Brühl, Volker

Article

Bitcoins, Blockchain und Distributed Ledgers: Funktionsweise, Marktentwicklungen und Zukunftsperspektiven

Wirtschaftsdienst

Suggested Citation: Brühl, Volker (2017) : Bitcoins, Blockchain und Distributed Ledgers: Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, Wirtschaftsdienst, ISSN 1613-978X, Springer, Heidelberg, Vol. 97, Iss. 2, pp. 135-142, http://dx.doi.org/10.1007/s10273-017-2096-3

This Version is available at:
http://hdl.handle.net/10419/196496

DOI: 10.1007/s10273-017-2096-3

Volker Brühl

Bitcoins, Blockchain und Distributed Ledgers

Funktionsweise, Marktentwicklungen und Zukunftsperspektiven

Virtuelle Währungen wie Bitcoins geraten zunehmend in den Blickpunkt des öffentlichen Interesses. Sie funktionieren auf Basis der Blockchain- bzw. Distributed-Ledger-Technologie. Volker Brühl erläutert ihre Funktionsweise und zeigt auf, dass diese Technologien nicht nur den Finanzsektor revolutionieren können.

Bitcoins und andere sogenannte virtuelle Währungen oder Kryptowährungen geraten vermehrt ins Visier von Aufsichtsbehörden, da diese anonym verwahrt, übertragen oder in klassische Währungen getauscht werden können und damit im Verdacht stehen, Geldwäsche als Folge illegaler Transaktionen zu erleichtern. Die Europäische Bankenaufsichtsbehörde (EBA) hat wiederholt auf die Risiken von Kryptowährungen hingewiesen.[1] Am 20. Mai 2015 wurde die vierte europäische Geldwäscherichtlinie (EU 2015/849) verabschiedet, die zunächst virtuelle Währungen nicht erfasst hat. Die EU-Kommission hat jedoch am 5. Juli 2016 vorgeschlagen, künftig auch die Betreiber von Umtauschplattformen und Anbieter von elektronischen Geldbörsen für virtuelle Währungen in die Regelungen der 4. Geldwäscherichtlinie einzubeziehen. Dadurch würde die bisherige Anonymität der Nutzer virtueller Zahlungsmittel weitgehend entfallen. Die nunmehr kurzfristig angeregte Erweiterung der 4. Geldwäscherichtlinie verdeutlicht einerseits, wie hoch der Handlungsbedarf auf politischer Seite eingeschätzt wird.[2] Andererseits befürchten Kritiker, dass durch eine strengere Regulierung von Kryptowährungen die Entwicklung eines innovativen Marktsegmentes in Europa gefährdet wird.

Die den Bitcoins und den meisten anderen Kryptowährungen zugrunde liegende Blockchain-Technologie, die auf dem Prinzip eines verteilten Hauptbuches mit Transaktionskonten (Distributed Ledger) beruht, wird das Potenzial zugeschrieben, nicht nur den Finanzsektor zu revolutionieren, sondern auch in anderen Branchen disruptive Veränderungen auslösen zu können. In der öffentlichen Diskussion werden häufig Bitcoins, Blockchain und Distributed Ledgers nicht ausreichend differenziert. Daher sollen im Folgenden zunächst Funktionsweise, Marktentwicklungen und das Ökosystem virtueller Währungen am Beispiel der Bitcoins erläutert werden. Anschließend werden die potenziellen Anwendungsfelder der Distributed-Ledger-Technologie skizziert.

Bitcoins und Blockchain im Überblick

Die Blockchain-Technologie wurde ursprünglich als Plattform für die Einführung von sogenannten „virtuellen Währungen“ entwickelt. Bei Bitcoins oder anderen Kryptowährungen handelt es sich nicht um Geld, sondern um Verrechnungseinheiten, die aufgrund privatrechtlicher Vereinbarungen als Zahlungsmittel in multilateralen Verrechnungskreisen eingesetzt werden können, ohne dass es dafür einer Genehmigung der Aufsichtsbehörden bedarf. Erweiterte Dienstleistungen wie z.B. die Vermittlung von An- und Verkäufen oder der Betrieb von Handelsplattformen können jedoch der Genehmigungspflicht unterliegen.[3]

Bei Kryptowährungen werden die elektronischen Zahlungen direkt zwischen Sendern und Empfängern abgewickelt, ohne dass es eines Finanzintermediärs (z.B. einer Bank) bedarf. Diese webbasierten Zahlungsverkehrssysteme verwenden Methoden der Kryptographie (Verschlüsselungstechnik), um mit Hilfe eines verteilten Rechnernetzwerks (sogenannte Peer-to-Peer-Netzwerke) sicher und kostengünstig Transaktionen abwickeln zu können. Obwohl sich die Algorithmen der jeweiligen Kryptowährungen in vielen Details unterscheiden, basieren die Transaktions-

1 Vgl. Europäische Bankenaufsichtsbehörde (EBA): Opinion on „virtual currencies“, Paris 2014.

2 Vgl. European Commission – Fact Sheet, Questions and Answers: Anti-money Laundering Directive, Straßburg, 5.7.2016.

3 Vgl. J. Münzer: Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, in: BaFin Journal, Nr. 1/2014.

Prof. Dr. Volker Brühl ist Geschäftsführer am Center for Financial Studies an der Goethe Universität in Frankfurt am Main.

prozesse weitgehend auf ähnlichen Grundprinzipien, die nachfolgend am Beispiel Bitcoin erläutert werden.

Bitcoin ist die erste und bislang am weitesten verbreitete Kryptowährung. Die dazu gehörige Referenz-Software wurde 2009 veröffentlicht.[4] Alle Transaktionen mit Bitcoins werden in einer verteilten Datenbank abgebildet und so zu Blöcken zusammengefasst und miteinander verknüpft, dass eine lückenlose und fälschungssichere Abfolge von Transaktionsblöcken (die sogenannte Blockchain) entsteht. Für jeden Teilnehmer des Netzwerks sind sämtliche Transaktionen der Blockchain einsehbar. Allerdings ist für Außenstehende nicht erkennbar, welche Personen tatsächlich Inhaber der virtuellen Geldeinheiten sind. Einmal getätigte Transaktionen sind irreversibel. Bitcoins werden nicht in einem klassischen Geldschöpfungsprozess durch das Zusammenwirken von geldpolitischen Instrumenten der Zentralbanken, Geschäftsbanken und Bankkunden erzeugt, sondern mit Hilfe eines definierten Anreizsystems, das diejenigen Teilnehmer des Zahlungsnetzwerks mit neuen Geldeinheiten belohnt, die besonders schnell die Authentizität von verschlüsselten Transaktionen mit Hilfe von mathematischen Algorithmen prüfen. Diesen Prozess der Validierung und damit einhergehenden Erzeugung neuer Einheiten an Kryptowährungen bezeichnet man als Mining. Bitcoins und andere Kryptowährungen beruhen also auf dem Vertrauen der Teilnehmer in die Integrität und Sicherheit eines dezentralen Computernetzwerks und nicht auf der Glaubwürdigkeit einer Notenbank. Während in klassischen Währungssystemen weder das Zentralbankgeld noch die Buchgeldschöpfung einer mengenmäßigen Begrenzung unterliegen, ist die Zahl der maximal erzeugbaren Einheiten an Kunstwährungen in der Regel systemimmanent begrenzt.

Ablauf einer Bitcoin-Transaktion

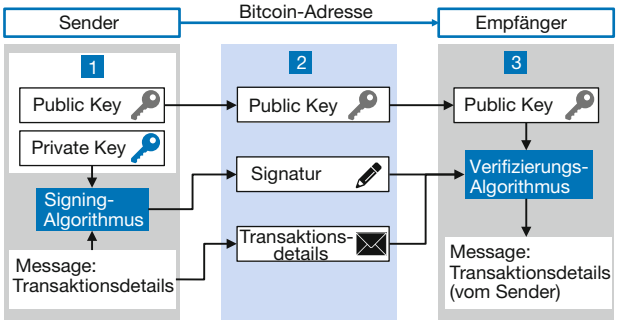
Jeder Teilnehmer am Bitcoin-Netzwerk muss über eine entsprechende Software (Wallet) verfügen, die Zugang zur Bitcoin-Referenz-Software bietet sowie die Durchführung von Transaktionen ermöglicht. Es gibt eine Vielzahl unterschiedlicher Wallet-Lösungen, die sich vor allem dadurch unterscheiden, ob sie nur die Basisfunktion zur Verwaltung von Bitcoin-Adressen und den eigenen Transaktionen ermöglichen oder ob sie den Nutzer in die Lage versetzen, einen vollständigen Bitcoin-Klienten zu replizieren. Abbildung 1 verdeutlicht den prinzipiellen Ablauf einer bilateralen Bitcoin-Transaktion.

1. Der Sender erzeugt zunächst ein „Schlüsselpaar“, das aus einem privaten (Private Key) und einem öffentlichen Schlüssel (Public Key) besteht. Der Private Key dient dem Sender zur Erzeugung einer verschlüsselten Signatur, der Public Key dient dem Empfänger und dem gesamten Bitcoin-Netzwerk dazu, die Signatur zu verifizieren und damit die Legitimität des Senders zu prüfen. Zur Übertragung von Bitcoins benötigt man die Bitcoin-Adresse des Empfängers. Bitcoin-Adressen sind bis zu 34-stellige Zeichenkombinationen, die mit Hilfe kryptografischer Verfahren erzeugt werden. Anders als bei Konten werden Bitcoin-Adressen aus Sicherheitsgründen in der Regel nur einmal für eine Transaktion verwendet.

2. Anschließend generiert der Sender von Bitcoins eine Transaktion, die nach einem festgelegten Format erzeugt werden muss und neben der Zieladresse unter anderem den Betrag sowie die Transaktionsreferenzen auf alle diejenigen vorherigen Bitcoin-Transaktionen enthält, die den Sender als rechtmäßigen Verfügungsberechtigen der nun zu verausgabenden Bitcoins ausweist. Anschließend erzeugt der Private Key mit einem Signierungsalgorithmus eine Signatur der Daten, die dann verschlüsselt zusammen mit dem Public Key über das Bitcoin-Netzwerk an den Empfänger versendet werden.

3. Der Empfänger kann nun mit dem Public Key des Senders die Transaktion verifizieren, d.h. prüfen, ob der Sender tatsächlich die Bitcoins an den Empfänger gesendet hat und dieser selbst berechtigter Inhaber dieser Bitcoins ist. Denn die Signatur kann nur vom Inhaber des Private Keys erzeugt worden sein, der zum gesendeten Public Key passt.

Abbildung 1
Ablauf einer Bitcoin-Transaktion



Quelle: eigene Darstellung in Anlehnung an CryptoCompare.com.

Das Prinzip der Blockchain

Parallel werden neue Transaktionen an alle Netzknoten versendet, die ihrerseits die Validität der Transaktionen

4 S. Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, White Paper, 2008.

dezentral prüfen und gegebenenfalls versuchen, diese zu einem neuen Block zusammenzufassen und der Blockchain hinzuzufügen. Um sicherzustellen, dass sämtliche Netzwerkknoten immer den gleichen Stand der Blockchain haben und einen Anreiz erhalten, die Validität der einzelnen Transaktionen und letztlich der Blockchain insgesamt kontinuierlich zu verifizieren, bedarf es eines Anreizsystems zur Generierung neuer Blöcke. Dies erfolgt mit Hilfe des sogenannten Miningprozesses, der vorsieht, dass zur Erzeugung eines neuen Blockes ein mathematisches Problem zu lösen ist.

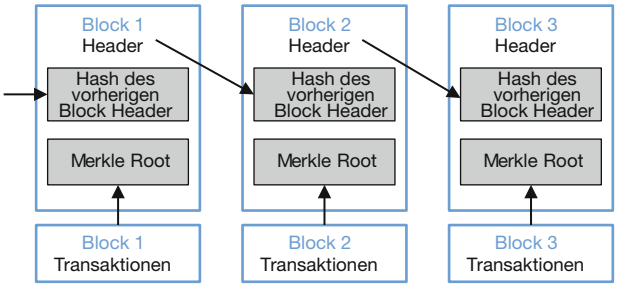
Um einen neuen Block zu erzeugen, muss ein mit einer kryptografischen Funktion erzeugter Verschlüsselungswert (sogenannter Hashwert) des „Blockheaders" erzeugt werden, der einen bestimmten Zielwert unterschreitet.

Abbildung 2 zeigt eine vereinfachte Darstellung der Blockchain. Jeder Block verfügt über einen eigenen Verschlüsselungswert, der sich aus den Verschlüsselungswerten der einzelnen Transaktionen im Block sowie der Referenz zum vorherigen Block ergibt. Dadurch entsteht eine lineare Verkettung der Blöcke zu einer Blockchain. Die jeweiligen Hashwerte werden durch sogenannte Hashfunktionen generiert, mit denen beliebige Zeichenfolgen nach vordefinierten Algorithmen in scheinbar zufällige Zeichenfolgen transformiert werden. Eine beliebte Hashfunktion, die auch das Bitcoin-System verwendet, ist die Funktion SHA 256, deren Output aus Hexadezimalfolgen mit einer Länge von 256 Bits besteht.[5] Bereits kleinere Änderungen der Ausgangsdaten führen zu nicht vorhersehbaren Änderungen der Output-Daten.

Jeder Block enthält mehrere neue Transaktionen, die im Transaktionsteil des Blocks gespeichert sind. Anschließend werden Kopien der Transaktionen zuerst einzeln und dann paarweise so lange verschlüsselt, also „gehasht", bis ein einzelner Hashwert verbleibt. Dieser wird auch als „Merkle Root" des aus den Transaktionen bestehenden „Merkle Trees" bezeichnet. Die Merkle Root ist im Blockheader gespeichert. Der Blockheader enthält außerdem den Hashwert des vorherigen Blockheaders sowie ein dezidiertes Feld NONCE (Number Only Used Once). Die Miner müssen nun durch einen algorithmischen Suchprozess solange Zufallszahlen für das NONCE-Feld suchen, bis die geforderte Zielgröße für den Hashwert des neuen Blocks unterschritten ist. NONCE können nur einmalig verwendet werden, um künftige Fälschungen zu erschweren. Diesen Vorgang bezeichnet man als Proof-of-Work, da die erfolgreiche Generierung eines zielkonformen Hashwertes den Einsatz entsprechender Rechnerkapazitäten erfordert und damit Kosten verursacht.

5 SHA steht für Secure Hash Algorithm.

Abbildung 2
Das Prinzip der Blockchain



Quelle: Bitcoin Developer Guide.

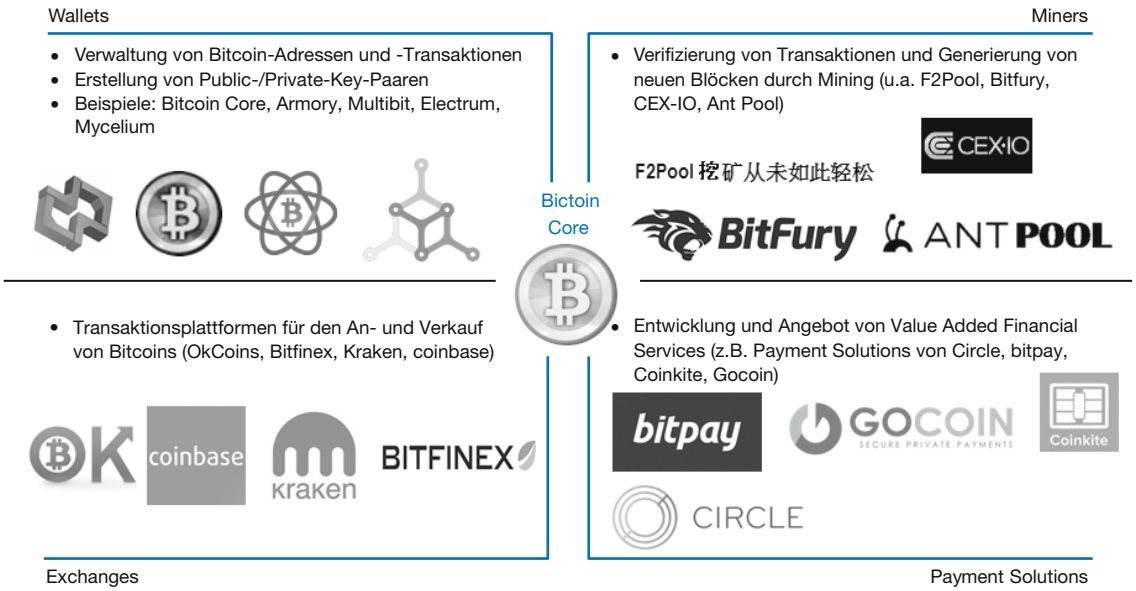
Anschließend wird der neu generierte Block einschließlich der darin befindlichen Transaktionen an alle Netzwerkknoten gesendet, die dann ihrerseits die Validität des Blocks verifizieren und diesen gegebenenfalls der Blockchain als neues Element hinzufügen können. Wenn konkurrierende Miner nahezu gleichzeitig einen neuen validen Block bilden, können temporär Gabelungen in der Blockchain entstehen. Diese lösen sich jedoch rasch auf, da das Netzwerk sich stets auf den längsten Block einigt. Es entsteht ein verteiltes Transaktionsregister, das eine lückenlose, unveränderliche Historie von Eigentums- und Übertragungsbeziehungen von Bitcoins enthält. Dieses Register ist zwar öffentlich, ermöglicht aber dennoch die Vertraulichkeit einzelner Transaktionsdetails, da diese nur mit dem jeweiligen Private Key des Berechtigten eingesehen werden können.

Die kryptografische Verkettung von Transaktionen und Blöcken hat zur Folge, dass nicht eine einzelne Transaktion verändert werden kann, ohne den Block insgesamt sowie alle folgenden Blöcke ebenfalls zu verändern. Das Proof-of-Work-Konzept verhindert somit, dass historische Transaktions- und Blockdaten leicht verändert werden können. Denn ein potenzieller Hacker müsste über mehr als 50% der Rechenleistung des gesamten Netzwerks verfügen, um Transaktionen ex post manipulieren zu können. Dies wäre mit enormen Kosten verbunden, ist aber theoretisch möglich.

Da die Miner im Zuge der Erzeugung eines neuen Blocks die Authentizität der darin enthaltenen Transaktionen sowie indirekt der gesamten Blockchain gewährleisten, erhalten die Miner im Gegenzug eine Entlohnung in Form einer bestimmten Menge an neuen Bitcoins (BTC). Diese wird alle 210 000 Blöcke halbiert, sodass die maximal zu erzeugende Menge an Bitcoins bei 21 Mio. liegt.[6] Weder

6 Vgl. Bitcoin.org.

Abbildung 3
Das Ökosystem der Bitcoin-Industrie



Quelle: eigene Darstellung.

die absolute Höhe des Mininglohns noch der zugrunde liegende Halbierungsalgorithmus oder der gewählte Anpassungszeitraum werden von den Bitcoin-Entwicklern nachvollziehbar begründet. Bei Einführung der Bitcoins lag der Mininglohn noch bei 50 BTC[7], dieser wurde dann erstmals im November 2012 auf 25 BTC halbiert. Seit Juli 2016 sind es 12,5 BTC, die an die Miner pro Block ausgeschüttet werden. Am 15.9.2016 waren ca. 15,8 Mio. BTC im Umlauf.

Je geringer der Zielwert festgelegt wird, umso größer ist im Durchschnitt der Rechenaufwand, der betrieben werden muss, um den entsprechenden Zielhashwert für einen neuen Block zu ermitteln. Der Schwierigkeitsgrad des Proof-of-Work wird im Bitcoin Core von Zeit zu Zeit angepasst, da die Rechenleistung des Bitcoin-Netzwerks im Laufe der Zeit steigt. Dabei wird der Schwierigkeitsgrad durch das Bitcoin Core so kalibriert, dass im Durchschnitt alle zehn Minuten ein neuer Block erzeugt wird.

Andere Kunstwährungen

Seit der Erfindung der Bitcoins hat es etliche Versuche gegeben, das Konzept mit unterschiedlichen Verschlüsselungstechnologien nachzuahmen. Inzwischen gibt es mehr als 700 solcher Kunstwährungen, von denen jedoch nur 16 eine Marktkapitalisierung von mehr als 20 Mio. US-$ haben (Stand Ende Oktober 2016).[8] Zu den Top drei gehören Ethereum, Ripple und Litecoin:

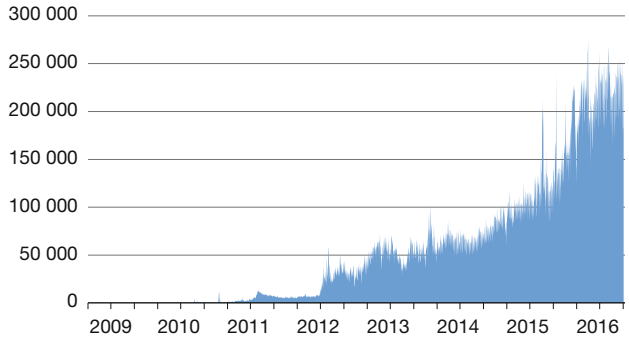
- *Ethereum*: Die Ethereum-Plattform wurde erst Mitte 2015 veröffentlicht. Im Unterschied zu den meisten anderen Kryptowährungen bietet Ethereum neben der eigenen Kunstwährung Ether den Nutzern die Möglichkeit, sogenannte „Smart Contracts" in der Ethereum-Blockchain abzubilden. Unter Smart Contracts versteht man Verträge, bei denen Rechte und Pflichten, Bedingungen und Folgen so strukturiert in Algorithmen digital abgebildet werden, dass diese als Anwendungen auf der Blockchain-Technologie implementiert werden können. Die Überwachung der Einhaltung der vertraglichen Vereinbarungen (Monitoring) sowie die automatische Einleitung von Konsequenzen bei entsprechenden Verstößen (Self-Execution) sind dadurch grundsätzlich möglich.

- *Ripple:* Das US-Unternehmen Ripple Labs hat mit „Ripple" eine Technologie entwickelt, die weltweit Zahlungen in multiplen Währungen mit Hilfe eines Interledger-Protocols (ILP) ermöglicht. Im Unterschied zu Bitcoin ersetzt Ripple nicht die Banken als Intermediäre, sondern stellt eine Plattform zur effizienten Vernetzung der bestehenden Zahlungssysteme von Banken bereit. Die Kunstwährung „Ripple" (XRP) kann

7 BTC steht für Bitcoin.

8 Vgl. Map of Coins: Explore the visualized history of the cryptocurrencies from their whitepapers up to present days, Juli 2016.

Abbildung 4
Zahl der täglichen Bitcoin-Transaktionen



Quelle: Blockchain Database.

dabei optional als Brückenwährung fungieren, um eine möglichst schnelle Durchführung von Zahlungen auch in illiquiden Devisenmärkten zu ermöglichen. Das Volumen der Kunstwährung XRP ist auf 100 Mrd. XRP beschränkt, die im Unterschied zu anderen Kryptowährungen nicht durch Mining erzeugt werden.

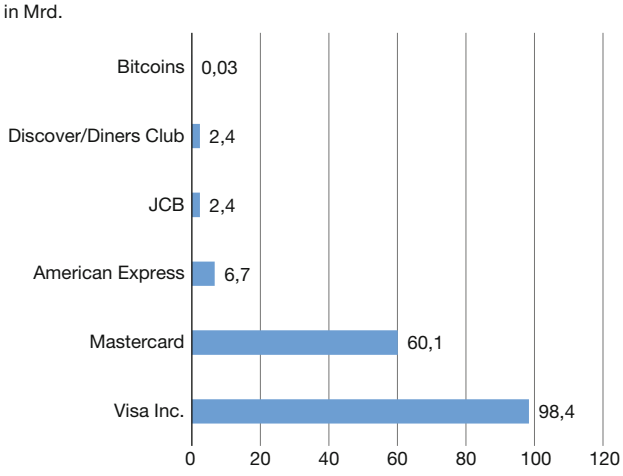
- *Litecoin:* Die 2011 gestartete Kryptowährung Litecoin ähnelt dem Bitcoin-System, da diese ebenfalls auf einem Peer-to-Peer-Netzwerk und der Blockchain-Methodik beruht. Der Unterschied zu Bitcoin besteht vor allem in der Ausgestaltung konkreter Blockchain-Parameter. Neue Blöcke werden im Litecoin-Netzwerk alle 2,5 Minuten erzeugt, sodass die Zahl der maximal schöpfbaren Litecoins gegen 84 Mio. konvergiert.

Das Ökosystem der Bitcoin-Industrie

Abbildung 3 gibt einen Überblick über das Ökosystem der Bitcoin-Industrie, das neben den Entwicklern der Bitcoin-Core-Software und den Minern aus Anbietern von Endkundendiensten (Wallets), Betreibern von Handelsplattformen (Bitcoin Exchanges) sowie Zahlungsverkehrslösungen und anderen Mehrwertdiensten besteht.

Wallets sind Software-Lösungen, die es Endkunden erlauben, Bitcoins zu empfangen, zu senden und zu verwalten. Inzwischen gibt es eine Vielzahl von Walletanbietern. Zu den bekanntesten Wallets, die es für alle gängigen Betriebssysteme gibt, zählen neben dem Bitcoin-Core Armory, MultiBit, Electrum und Mycelium. Miners sind Rechnerverbünde, die im Wettbewerb systematisch neue Transaktionen validieren und diese zu neuen Blöcken zusammenfassen. Da die Wahrscheinlichkeit, neue Blöcke zu generieren mit der Rechenleistung steigt und gleichzeitig der Miningerlös im Zeitablauf sinkt, ist das Geschäftsmodell der Mining Pools auf Größenvorteile ausgerichtet. Zu den größten Mining Pools gehören F2Pool, Bitfury, CEX-IO und Ant Pool. Aufgrund des hohen Energieverbrauchs befinden sich zahlreiche Mining Pools in China. Andere Anbieter positionieren sich als Betreiber von Börsen für Kryptowährungen, über die man Kryptowährungen untereinander oder gegen reale Währungen kaufen und verkaufen kann. Zu den größten Bitcoin-Börsen zählen derzeit OKCoin, Kraken, Coinbase oder Bitfinex. Zahlungsverkehrsdienste mit erweiterten Funktionalitäten bieten z.B. Circle, bitpay, Coinkite oder Gocoin an.

Abbildung 5
Zahl der Transaktionen nach Zahlungssystemen, 2014



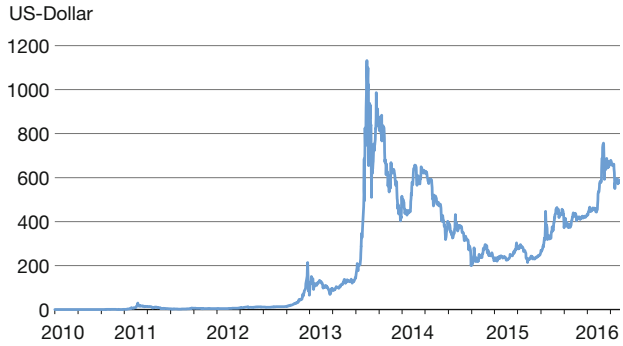
Quelle: eigene Berechnungen, Unternehmensangaben.

Marktentwicklung und Perspektiven

Obwohl sich in den letzten Jahren die Zahl der Anbieter in der Bitcoin-Industrie vervielfacht hat, kann von einem Durchbruch bei der Nutzerakzeptanz keine Rede sein. Abbildung 4 zeigt, dass die durchschnittliche Zahl von Bitcoin-Transaktionen pro Tag zwar deutlich gewachsen ist, jedoch derzeit weltweit nur bei ca. 250 000 liegt. Im Vergleich zu Kreditkartensystemen wie Visa oder Mastercard ist die Bedeutung von Bitcoins noch marginal (vgl. Abbildung 5). So lag 2014 die Zahl der Transaktionen von Visa bei fast 100 Mrd. Insgesamt scheinen die Wachstumsdynamik und die Diffusionsgeschwindigkeit von Bitcoin zu gering, als dass es in absehbarer Zeit zu einer Bedrohung etablierter Zahlungssysteme kommen könnte.

Ein wesentlicher Grund dürfte gerade in einem Aspekt bestehen, der von den Protagonisten von Bitcoins immer wieder als Vorteil dieser Kunstwährung genannt wird: das Fehlen einer zentralen Instanz wie einer Notenbank, die letztlich durch eine auf Preisstabilität ausgerichtete Geldpolitik für Glaubwürdigkeit in die Wertbeständigkeit der Währung sorgen soll. Gerade die Anonymität virtueller Währungen ist augenscheinlich eine zentrale Barriere für eine breitere Akzeptanz, da mögliche Verursacher von

Abbildung 6
Kursentwicklung des Bitcoin



Quelle: BitcoinAverage.com.

Vermögensschäden etwa infolge des Diebstahls von Private Keys bei Hackerangriffen in einem anonymen Netzwerk kaum identifiziert und strafrechtlich verfolgt werden können. Dies hat auch dazu geführt, dass sich das Bitcoin-Netzwerk zum Teil als besonders geeignet für illegale Geschäfte erwiesen hat. Der bekannteste Fall ist die Plattform „Silk Road", die als ebay für illegale Transaktionen zu zweifelhafter Berühmtheit gelangt ist und im Oktober 2013 abgeschaltet wurde. Hinzu kam die Insolvenz der Bitcoinbörse Mt. Gox im Jahr 2014 und der erst im August 2016 vermeldete Verlust von geschätzten 70 Mio. US-$ der in Hongkong ansässigen Bitcoinbörse Bitfinex infolge eines Hackerangriffs.

Ein weiterer Aspekt besteht in den niedrigen Markteintrittsbarrieren für die Etablierung solcher Kunstwährungen. Im Grunde benötigt man lediglich ein kryptografisches Verfahren für die Verschlüsselung, einen Miningprozess sowie einen Konsensusalgorithmus, die in einer Open-Source-Software kodifiziert und öffentlich zugänglich gemacht werden. Die hohe Zahl an Kunstwährungen unterstreicht, dass es sich in den meisten Fällen um kein tragfähiges Geschäftsmodell handeln dürfte.

Die hohe Unsicherheit über die Zukunft von Bitcoins manifestiert sich auch in der volatilen Preisentwicklung. Die Handelsvolumina an den verschiedenen Bitcoinbörsen sind überschaubar und Investitionen in virtuelle Währungen als hoch spekulativ einzuordnen. Abbildung 6 zeigt, dass der Wert des Bitcoin in Spitzenzeiten bei mehr als 1000 US-$ lag, während er derzeit zwischen ca. 600 US-$ und 700 US-$ schwankt.

Disruption durch Distributed Ledgers

Das eigentliche Disruptionspotenzial geht nicht von den virtuellen Währungen an sich, sondern von der verwendeten Blockchain-Technologie aus. Dabei ist zu berücksichtigen, dass die Blockchain nur eine Variante der Distributed-Ledger-Technologie darstellt. Grundsätzlich versteht man unter Distributed Ledgers verteilte Kontoführungssysteme, bei denen digitale Daten über mehrere Standorte gemeinsam genutzt, repliziert und synchronisiert werden. Dabei wird mit Hilfe kryptografischer Verfahren eine fälschungssichere Abbildung von Transaktionen ermöglicht.[9] Werden die Transaktionen mit Hilfe eines Proof-of-Work-Verfahrens in miteinander verbundenen Blöcken abgebildet, spricht man von einer Blockchain.

Es gibt verschiedene Ausgestaltungsmöglichkeiten von Distributed Ledgers, die sich hinsichtlich der Zahl der Nutzer, der eingesetzten kryptografischen Methoden und der Verfahren unterscheiden, mit denen die Integrität und jederzeitige Korrektheit der Datenbank geprüft wird. Den Kryptowährungen liegen sogenannte öffentliche Distributed Ledgers zugrunde, die grundsätzlich jedem Nutzer offenstehen, der über die erforderliche Software verfügt. Neue Transaktionen, die zu einer Veränderung der Datenbank führen, werden auf der Grundlage eines Konsensusalgorithmus zu neuen Blöcken zusammengefasst und können von jedem Netzwerkknoten validiert werden. Da die mit offenen Distributed Ledgers wie bei Bitcoin einhergehende Anonymität insbesondere unter dem Gesichtspunkt der Geldwäsche kritisch zu beurteilen ist, erscheinen geschlossene Distributed Ledgers erfolgversprechender.

Diese auch als „private" oder „permissioned" bezeichneten Distributed Ledgers werden von einer definierten Zahl von Mitgliedern betrieben. Durch den Einsatz von Verschlüsselungstechniken soll eine fälschungssichere Abwicklung von Transaktionen in einem geschlossenen multilateralen Abwicklungssystem möglichst in Echtzeit erfolgen. Darüber hinaus sollen Effizienzsteigerungen durch die gemeinsame Nutzung von Datenbeständen (Shared Ledger) ermöglicht werden. Die Teilnahme erfolgt in der Regel über ein Proof-of-Identiy-Verfahren, bei dem sich jeder Teilnehmer einem Registrierungsprozess unterziehen muss. Dadurch ist es möglich, bei Betrugsfällen Rückschlüsse auf die Identität der jeweiligen Nutzer zu ziehen. Allerdings dürfte es im Einzelfall eine Herausforderung sein, die Zugangsrechte so auszugestalten, dass Transparenz und Überprüfbarkeit der Datenbankeinträge einerseits und der Anspruch auf Datenschutz andererseits in Einklang gebracht werden können. Bei privaten Distributed Ledgers kann die fortlaufende Validierung des Transaktionsverzeichnisses auch durch als vertrauenswürdig eingestufte Netzwerkknoten oder die Betreiber der Datenbank erfolgen.

9 Vgl. BlockchainTechnologies.com.

Die Entwicklung der Distributed-Ledger-Technologie befindet sich noch im Anfangsstadium, sodass sich das Potenzial der Technologie gegenwärtig nur in Ansätzen erfassen lässt. Es ist jedoch zu erwarten, dass vor allem transaktions- und informationsintensive Branchen durch die Anwendung von Distributed Ledgers disruptiven Veränderungen ausgesetzt sein werden. Dazu zählt der Finanzsektor und hier vor allen das „Transaction Banking". Darunter versteht man sämtliche Dienstleistungen, die von Banken im Zusammenhang mit der Abwicklung des Zahlungsverkehrs sowie von Devisen- und Wertpapiertransaktionen erbracht werden.

Zahlungsverkehr

Die Abwicklung des Zahlungsverkehrs in der Eurozone hat mit SEPA (Single Euro Payments Area) und dem Target2-System erhebliche Fortschritte gebracht.[10] Denn mit SEPA, dem einheitlichen Euro-Zahlungsverkehrsraum, wurden europaweit einheitliche Verfahren für den bargeldlosen Zahlungsverkehr eingeführt. Das Target2-System ist das Zahlungssystem der Zentralbanken des Eurosystems für die schnelle Abwicklung von Überweisungen in Echtzeit. Dennoch werden Überweisungen der Endkunden auch innerhalb der Eurozone in der Regel erst am nächsten Bankarbeitstag valutiert. Diese Settlement-Fristen können deutlich länger werden, wenn es sich um internationale Überweisungen über das SWIFT-System handelt, bei denen die Regulierung der Zahlungen über Korrespondenzbanken abgewickelt wird.

Gerade der Zahlungsverkehr ist prädestiniert für die Anwendung der Distributed-Ledger-Technologie. Ähnlich wie im Bitcoinnetzwerk könnten künftig auch Zahlungen in klassischen Währungen grenzüberschreitend in nicht anonymen Peer-to-Peer-Netzwerken in Echtzeit direkt zwischen den Vertragsparteien durchgeführt werden, ohne dass es weiterer Intermediäre bedarf. Bislang benötigen selbst webbasierte Zahlungsverkehrssysteme wie Paypal immer noch Banken und Kreditkartenunternehmen als Dienstleister.

Derartige „Instant-Payment-Systeme" müssen jedoch nicht zwangsläufig auf der Blockchain-Technologie beruhen, sondern können durchaus auf einer weiteren Modernisierung von Target2 oder spezifischen transaktionsorientierten Messangerdiensten basieren. In Europa treiben die Europäische Zentralbank und das im Dezember 2013 gegründete European Retail Payments Board (ERPB) die Entwicklung eines Echtzeitzahlungssystems auf Basis der SEPA-Formate und die Erarbeitung der damit verbundenen Regelwerke voran.[11]

Wertpapierdienstleistungen

Für Wertpapierdienstleistungen sind vor allem bei den Nachhandelsaktivitäten erhebliche Effizienzsteigerungen zu erwarten. Diese Aktivitäten variieren zwar je nach Komplexität der Finanzprodukte, erfolgen jedoch vom Grundsatz her in den folgenden Schritten: Nach dem Eingang der Kauf- bzw. Verkaufsaufträge geschieht über das Order Routing eines Intermediärs (Bank/Broker) die Weiterleitung an eine elektronische oder physische Handelsplattform. Anschließend erfolgt das Clearing. Darunter versteht man das Feststellen gegenseitiger Forderungen, Verbindlichkeiten und Lieferverpflichtungen. Beim anschließenden Settlement wird das Wertpapier übertragen und im Gegenzug der korrespondierende Geldbetrag überwiesen. Banken und Broker fungieren als Intermediäre zwischen den Käufern bzw. Verkäufern und den Zentralverwahrern.

Gegenwärtig beträgt die Abwicklungsdauer beispielsweise im Aktienhandel mit girosammelverwahrten Wertpapieren zwei Tage. Die Geldregulierung erfolgt innerhalb der Eurozone in der Regel über das Target2-System. Mit Target2-Securities (T2S) wird in verschiedenen Stufen bis 2017 eine zentrale Wertpapierabwicklung in Zentralbankgeld implementiert, wobei die Wertpapierverwahrung und die damit verbundenen Dienstleistungen bei den nationalen Zentralverwahrern (Central Securities Depositories) verbleiben. Das Konzept von T2S basiert auf einer Zusammenführung der Zentralbankgeld- und Wertpapierseite auf einer Plattform im „Delivery-versus-Payment-Modus".[12] Wesentlich komplizierter bleiben grenzüberschreitende Wertpapierabwicklungen, wenn mindestens ein Transaktionspartner außerhalb der Eurozone sitzt. Dann vervielfachen sich die Schnittstellen und damit die Abwicklungszeiten zwischen den beteiligten Banken, Brokern, Zentralverwahrern, Clearinghäusern, Verwaltern von Sicherheiten und Korrespondenzbanken.

Die Distributed-Ledger-Technologie kann hier zu einer deutlichen Verschlankung der Prozesse beitragen. Wenn es gelingt, Wertpapiertransaktionen in einer verteilten Datenbank mit Hilfe kryptografischer Verfahren fälschungssicher zu übertragen, können in der Endausbaustufe die heute zeitintensiven Clearing- und Settlementprozesse soweit verschmelzen, dass Handel und Abwicklung nahezu in Echtzeit erfolgen können. Dies könnte bedeuten,

10 Target steht für Trans-European Automated Real-time Gross Settlement Express Transfer.

11 Vgl. European Retail Payments Board (ERPB): Statement following the fourth meeting of the Euro Retail Payments Board held on 26.11.2015.

12 Vgl. Deutsche Bundesbank: TARGET2-Securities maximiert die Abwicklungseffizienz im europäischen Wertpapiermarkt, Frankfurt 2015.

dass die heutigen Zentralverwahrer zu einer reinen Lagerstelle mutieren und es auch die Depotdienstleistungen der Banken in der Form nicht mehr geben muss. Denn Dividenden- oder Couponzahlungen können über Smart Contracts als Anwendung auf der Blockchain ebenfalls automatisiert werden.

Smart Contracts

Smart Contracts stellen die digitale Abbildung vertraglicher Vereinbarungen dar, die im Distributed Ledger als ausführbare Programme kodiert sind. Diese ermöglichen die automatische Auslösung von Aktivitäten, wenn deren Ausführung an den Eintritt bestimmter vertraglicher Bedingungen geknüpft ist. Dies kann Zins- und Tilgungszahlungen ebenso betreffen wie Kaufpreisnachlässe, Gutschriften oder die automatische Anpassung von Versicherungsprämien in Abhängigkeit von der Schadenshistorie.

Die Prinzipien der Distributed-Ledger-Technologie lassen sich auch außerhalb des Finanzsektors auf materielle Transaktionsobjekte wie beispielsweise Immobilien, Maschinen und Anlagen oder den Transfer von immateriellen Vermögensgegenständen wie geistige Eigentumsrechte übertragen. Sofern diese Vermögensgegenstände etwa über Sensoren, RFID-Transponder, einen QR-Code oder eine IP-Adresse elektronisch erfasst werden, können Übertragungsvorgänge digital in einem Ditributed Ledger wie z.B. einer Blockchain abgebildet und nachverfolgt werden.

Smart Government

Dadurch werden virtuelle Notardienstleistungen bei Immobilientransaktionen oder dem Verkauf von Unternehmen mit Hilfe von kryptografischen Verfahren denkbar. Distributed Ledgers können auch dazu beitragen, die Effizienz administrativer Prozesse im öffentlichen Dienst zu verschlanken (Smart Government), wenn beispielsweise sämtliche steuerrelevanten Daten von Privatpersonen, Unternehmen und öffentlichen Einrichtungen in einer verteilten Datenbank bereitgestellt und fälschungssicher in Echtzeit zugeordnet werden können. Steuerhinterziehung würde dadurch erheblich erschwert, Steuererklärungen könnten leichter oder im Idealfall durch intelligente Apps automatisch erstellt werden. Die Führung von Grundbüchern und Katastern bietet sich ebenso für eine Blockchain-Lösung an wie zahlreiche Dienstleistungen der Standesämter.

Ähnliche Ansatzpunkte gibt es im Gesundheitswesen (Smart Health), indem z.B. Patientendaten oder Behandlungsverläufe in einer verteilten Datenbank Kliniken, Ärzten und Versicherungen zur Verfügung gestellt werden können. Die Vergabe der Zugangsrechte würde aus datenschutzrechtlichen Gründen beim Patienten verbleiben. Administrative Prozesse in der medizinischen Versorgung könnten verschlankt und Daten für Forschungsprojekte in anonymisierter Form rascher und umfassender bereitgestellt werden.

Distributed Ledgers können in Verbindung mit Smart Contracts auch die Entwicklung von Industrie 4.0 befördern, die auf der Verschmelzung von virtuellen und physischen Systemen zu sogenannten Cyber Physical Systems in der industriellen Produktion beruht. Denn in zahlreichen Branchen ist es wichtig, Herkunft, Echtheit, Qualität oder die Einhaltung von Umweltstandards zuverlässig zu erfassen. Dies gilt z.B. für die Lebensmittelbranche etwa beim Nachweis biologischer Anbauformen, für die Rohstoffindustrie bei der Überprüfung von Abbaurechten oder für die Textilindustrie bei der Überprüfung von Arbeitsbedingungen in den Herstellerländern. In all diesen Fällen ist es denkbar, Erzeugung, Transport und Weiterverarbeitung von Erzeugnissen lückenlos und fälschungssicher in einem Distributed Ledger zu dokumentieren. Die Fälschung von Herkunftsangaben, die Nicht-Einhaltung von Qualitätsstandards oder eine unsachgemäße Entsorgung von Reststoffen würden erheblich erschwert. Die Distributed-Ledger-Technologie kann also disruptive Veränderungen in unterschiedlichen Bereichen auslösen und sich damit zu einer Schlüsseltechnologie innerhalb der IT entwickeln. Daher sollte eine verstärkte Förderung der Forschung auf diesem Gebiet in Erwägung gezogen werden.

Title: ***Bitcoins, Blockchain, and Distributed Ledgers***

Abstract: *Cryptocurrencies such as bitcoin were invented to facilitate instant payment services without the need for a central bank or financial intermediaries executing payments. Using cryptographic functions, any user of the bitcoin system can transfer units of the virtual currency globally on an anonymous basis. However, financial supervisory authorities are about to increase regulation of virtual currencies due to concerns that the anonymous character of the system facilitates money laundering and the financing of illegal transactions. Nevertheless, the underlying blockchain technology, or in broader terms the distributed ledger technology, may revolutionise several industries. This paper illustrates the functioning and recent market developments in the bitcoin industry as well as the disruptive potential of the underlying technologies.*

JEL Classification: *G10, G20, G29*