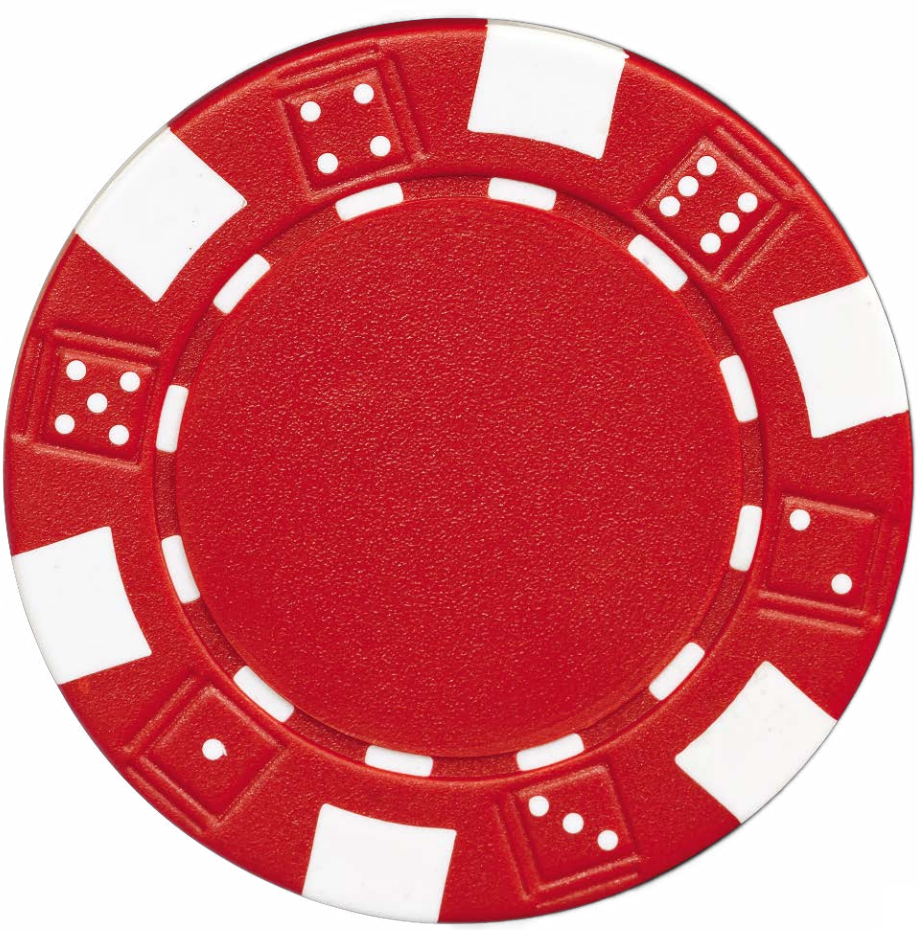
Deloitte.



Welchen Wert hat der Bitcoin?

Wie entsteht der Wert einer Kryptowährung? Ist er langfristig gewahrt? Welche neuen Geschäftsmodelle sind möglich und tragen zur Wertsteigerung bei? Deloitte gibt Antworten!

Der Wert von Währungen

Anforderungen an ein Zahlungsmittel
Ein Zahlungsmittel muss wenigstens drei Grundfunktionen bieten: es muss sich gegen Waren und Dienstleistungen eintauschen lassen (Bezahlfunktion), man muss Werte akkumulieren können (Sparfunktion) und Menschen müssen in der Lage sein, den Wert von Gütern in der Dimension der Währung einzuschätzen (Bewertungsfunktion).

Die Forderung nach der Möglichkeit des Sparens verbietet längere Phasen mit Inflationsraten über dem Zinssatz für risikoarme Kapitalanlagen, die Funktion ist für viele Anwender essentiell: Werden wir als Rentner von unserem Ersparten leben können? Außer der Inflation könnten auch Kopien von Einheiten des Zahlungsmittels seinen Wert mindern, gutes Geld muss demnach fälschungssicher sein und seine Buchführung strengen Regeln folgen.

Selbstverständlich muss sich das Zahlungsmittel elektronisch übertragen und speichern lassen, was den Einsatz von ausschließlich physikalisch darstellbaren Assets verunmöglicht.

Der Wert des Zahlungsmittels ergibt sich also aus seinem Nutzen – erfüllt es die Grundfunktionen und lässt es sich einfach transferieren, dann ist es wertvoll.

Fiatgeld

Spätestens seit dem Zusammenbruch des Systems von Bretten Woods im Jahr 1973 verfügt keine der wichtigen Währungen mehr über einen intrinsischen Wert, also einen Wert „an und für sich", der aus dem früher von Zentralbanken gegebenen Versprechen resultierte, eine Banknote jederzeit gegen Gold, Silber oder ein anderes wertvolles, nicht beliebig vermehrbares Gut einzutauschen. Wir hoffen, dass das Geld nach seiner Schöpfung einen extrinsischen Wert annehmen wird, der aus der zuverlässigen Verfügbarkeit der Grundfunktionen eines Zahlungsmittels resultiert. Wir bezeichnen es deshalb als Fiatgeld (lat.: fiat = es geschehe).
Aber diese Funktionen fußen auf unserem Vertrauen in zentrale Institutionen.

Die Sparfunktion des Fiatgelds gründet auf unserem Vertrauen, dass Zentralbanken in demokratischen Staaten unabhängig sind und nicht der Regierung, sondern einzig dem Dreiklang aus Geldwertstabilität, Wirtschaftswachstum und außenwirtschaftlichem Gleichgewicht verpflichtet sind.
Sie werden demnach die Geldmenge, die ja ohne den Zwang eines Goldstandards prinzipiell keiner technischen Beschränkung unterliegt, nur unwesentlich stärker als das reale Wachstum des Bruttosozialprodukts erhöhen und so die Inflation deckeln. Obwohl Regierungen durch eine höhere Inflation ihre Schulden leichter „mit schlechtem Geld" begleichen könnten.

Wir müssen auch Banken, Kreditkartengesellschaften und anderen Grundpfeilern des modernen Zahlungsverkehrs vertrauen, die eine sichere Bezahlfunktion gewährleisten: Durch die zentrale Buchführung der Finanzintermediäre kann Fiatgeld nicht mehrfach ausgegeben werden und Fremde können unsere Konten nicht ohne unsere Autorisierung belasten. Dieses System funktioniert aber nur dann, wenn nicht nur wir den Intermediären sondern diese sich auch untereinander vertrauen, was vermutlich die verwundbarste Stelle unseres aktuellen Zahlungsverkehrssystems ist.

Open Source statt Finanzintermediäre

Während wir nach wie vor bereit sind, den Zentralbanken großes Vertrauen zu schenken, beunruhigt uns die Möglichkeit des Zusammenbruchs einer großen Geschäftsbank, der sich wegen der engen internationalen Verflechtung der Finanzunternehmen schnell zu einem Szenario entwickeln kann, dass ganze Gemeinwesen in die Zahlungsunfähigkeit treibt. Und die deshalb ihre Versprechen einer Einlagensicherung nicht mehr halten können.
Es verwundert deshalb nicht, dass im Oktober 2008, nur wenige Monate nach dem Zusammenbruch von Lehman Brothers, unter dem Pseudonym Satoshi Nakamoto mit Bitcoin: A Peer-to-Peer Electronic Cash System ein verteilt organisiertes Zahlungsverkehrssystem beschrieben wurde, das ohne zentrale Instanzen funktioniert.
In der Veröffentlichung wurden Erkenntnisse und Methoden aus Spieltheorie und Kryptografie, R.C. Merkles Hash-Baum von 1980, die bereits 1991 von S. Haber und W. Stornetta erfundene Blockchain und der 2002 von A. Back entwickelte Proof-of-Work zu einem funktionierenden Ganzen zusammengefasst.

Bitcoin sollte Geldschöpfung ohne Nationalbanken ebenso ermöglichen wie Transaktionen ohne Finanzintermediäre. Der Geldwert sollte nicht mehr Vertrauen in zentrale Institutionen erfordern, sondern durch die fehlerfreie, unbestechliche Funktion von Algorithmen gewährleistet sein. Die Intransparenz zentraler Entscheidungsprozesse sollte durch die Transparenz eines quelloffenen und gemeinfreien Softwareprojekts abgelöst werden – nichts weniger als die Demokratisierung des Geldes.

Tatsächlich benötigt man zur Teilnahme am Zahlungsverkehrssystem nur einen Internetzugang und eine App, die man aus dem Github herunterlädt, das Bitcoin-Wallet.

Kryptowährungen

Konsens in dezentralen Systemen

Mit dem Verzicht auf zentrale Instanzen muss deren Kontoführungsrolle ein verteiltes Kassenbuch (engl.: distributed ledger) übernehmen. Es speichert keine Kontostände, sondern alle jemals erfolgten Zahlungstransaktionen und wird im Falle der Kryptowährung Bitcoin als Blockchain auf den Rechnern der Nutzer des Zahlungsverkehrssystems redundant gespeichert. Die Rechner sind über das Web in einem öffentlichen Peer-to-Peer-Netzwerk verbunden, wie man es von Napster oder BitTorrent kennt. Dort wie hier gibt es im System per Definition keine zentrale Autorität und keine Zugangskontrolle oder andere Barrieren.

Das Bitcoin-Netzwerkprotokoll gleicht die Datenstände der Nutzer automatisch ab und sorgt dafür, dass die Blockchain nur wahre Daten, also gültige Transaktionen enthält. Das Protokoll verhindert, dass Nutzer bereits verbrauchtes Geld ausgeben (engl.: double spending) oder Geld tansferieren, das ihnen gar nicht gehört. Dieser Konsensalgorithmus ist das Herzstück jeder Kryptowährung.

Bitcoin findet Konsens in Zyklen, die ungefähr 10 Minuten dauern und in denen jeweils folgendes passiert:

1. Nutzer erzeugen eine Überweisung mit ihrem Wallet. Die Adresse des Zahlungsempfängers haben sie mit Hilfe eines QR-Codes erfasst. Neue Zahlungstransaktionen werden von der Software an alle Knoten im P2P-Netzwerk verteilt.

2. Jeder Knoten, der aktiv an der Konsensfindung teilnimmt, fasst neue Transaktionen zu einem Block zusammen. Vor der Aufnahme in einen Block prüft er die Gültigkeit der Transaktion: ist das Geld nicht bereits ausgegeben? Stimmt die digitale Signatur des Zahlers? Zusätzlich zur Validierung muss der Knoten den Block so um Zahlen ergänzen, dass der Hash-Wert eine vorgegebene Anzahl führender Nullen aufweist (engl.: difficulty). Dieses Hash-Puzzle ist nur durch Ausprobieren lösbar, die genaue Dauer der Lösungsfindung ist nicht vorhersagbar, sie folgt einer Bernoulli-Verteilung. Im Durchschnitt beträgt sie 10 Minuten und gibt damit die Bitcoin-Konsenszykluszeit vor.

3. Die Knoten aus Schritt 2 stehen bei der Lösung des Hash-Puzzles im Wettbewerb, der Ausgang dieses Rennens ist rein zufällig. Der neu gebildete Block des Siegers ist der erste, der im Netz verteilt wird.

4. Die anderen Knoten akzeptieren den neuen Block nur dann, wenn alle enthaltenen Transaktionen gültig sind.

5. Die Akzeptanz des neuen Blocks führt dazu, dass er an die Blockchain angehängt wird. Und zwar an den Block, den der blockbildende Knoten zu Beginn seines Hash-Puzzles als den letzten in der Kette betrachtete.

Die Knoten verfolgen immer den längsten Pfad in der Kette. Kinderlose Verzweigungen werden von der Software abgeschnitten.

Die zufällige Auswahl eines Blocks als Ergebnis von Schritt 2 ist spieltheoretisch von großer Bedeutung: Es ist für einen Angreifer nicht prognostizierbar, welcher Block als nächster in die Kette aufgenommen wird.

Proof-of-Work
Neben der Rolle als Zufallsgenerator ist die mit Aufwand verbundene Lösung des Hash-Puzzles auch ein Arbeitsnachweis, der Proof-of-Work (PoW). Er erfüllt zwei Zwecke:

- **Selbst wenn es einem Angreifer gelänge, schreibenden Zugriff auf die Blockchains aller Teilnehmer zu erlangen, wären nachträgliche Änderungen an Blöcken aufgrund des Rechenaufwandes fast unmöglich – der PoW müsste für jeden von der Modifikation betroffenen Block neu erbracht werden.**

- **Es existiert in Bitcoin keine zentrale Instanz, die Teilnehmer authentisiert. Ohne Arbeitsnachweis könnte ein Angreifer ohne großen finanziellen und organisatorischen Aufwand eine Sybil-Attacke starten, d.h. viele Rechner mit falschen Identitäten in das Peer-to-Peer-Netzwerk einbringen und das Vertrauen in die Blockchain durch das Hinzufügen ungültiger Blöcke untergraben.**

Der Bitcoin-Konsensalgorithmus hat sich als überaus zuverlässig erwiesen. Sein PoW auf Basis der Hashfunktion SHA-256 steht jedoch hauptsächlich wegen des wettbewerbsbedingten hohen Energieverbrauchs und der ASIC-Affinität mit der Tendenz zur Zentralisierung der Blockbildung in der Kritik. Wir kommen später noch einmal darauf zurück.

Der Wert des Bitcoin aus den Funktionen eines Zahlungsmittels

Bezahlen

Die Bezahlfunktion von Bitcoin ist grundsätzlich gegeben, einige Merkmale stehen jedoch einem Einsatz der Währung als universelles Zahlungsverkehrssystem im Weg:

- Das Bitcoin-Netzwerk kann nur ca. 3 Transaktionen pro Sekunde (tps) bestätigen. Das ist im Vergleich zu den Kreditkartensystemen mit über 10.000 tps nicht konkurrenzfähig.
- Die Transaktionskosten unterliegen großen Schwankungen. Sie lagen in der Vergangenheit zeitweise über 10 €, wodurch die Überweisung kleiner Beträge wirtschaftlich unmöglich war.
- Es kommt vor, dass gültige Transaktionen nicht Teil der Blockchain werden. Das passiert immer dann, wenn die Transaktion in einem Block bestätigt wurde, dessen Pfad später nicht weiterverfolgt wird. Die Transaktion muss in diesem Fall wiederholt werden.

Trotz dieser Einschränkungen kann jederzeit mit Bitcoin bezahlt werden, sofern ein Verkäufer von Waren oder Dienstleistungen diese Bezahlmöglichkeit anbietet. Der Käufer muss keine Kreditkartendaten publizieren und bleibt pseudonym. Es gibt im Ökosystem auch keine Server, die in Wartungsfenstern oder wegen eines Cyberangriffs nicht erreichbar sind.

Sparen

Kann man mit Bitcoin sparen? Die würde das Fehlen von Geldentwertung durch Inflation oder Fälschungen voraussetzen.

Die Geldschöpfung findet in Schritt 2 des Konsensalgorithmus statt, weshalb die blockbildenden Knoten in Kryptowährungssystemen als Miner bezeichnet werden. Als Gegenleistung für die Bildung eines Blockes erhält der Miner nicht nur die Transaktionsgebühren, die von den Zahlern einer Überweisung stammen. Zusätzlich werden ihm für die Blockbildung Währungseinheiten gutgeschrieben (engl.: block reward), die zuvor noch nicht im System waren. Diese Belohnung beträgt aktuell 12,5 Bitcoin (BTC) und wird alle vier Jahre halbiert, das nächste Mal im Juni 2020.

Auf Basis eines Kurses von 7.000 €/BTC und sechs neuen Blöcken pro Stunde wird so pro Jahr eine Geldmenge von umgerechnet ca. 4,6 Mrd. € geschöpft. Bei einer aktuellen Bitcoin-Marktkapitalisierung von 144,3 Mrd. € entspricht das einem Geldmengenwachstum von 3,1 % (Stand: 21. April 2018). Durch die periodische Halbierung der Bitcoin-Geldschöpfung kann die total erreichbare Geldmenge mit der Summe einer geometrischen Reihe abgeschätzt werden: es wird nie mehr als 21.024.000 BTC im System geben, die Erzeugung neuen Gelds verebbt um das Jahr 2042 herum.

Inflation sieht anders aus - aber was ist mit der Fälschungssicherheit? Ausgeben können Nutzer nur solche Währungseinheiten, die sie in einer zurückliegenden Transaktion empfangen und noch nicht überwiesen haben (UTXO – Unspent Transaction Output). Sie müssen den Besitz durch eine digitale Signatur nachweisen, die sie mit ihrem privaten kryptographischen Schlüssel anfertigen. Die Gültigkeit der Signatur wird vom Netzwerk bei der Blockbildung überprüft, ebenso wie die Einmaligkeit der Ausgabe.

Wert aus neuartigen Anwendungen im Blockchain-Ökosystem

Protokoll und Konsensalgorithmus von Bitcoin haben sich als so robust erwiesen, dass im Laufe der Zeit zahlreiche Anwendungen entstanden sind, die nur indirekt die Funktionen der Kryptowährung nutzen. Dabei geht es nicht um bezahlen oder sparen.

Die Anwendungen fußen primär auf die Fähigkeit der Blockchain, Ereignisse in der tatsächlichen Reihenfolge ihres Eintretens unveränderbar zu speichern. Die zeitliche Auflösung wird dabei von der Konsenszykluszeit bestimmt, d.h. alle innerhalb von 10 Minuten aufgezeichneten Ereignisse haben aus der Sicht der Blockchain gleichzeitig stattgefunden.

Man kann also mit Bitcoin sparen und bezahlen, und zwar seit vielen Jahren. Die stabile Wertentwicklung der Kryptowährung ist demnach bereits mit den beiden wichtigsten Grundfunktionen des Zahlungsmittels erklärbar.
Aber Bitcoin kann noch mehr.

Eine der vielen technischen Grundlagen ist die OP_RETURN-Anweisung der Bitcoin-Skriptsprache, mit der sich bis zu 80 Bytes in einer Bezahl-Transaktion speichern lassen. Das ist bereits ausreichend zur Ablage von Daten wie

- Kurzlink (aka.ms, bit.ly) und Hashwert eines Dokuments
- Fahrgestellnummer (17 Stellen nach ISO 3779), Kilometerstand und momentaner Kraftstoffverbrauch eines Fahrzeugs (über die OBD-Schnittstelle OEM-unabhängig auslesbar)
- Nummer und Kaufpreis eines Flurstücks.

Insbesondere für den Nachweis der Urheberschaft an einem Werk oder dem Besitz einer Urkunde ist die öffentliche Blockckain prädestiniert. So kann man in Staaten, die bislang über kein Katasterwesen verfügen, die Rechtssicherheit beim Handel mit Immobilien dramatisch verbessern, ohne ein teures zentrales System mit Grundbuchämtern und Notaren aufbauen zu müssen. Diesen Weg geht z.B. Afrika momentan sehr erfolgreich.

Die Nutzung dieser neuen Anwendungen kostet Einheiten von Bitcoin, was den Wert der Kryptowährung weiter steigert. Dies gilt natürlich auch für alle anderen Kryptowährungen, insbesondere für solche mit leistungsfähiger Skriptsprache wie etwa Ethereum, wo mit Solidity die Implementierung automatischer Verträge (engl.: smart contracts) sehr gut unterstützt wird.

Volatilität und andere Risiken

Ja, auch mit Fiatgeld ließen sich sachfremde Anwendungen definieren. Man könnte mit einer SEPA-Überweisung Nachrichten im Feld „Verwendungszweck“ europaweit zuverlässig und fälschungssicher übertragen. Oder auf Basis der Seriennummer von Banknoten ein anonymes Ticketsytem für öffentliche Veranstaltungen aufbauen (Kino, Theater, Konzerte). Aber diese Anwendungen verfügen nicht einmal ansatzweise über das disruptive Potenzial wie jene auf Basis der Kryptowährungen.

Anleger beunruhigen die starken Schwankungen des Bitcoin-Wertes, die in den letzten Monaten beobachtet wurden.

Die Kryptowährungen suchen immer noch ihren Wert. Selbst professionelle Marktteilnehmer kennen sie noch nicht sehr lange und nur wenige Menschen verstehen, wie sie intern funktionieren. Aber das ändert sich mit der Zeit, Kryptowährungen sind Teil der digitalen Transformation unserer freien Welt.

Die hohe Volatilität rührt aber auch daher, dass es noch fast keine Futures gibt: Fiele z.B. der ¥ gegenüber dem € um 30 Prozent, dann würden viele Softwareprogramme Yen kaufen, um so günstig zeitlich naheliegende Verpflichtungen aus Leerverkäufen zu befriedigen - der Kurs stiege sofort wieder und vice versa. Dieser Tiefpass fehlt den Kryptowährungen allgemein noch, aber auch das wird sich durch neue Anbieter von Finanzdienstleistungen bald ändern.

Staaten können aus vielen Gründen geneigt sein, den Handel von Kryptowährungen gegen Fiatgeld einzuschränken oder ganz zu verbieten. Zumindest in Deutschland scheint dieses Risiko gering. So ist im Koalitionsvertrag der 19. Wahlperiode des Bundestags vereinbart, dass „wir eine umfassende Blockchain-Strategie entwickeln und uns für einen angemessenen Rechtsrahmen für den Handel mit Kryptowährungen und Token auf europäischer und internationaler Ebene einsetzen.“

Anleger beunruhigen die starken Schwankungen des Bitcoin-Wertes, die in den letzten Monaten beobachtet wurden.

Die Zukunft der Kryptowährungen

Bitcoin Private – zurück zu den Wurzeln

Weiter oben haben wir auf den hohen Energieverbrauch des Bitcoin-PoW hingewiesen. Er resultiert nicht aus aufwändiger Kryptographie – die Gültigkeit von Transaktionen könnte man in 10 Minuten locker auf einem Notebook der 1.000 €-Klasse prüfen. Es ist vielmehr das Ergebnis eines ungesunden Wettrüstens im Kampf um die lukrative Lösung des Hash-Puzzles.

Unter anderem mit dem Ziel der Abkehr von „Mining-Farmen“ wurde am 28. Februar 2018 Bitcoin Private (BTCP) von den Kryptowährungen Bitcoin und Zclassic abgespalten („merge fork“).
Ziele der Abspaltung waren:

- Verbesserung der Transaktionsleistung durch die Erhöhung der Blockgröße von 1 auf 2 Megabyte und die Verkürzung der Konsenszykluszeit von 10 auf 2,5 Minuten
- Wahrung der Anonymität der Nutzer durch den Algorithmus zk-SNARK
- Reprivatisierung des Minings durch die Verwendung von Equihash statt SHA-256 als Hashfunktion im PoW.

Fast 10 Jahre nach der Veröffentlichung von Satoshi Nakamoto kehrt Bitcoin damit zu seiner ursprünglichen Idee eines strikt dezentralen Systems zurück: der Konsensalgorithmus von BTCP ermöglicht wieder allen Nutzern die Teilnahme am Wettbewerb der Blockbildung.

Kontakt

Dirk Siegel
Partner | Consulting
Lead Blockchain Institute
Tel: +49 (0)151 5800 2835
disiegel@deloitte.de

Dr. Markus Stulle
Senior Manager | Technology,
Strategy & Architecture
Tel: +49 (0)151 5807 1139
mstulle@deloitte.de

Deloitte.

Stand 06/2018