Skalierbarkeit

Handlungsräume

Erwartungen durch Erfahrung objektivieren

Die prinzipiellen Möglichkeiten von Smart Contracts sind momentan nur sehr eingeschränkt nutzbar. Vielversprechende Anwendungsfälle sollten prototypisch unter Einbindung aller Stakeholder umgesetzt und evaluiert werden. Dabei sollten sich die Anwendungen zunächst auf Verträge mit vollständigen Bedingungen und hohem Automatisierungspotenzial konzentrieren.

Rechtliche Regelungen

Das Fehlen expliziter Regeln und einer entsprechenden Rechtsprechung stellen derzeit ein großes Hindernis zur höheren Verbreitung von Smart Contracts dar. Eine bessere Vorhersehbarkeit der Rechtsfolgen sowie Standardisierung und Zertifizierung könnten dem Konzept zum Durchbruch verhelfen.

Lösungen für technische Herausforderungen

Eine genaue Beobachtung und Abschätzung der Basistechnologie Blockchain und möglicher Alternativen sind notwendig, um die bestehenden technischen Schwachstellen zu lösen und die Tragfähigkeit von Smart Contracts zu verbessern.