ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 37:

Blockchain

Stand: September 2017

Herausgeber:
Mike Weber
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, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen:
Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

September 2017

Autorinnen/Autoren:
Christian Welzel et al.

Bibliographische Angabe:
Christian Welzel et al. 2018, Blockchain, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/-/blockchain

Blockchain

Die Blockchain gilt als neuer Stern am Himmel der IT-Szene. Bekannt vor allem als Grundlage der Kryptowährung Bitcoin, wird ihr das Potenzial zugesprochen, ganze Wirtschaftszweige zu verändern: Klassische Banken sollen durch die Blockchain-Technologie ersetzt und smarte Verträge darüber abgewickelt werden können. Eine komplexe Technologie, die völlig ohne zentrale Instanzen auskommen will, verspricht neue Freiheiten und Transparenz. Doch wie funktioniert die Blockchain? Handelt es sich wirklich um einen Mechanismus, der die Gesellschaft nachhaltig verändern wird – oder doch nur um eine verteilte Datenbank, wie es sie schon lange gibt?

Transaktionsabsicherung ohne zentrale Instanzen

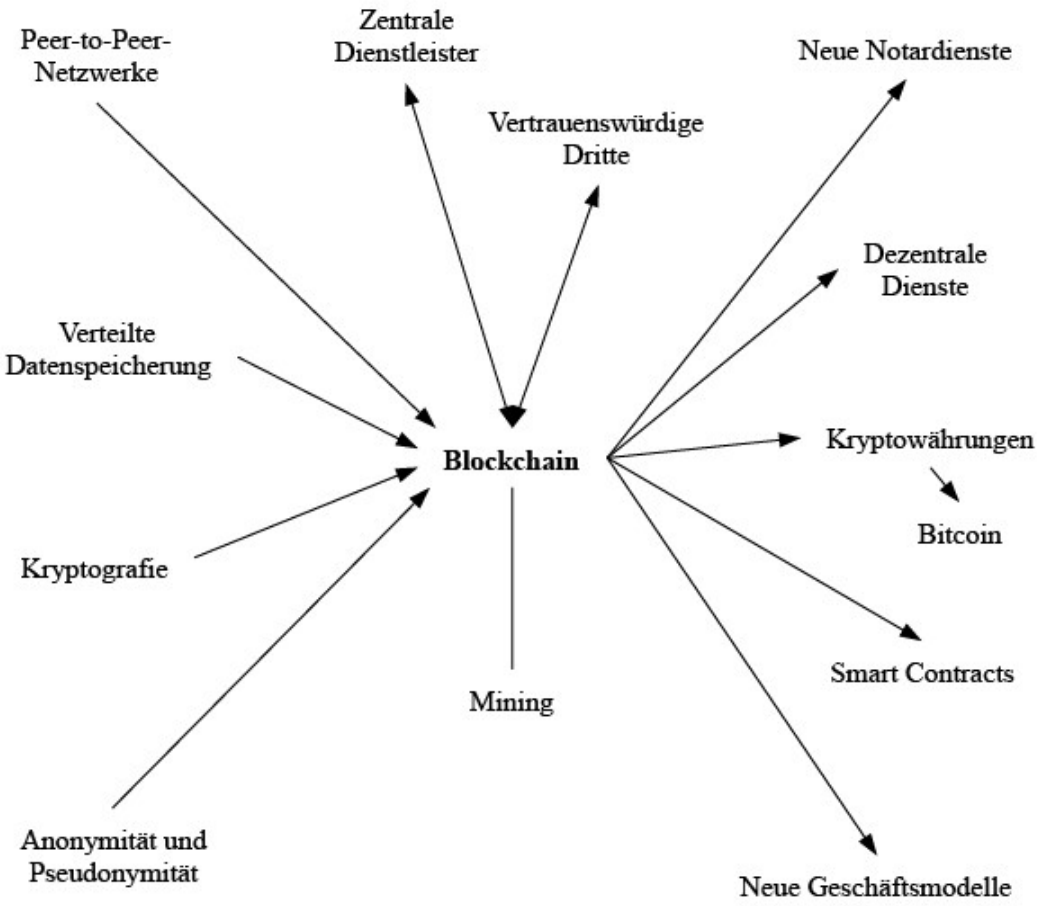
Als im Jahr 2008 eine internationale Finanzkrise die Welt zu erschüttern beginnt, wird deutlich, wie abhängig die Wirtschaft von Banken als systemrelevanten Institutionen ist. In dieser Zeit entsteht die Idee einer Kryptowährung namens Bitcoin, die völlig ohne zentrale Institutionen auskommt (siehe Selbstorganisation). Die Herausforderung eines solchen Systems besteht darin, Werttransfers zwischen unbekannten Akteuren abzusichern, ohne dabei auf einen Dritten bspw. eine Bank angewiesen zu sein (siehe Mobile Money). Dazu wurde ein komplexes Verfahren bestehend aus kryptografischen Funktionen und verteilter Datenspeicherung entworfen. In der sogenannten Blockchain werden Transaktionen unveränderbar und für alle nachvollziehbar abgespeichert.
Die Besonderheit des Blockchain-Protokolls liegt darin, eine nachweisbare, transparente Transaktionsabsicherung zwischen unbekannten Parteien ohne zentrale Instanzen zu ermöglichen. Dies wird durch drei Mechanismen erreicht: (1) Ein Anreizsystem, wird so gestaltet, dass jeder Teilnehmer im eigenen Interesse für ein funktionierendes Gesamtsystem sorgt. (2) Die Transaktionen sind transparent. Alle jemals durchgeführten Transaktionen werden in einem Register gespeichert, das an alle Teilnehmer einer Blockchain über ein Peer-to-Peer-Netzwerk verteilt wird und für jeden einsehbar ist. Damit können alle Transaktionen bis zu ihrem Ursprung zurückverfolgt werden. Das Register ist in einzelne Blöcke unterteilt, in denen die Transaktionen gespeichert und validiert werden können. (3) Über kryptografische Funktionen sind die Blöcke untrennbar miteinander verkettet. Das Register wird daher auch Blockchain genannt. Die Blöcke enthalten neben einer oder mehreren Transaktionen auch eine Zusammenfassung aller vorherigen Blöcke in Form eines Hash-Wertes. Der Hash-Wert dient der Fälschungssicherheit. Mit ihm kann jeder die

Echtheit einer Transaktionskette überprüfen. Bei einer Manipulation würde der Hash-Wert nicht mehr stimmen (siehe Security by Design). Darüber hinaus können die Blöcke um weitere Informationen ergänzt werden, was zusätzliche Anwendungsfälle ermöglicht. Jeder darf neue Einträge zur Blockchain hinzufügen, bestehende Einträge sind jedoch schreibgeschützt und können nachträglich nicht verändert werden.

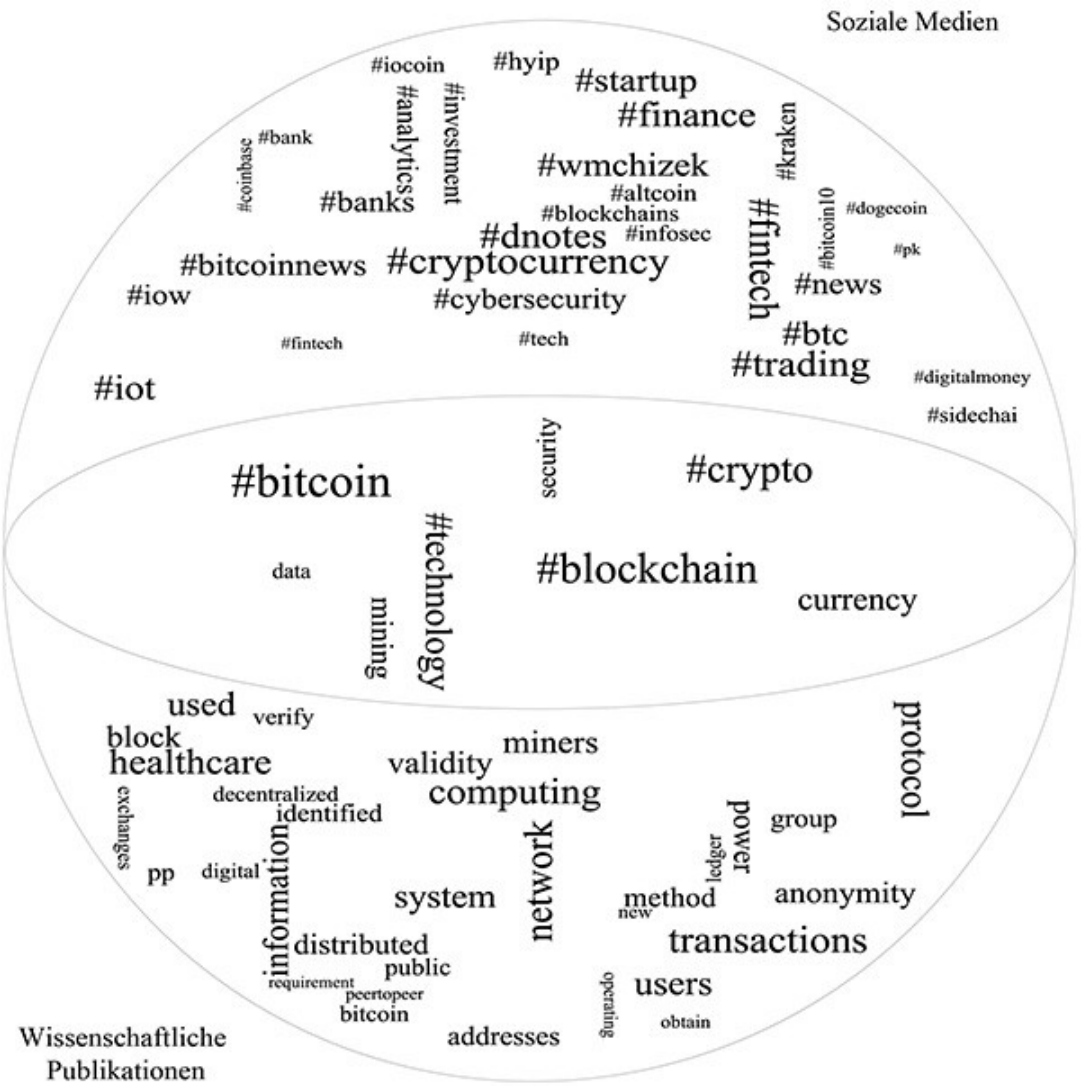
Transparenz und Anonymität

Um Transaktionen durchführen zu können, erhält jeder Teilnehmer der Blockchain einen privaten und einen öffentlichen Schlüssel. Der öffentliche Schlüssel stellt eine eindeutige Adresse (eine Art Kontonummer) dar, die als Empfangsadresse für eingehende Transaktionen verwendet wird. Der private Schlüssel muss geheim gehalten werden; mit ihm werden ausgehende Transaktionen bestätigt. Für eine Transaktion muss der Sender lediglich den öffentlichen Schlüssel des Empfängers angeben sowie über die notwendigen privaten Schlüssel für die zu transferierenden Einheiten verfügen. Da für eine Transaktion keine weiteren Informationen benötigt werden, müssen die Teilnehmer nicht mit ihren Klarnamen oder einer geprüften Identität auftreten. Die Blockchain erlaubt damit nicht nur Transparenz, sondern auch ein hohes Maß an Anonymität – ein Umstand, der zumindest virtuelle Währungen auch für kriminelle Akteure interessant macht (siehe Darknet).
Die Blöcke der Blockchain müssen eine bestimmte Struktur aufweisen, die in aufwendigen Rechenoperationen generiert wird. Grundsätzlich kann jeder mit seiner Rechenleistung dazu beitragen, neue passende Blöcke zu finden und als sogenannter Miner auftreten. Für ihre Arbeit werden die Miner mit Transaktionsgebühren oder anderen Anreizen entlohnt. Alle Miner konkurrieren darum, neue Blöcke zu finden, wodurch das System am Leben erhalten wird. Der Aufwand neue Blöcke zu finden steigt mit der im Netzwerk verfügbaren Rechenleistung. Für einige Blockchains ist die Erstellung neuer Blöcke inzwischen zu einem eigenständigen Geschäftsmodell geworden. Im Handel gibt es spezielle Hardware, die explizit für die aufwendige Berechnung der Blöcke konzipiert ist.

Begriffliche Verortung



Netzwerkartige Verortung des Themenfeldes



Gesellschaftliche und wissenschaftliche Verortung

Vielfältige Anwendungsgebiete

Im Ergebnis ist die Blockchain eine verteilte Datenbank. Verteilte Datenbanken sind nicht neu und es gibt bereits weitaus performantere Lösungen. Was Blockchain innovativ macht, sind vielmehr die Mechanismen, die Einvernehmen über geschäftliche Transaktionen zwischen unbekannten Akteuren herstellen. Diese Fähigkeit wird erreicht durch komplexe Rechenoperationen und damit einhergehend hohem Stromverbrauch für die Erzeugung neuer Blöcke. Das Konzept geht von dem

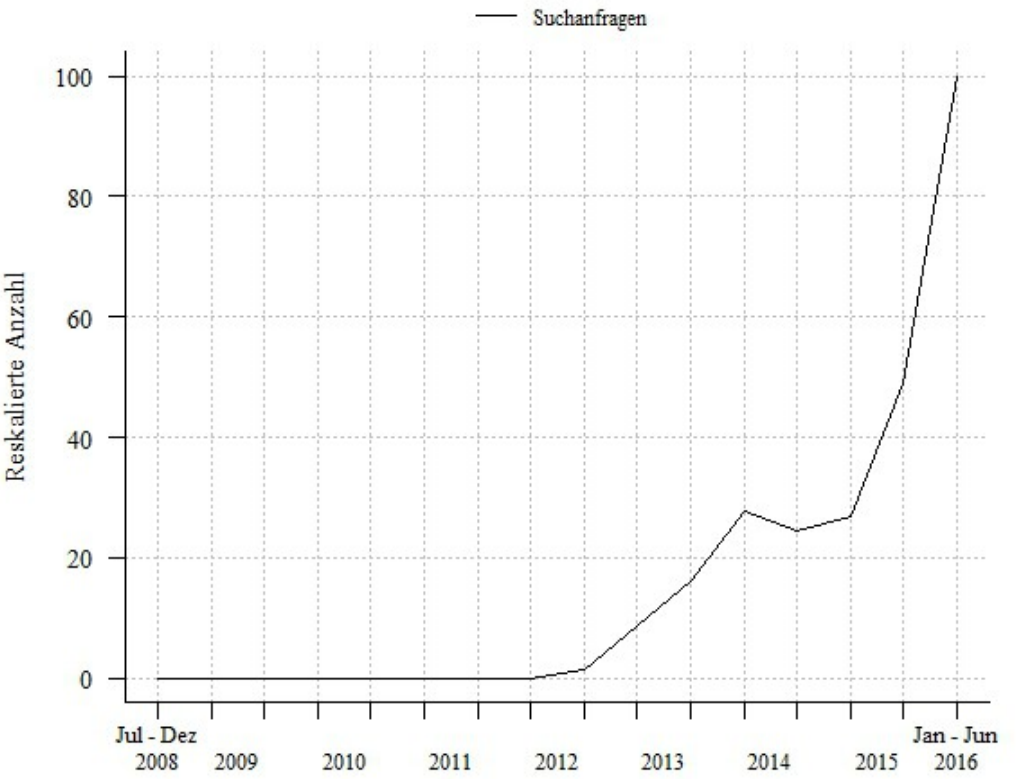
Grundprinzip aus, dass die Mehrheit der Rechenleistung über die Vertrauenswürdigkeit einer Blockchain entscheidet. Betreiber großer Rechenzentren, Cloud-Anbieter oder auch Botnetz-Betreiber haben daher einen klaren Vorteil. Damit ein Teilnehmer nicht die Hoheit über eine Blockchain erhält, ist es entscheidend, dass die Mehrheit der Rechenleistung auf mehrere Parteien verteilt ist. Je weniger Parteien ein Blockchain-Netzwerk hat, desto leichter ist es angreifbar – ein Problem, das vor allem neue Blockchain-Projekte betrifft.
Die Fähigkeit der dezentralen Konsensbildung macht das Konzept der Blockchain dennoch über den Finanzsektor hinaus für eine Vielzahl weiterer Anwendungsfälle interessant. Überall dort, wo zentrale Dienstleister oder Vermittler benötigt werden, kann die Blockchain eine Alternative darstellen. Dies gilt beispielsweise für viele Leistungen von Notaren oder Treuhändern (siehe Digitaler Nachlass). So könnten Eigentumsübertragungen oder auch Sportwetten nachvollziehbar in einer Blockchain abgebildet werden. Weitere Vorhaben realisieren mit der Technologie dezentrale soziale Netzwerke, die ohne ein Unternehmen als Betreiber fungieren. Darüber hinaus existieren Ideen, die Blockchain-Technologie für die automatisierte Einhaltung von Verträgen (sogenannte Smart Contracts) zu nutzen. In den Blöcken wird dann neben Transaktionen auch der Vertragsstatus gespeichert. Ein anderes Projekt wiederum will Grundbücher in einer Blockchain abbilden, um dadurch Korruption zu erschweren.

Wird die Blockchain überschätzt?

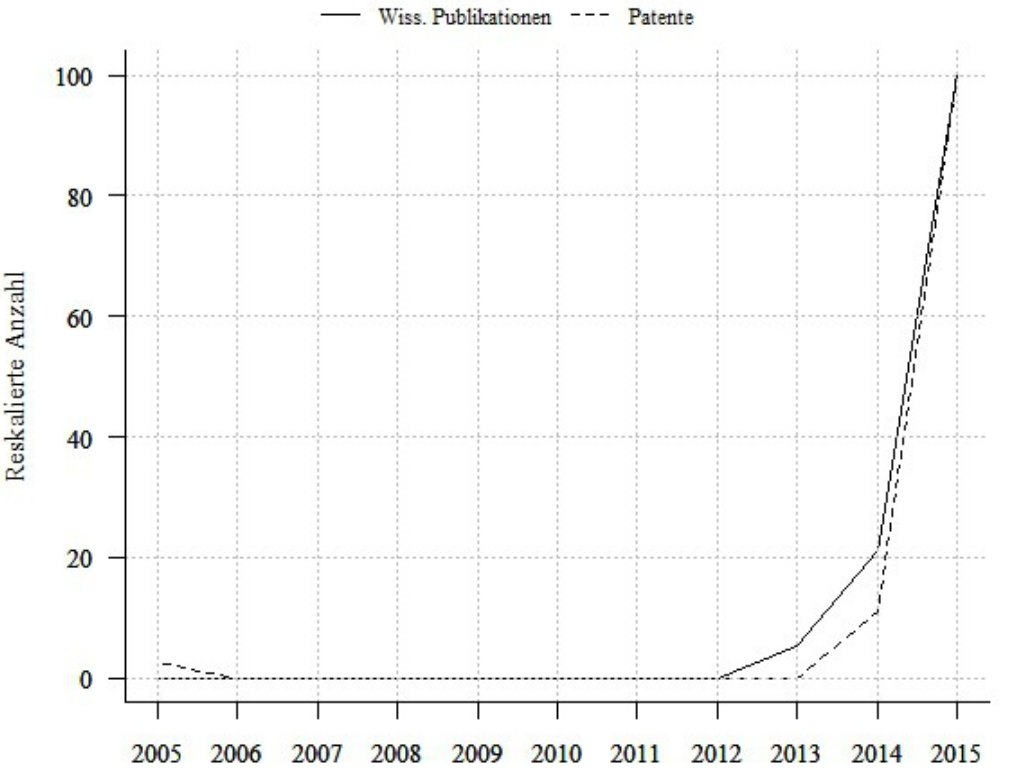
Das Potenzial der Blockchain-Technologie ist aus heutiger Perspektive noch schwer abzusehen. Schätzungen zufolge sind bereits mehr als 1 Milliarde US-Dollar Investitionen in die Technologie geflossen. Bei all diesen Ideen müssen jedoch die besonderen Anforderungen der Blockchain betrachtet werden. Jede Blockchain benötigt ein geeignetes Anreizsystem, das zum einen zur Teilnahme motiviert und Systemvertrauen schafft, zum anderen eine Manipulation des Gesamtsystems unattraktiv macht. Außerdem ist eine kritische Masse an Teilnehmern notwendig, damit eine Partei nicht mehr als die Hälfte der Rechenleistung auf sich vereinen kann. Da eine zentrale Steuerungsinstanz fehlt, sind nachträgliche Änderungen oder Erweiterungen der technischen Protokolle sehr aufwendig und bedürfen im Zweifelsfall der Mitwirkung aller Teilnehmer. Nicht zuletzt muss die Sicherheit der kryptografischen Protokolle dauerhaft gewährleistet werden.
Auch wenn sich viele der heutigen Ideen am Markt nicht durchsetzen sollten, so stellt der Ansatz der dezentralen Vertrauensbildung doch eine interessante Alternative zu herkömmlichen vertrauensbildenden Instanzen dar. Die dahinter liegende Frage lautet: Schafft die Technologie durch mehr Transparenz und Unabhängigkeit von Intermediären, insbesondere staatlichen oder zumindest staatlich legitimierten Zentralinstanzen, auch ein Mehr an Freiheit für jeden Einzelnen? Oder geben wir damit noch ein Stück Kontrolle an komplexe

Algorithmen (siehe Denkende Maschinen) ab, die unsere Daten und Eigentumswerte verwalten?

Themenkonjunkturen



Suchanfragen für »Blockchain«



Wissenschaftliche Publikationen und Patentanmeldungen

Folgenabschätzung

Möglichkeiten

- Dezentrale Konsensbildung ohne Vermittler
- Direkte Durchführung von Transaktionen
- Verstärkte anonyme bzw. pseudonyme Nutzung von Diensten
- Erhöhte Transparenz und damit einhergehend Erschweren von Willkür
- Erhöhte Fälschungssicherheit durch nachvollziehbare Produktionsketten
- Kontrollmöglichkeit von Transfers innerhalb des Systems

Wagnisse

- Regulierung wird erschwert, da keine zentralen Adressaten vorhanden sind

(beispielsweise Einzug der Quellensteuer durch Banken)
- Starke Abhängigkeit von der dauerhaften Vertrauenswürdigkeit kryptografischer Funktionen
- Einflussnahme durch massive Rechenkapazität möglich
- Steigender Energieverbrauch für die Berechnung neuer Blöcke
- Dauerhaftes Anreizsystem notwendig, um Blockchain-Infrastruktur lauffähig zu halten

Handlungsräume

Entwicklung beobachten

Noch ist die Wirkungsentfaltung der Blockchain-Technologie nicht absehbar. Durch die Befassung mit der neuen Technologie und die Beobachtung der weiteren Entwicklung können disruptive Veränderungspotenziale frühzeitig erkannt werden. Auch die eigene Anwendung sollte dabei im Blick bleiben: in Großbritannien werden bspw. bereits Anwendungsfelder für die Verwaltung untersucht.

Staatliche Einflussmöglichkeiten bewahren

Damit der Staat seine Funktion als Rahmengeber wahrnehmen kann, sollte er die Blockchain-Technologie nicht nur beobachten, sondern auch aktiv begleiten. Die Eigenschaften der pseudonymen Nutzung und das Fehlen eines zentralen Ansprechpartners erschweren die Regulierung systemrelevanter Dienste schwierig.

Lösung für spezielle Infrastruktur-Probleme

Blockchain-Anwendungen können eine Alternative zu zentralen Institutionen darstellen. Fehlen erforderliche Institutionen in Ländern oder Sektoren, lassen sich so tragfähige, dezentrale Strukturen aufbauen. Durch die erhöhte Transparenz kann auch Korruption erschwert werden. Einzige Voraussetzung ist ein Internetzugang für die Betroffenen.