ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 3:

Kryptowährung

Stand: Juli 2016

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, Michael Rothe, Oliver Schmidt, Nicole Opiela, Florian Friederici, Jan Gottschick, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen:
Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Juli 2016

Autorinnen/Autoren:
Petra Hoepner et al.

Bibliographische Angabe:
Petra Hoepner et al. 2019, Kryptowährung, 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/-/kryptowahrung

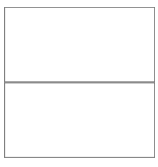
Kryptowährung

In den vergangenen Jahren hat sich eine Vielzahl virtueller Währungen zunächst mit der Zielsetzung entwickelt, einfaches Bezahlen online zu ermöglichen. Aber auch Ingame-Währungen als geldwerte Tauschmittel in Spielen sind entstanden. Für Kryptowährungen, bei denen der Prozess der Geldschöpfung und der Zahlungsverkehr auf kryptographischen Algorithmen beruhen, lässt sich inzwischen ein Prozess der Etablierung beobachten. Kryptowährungen kommen ohne zentrale Ausgabestelle aus. Nicht Zentralbanken, sondern Algorithmen und deren Anwendung bestimmen die verfügbare Geldmenge. Große Kursschwankungen zu gesetzlichen Zahlungsmitteln laden dabei zu Spekulationen ein. Die hohe Volatilität zeigt sich etwa bei Bitcoins als bekanntestem Vertreter.

Virtuelle Währung

Schon in den 80er Jahren wurde die Idee geboren, ebenso wie mit Bargeld auch digital anonym bezahlen zu können. Elektronisches Geld entstand. Der Kunde musste bei einer lizenzierten Bank ein entsprechendes Konto eröffnen, das mit einem klassischen Bankkonto verbunden wurde. Kryptowährungen benötigen weder Kreditinstitut noch Bankkonto. Die Idee einer kryptographischen, virtuellen Währung wurde im Jahre 2008 veröffentlicht. Basierend auf dieser Idee entstand das Bitcoin-Netzwerk am 3. Januar 2009 mit der Berechnung des ersten sogenannten Blocks mit den ersten 50 Bitcoins. Neben Bitcoin existieren derzeit unzählige weitere Kryptowährungen wie Ripple, Litecoin, Peercoin, Dogecoin – und die Dynamik ist enorm. Das Schaffen einer eigenen Währung wird inzwischen als Webdienst auf einschlägigen Seiten angeboten.
Die Spezifikationen und Methoden für die Generierung von Coins sind ähnlich, unterscheiden sich aber in Details. Allen Kryptowährungen liegen kryptographische Operationen zugrunde. Jeder Teilnehmer kann ein oder mehrere Schlüsselpaare mit jeweils einem öffentlichen und einem privaten Schlüssel erzeugen. Mit dem öffentlichen Schlüssel kann man am Zahlungsverkehr teilnehmen; dieser fungiert als Pseudonym des Teilnehmers. Mit dem geheimen, privaten Schlüssel wird eine Zahlung autorisiert. Virtuelles Geld wird direkt zwischen den Teilnehmern transferiert. Die Gemeinschaft aller Beteiligten bildet ein dezentrales Peer-to-Peer-Netzwerk, das Transaktionen automatisch überwacht (siehe Selbstorganisation). Bei der von Bitcoin umgesetzten Lösung wird beispielsweise jede Transaktion in der Bitcoin-Datenbank festgehalten. Jeder Teilnehmer kann die gesamte Datenbank herunterladen. Durch diese Überprüfung können doppelte Coin-Ausgaben verhindert werden.

Begriffliche Verortung

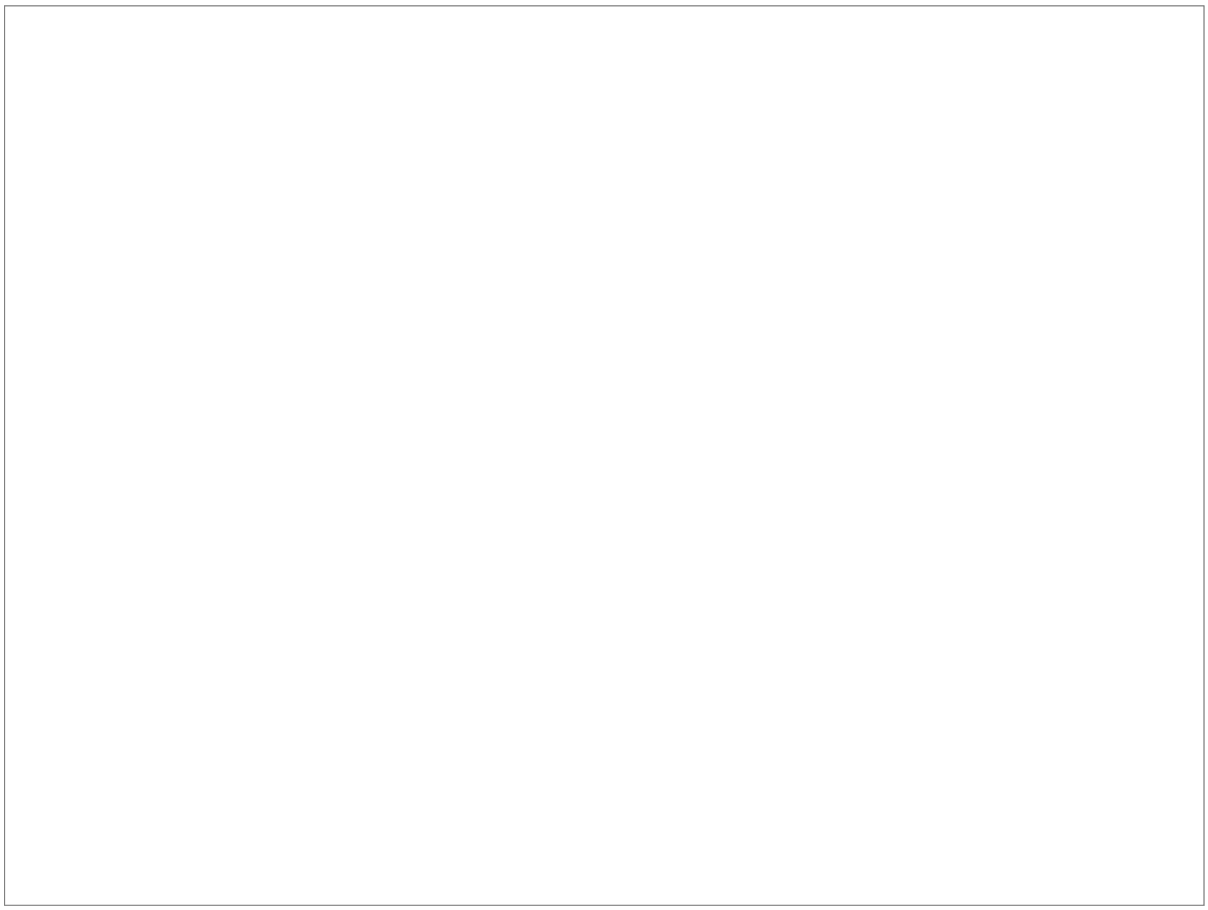


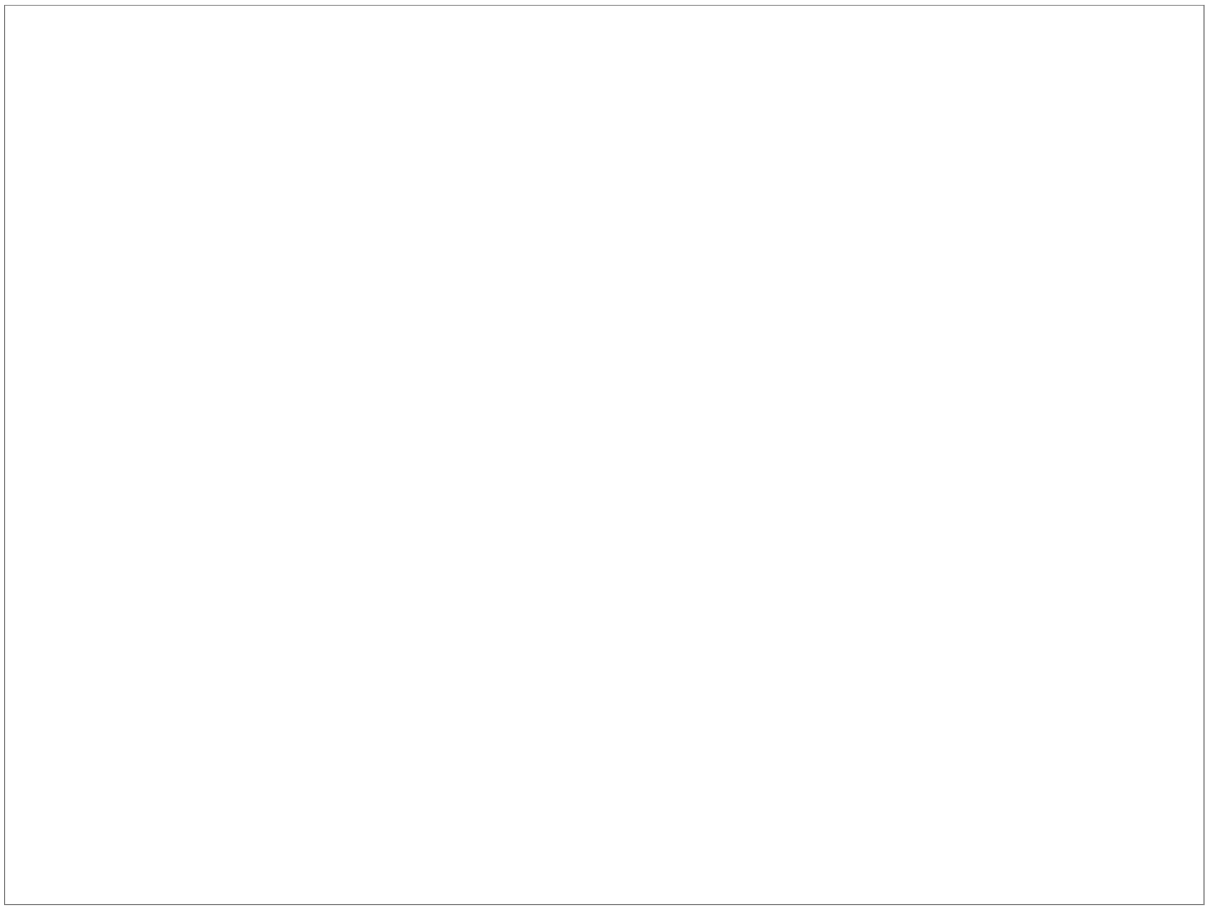
Weder Geld noch E-Geld

Neben dem Zahlungsverkehr ist die Geldschöpfung mit komplexen Rechenoperationen eine weitere kryptographische Operation, die theoretisch jeder ausführen kann, der eine geeignete Hardware besitzt. Dieses Generieren bezeichnet man auch als Mining respektive als Schürfen. Die Gesamtmenge ist dabei endlich. Kryptowährungen werden in virtuellen Geldbörsen, sogenannten Wallets, aufbewahrt. Die Wallets können sich auf dem Desktop, Handy oder im Web befinden. Wallets müssen aber gegen Verlust durch Ausspähen und Schadsoftware geschützt werden. Der Besitz von Geldeinheiten wird durch den

Besitz der kryptographischen Schlüssel nachgewiesen. Wichtig ist, dass man seine privaten Schlüssel nicht verliert, denn dann ist das virtuelle Geld auch für immer verloren. Kryptowährungen werden von der Bundesanstalt für Finanzdienstleistungsaufsicht als Rechnungseinheit behandelt, sind also weder Geld noch E-Geld. An Online-Börsen können diese Rechnungseinheiten mit Geld als gesetzlichem Zahlungsmittel ge- und verkauft werden. Inzwischen nutzen auch Banken Kyptowährungen und die dahinter liegende Blockchain-Technologie für weltweite Finanztransaktionen und als Verrechnungseinheit.
Je nach eingenommener Perspektive kommt Kryptowährungen eine höchst unterschiedliche gesellschaftliche Bedeutung zu. Als Rechnungseinheiten dienen sie lediglich der medienbruchfreien Abwicklung von Online-Zahlungsvorgängen (siehe Mobile Money). Als vollwertiger Währungsersatz wird ihnen demgegenüber mitunter das Potenzial zugeschrieben, das Wirtschaftssystem durch die Entkoppelung von traditionellen Finanzmärkten bei gleichzeitiger Nachvollziehbarkeit von Zahlungsvorgängen maßgeblich korrigieren zu können. Perspektivenübergreifend zeigt sich, dass mit dem Schürfen von Coins, die keine Entsprechung in gesetzlichen Zahlungsmitteln mehr haben müssen, vormals staatliche Aufgaben von privaten Akteuren wahrgenommen werden. Diese Funktionsübertragung wird von großen Kursschwankungen, Geldwäschevorwürfen (siehe Darknet), der Insolvenz der Bitcoin-Börse Mt. Gox (2014) und dem Entwenden oder Verschwinden von mehrstelligen Millionenbeträgen anderer Bitcoin-Börsen wie MyCoin und Bitstamp (2015) begleitet. Zunehmend stellt sich die Frage, ob sich daraus ein Regulierungserfordernis ergibt. Die Bestrebungen, Kryptowährungen für das etablierte Bankensystem nutzbar zu machen, deuten dabei allerdings auf eine Bändigung der zwischenzeitlich zugeschriebenen, disruptiven Wirkungen für Finanzsystem, Bankenaufsicht und Weltwirtschaft.

Themenkonjunkturen





Folgenabschätzung

Möglichkeiten

- Unabhängigkeit von internationaler und nationaler Finanzmarktpolitik, Banken, Zahlungsdienstleistern und staatlichen Währungen
- Geringe Gebühren für Zahlungen
- Beglaubigte Zahlungen sind im Gegensatz zu anderen elektronischen Zahlungsdiensten nicht mehr rückholbar, Betrugsrisiko wird gesenkt
- Nicht anonym, aber hoher Schutz der Privatsphäre

Wagnisse

- Hoher Schutzbedarf für private Schlüssel, da diese Eigentum an Währungseinheiten nachweisen
- Gefahr von irreversiblen Verlusten durch Malware, Datenverlust, Einbrüchen, Softwarefehlern oder Betrug nach dem Schneeballsystem
- Große Kursschwankungen mit unklarer Perspektive
- Möglichkeiten zu Geldwäsche und Steuerentzug
- Kein gesetzliches Zahlungsmittel, eine Einlagensicherung existiert nicht

Handlungsräume

Betrug und Geldwäsche verhindern

Gesetzliche Regelungen und Sicherheitskontrollen bei Kryptowährungen und Tauschbörsen können wie bei herkömmlichen Banken für mehr Sicherheit sorgen und Geldwäsche verhindern.

Steuern erheben

In Deutschland müssen Spekulationsgewinne aus dem Handel mit virtuellen Währungen bereits versteuert werden, wenn weniger als ein Jahr zwischen Kauf und Verkauf liegt. Weitere Steuern sind in anderen Ländern in Diskussion, beispielsweise der Einzug der Umsatzsteuer.

Vertrauen stärken durch Kontrollmechanismen und Qualitätsstandards

Um Bürger und Unternehmen zu schützen und trotzdem virtuelle Währungen zuzulassen, sollten geeignete Kontrollmechanismen und Qualitätsstandards international etabliert werden.