

We could envisage proposals in the near future for issuers of electronic payment obligations, such as stored value cards or digital cash, to set up specialized issuing corporations with strong balance sheets and public credit ratings. (Alan Greenspan 2006)

Zusammengefasst nutzen Kryptotransaktionssysteme den hohen technischen Fortschritt auf dem Gebiet der asymmetrischen Kryptologie, um Transaktionen verschlüsselt durchzuführen und in einer transparenten, nachvollziehbaren und fälschungssicheren Datenbank (Blockchain oder Cryptolledger genannt) zu erfassen. Sowohl die Durchführung als auch die Erfassung der Transaktionen in der Datenbank erfolgt dabei zur Gänze in einem (dezentralen) Peer-to-Peer-Netzwerk, dessen Algorithmus auf einem Konsensus-Mechanismus basiert.

Der derzeit bekannteste Vertreter dieser Technologien ist das Bitcoin-Protokoll, dessen erster Client (Version 0.1) als Open-Source im Januar 2009 von Satoshi Nakamoto<sup>1</sup> veröffentlicht wurde.

---

## 2.1 Hintergrund und philosophische Betrachtung

Privatsphäre ist ein Recht wie jedes andere. Man muss es in Anspruch nehmen oder man riskiert es, zu verlieren. (Phil Zimmermann)<sup>2</sup>

---

<sup>1</sup> Die Identität vom Bitcoin-Entwickler Satoshi Nakamoto ist unbekannt. Wobei auch nicht geklärt ist, ob es sich bei Satoshi Nakamoto um eine Einzelperson oder um eine Gruppe von Personen handelt. Laut den vorliegenden Aufzeichnungen (Forenpostings usw.) hat Satoshi Nakamoto bereits 2007 begonnen, am Design und am Code des Bitcoin-Protokolls zu arbeiten. Sein letztes dokumentiertes Posting in einem der Bitcoin-Foren stammt aus Dezember 2010.

<sup>2</sup> [https://de.wikipedia.org/wiki/Phil\\_Zimmermann](https://de.wikipedia.org/wiki/Phil_Zimmermann); Philip R. Zimmermann (\* 12. Februar 1954 in Camden, New Jersey) ist der Erfinder der E-Mail-Verschlüsselungssoftware Pretty Good Privacy (PGP). Er hat einen B.S.-Abschluss für Informatik an der Florida Atlantic University (Abruf: 01.01.2016).

Die ersten Überlegungen zur Notwendigkeit und Nutzung von Kryptografie in neuen digitalen Geld- und Währungssystemen gab es bereits vor mehr als 25 Jahren ausgehend von den Cypherpunks, einer Gruppe von Datenschutzaktivisten. Bereits zu Beginn der 90er Jahre arbeitete diese Online-Community an einem digitalen Zahlungsmittel, dessen Anonymitätsgrad der Anonymität von Bargeldzahlungen entsprechen sollte.

Die Cypherpunks erkannten bereits damals, dass durch die zunehmende Digitalisierung der Schutz der Privatsphäre im Web eine Herausforderung werden würde. Dies war lange, bevor mit Hilfe von Edward Snowden im Jahre 2013<sup>3</sup> Details über das tatsächliche Ausmaß der Spionageprogramme der National Security Agency (NSA) bekannt wurden.

Seit ihren Anfängen im alten Ägypten liegt das Wesen der Kryptografie in der Kunst, Botschaften zu verschlüsseln, um Nachrichten geheim zu halten. Kryptografie im informationstechnologischen Sinne beschäftigt sich mit den Konzepten und Implementierungen von Systemen, die für den Schutz persönlicher, betrieblicher und behördlicher Daten in Computersystemen zuständig sind.

Die Cypherpunks sehen die Notwendigkeit eines erhöhten Schutzes der Privatsphäre im digitalen Zeitalter, um eine offene Gesellschaft aufrechtzuerhalten und entwickeln dementsprechend Instrumente, mit denen die Internetbenutzer ihre Anonymität erhalten können. Gleichzeitig soll der Einflussbereich und die Macht der großen, zentralen Institutionen auf die Menschen eingeschränkt werden.

Das elektronische Geld, an dem die Kryptografen seit 1993 arbeiteten, sollte all jene Merkmale aufweisen, die notwendig waren, um es zu richtigem „Geld“ zu machen: Es sollte haltbar, übertragbar, teilbar und nur beschränkt verfügbar sein.

Folgende wesentliche Konzepte und Technologien, die sich teilweise in der Folge auch in der Bitcoin-Architektur wiederfinden, wurden diskutiert:

- Die Freeware-E-Mail-Verschlüsselungssoftware Pretty Good Privacy (PGP) wurde 1991 vom Kryptografen Phil Zimmermann veröffentlicht<sup>4</sup>.
- Bereits 1989 wurde das Unternehmen DigiCash, vom bekannten Kryptografen David Chaum, gegründet. Chaum bezeichnete den von ihm konzipierten Wert in den 90er Jahren als *Cybercoin*. Das Peer-to-Peer-Zahlungssystem eCash der DigiCash nutzte ein Gutscheinsystem, bei dem jede digitale Münze anonym durch eine digitale Seriennummer dargestellt wurde, die auf der Festplatte des Benutzers in einem Wallet gespeichert wurde. Die Anonymisierung der Nutzer erfolgte bereits anhand einer Public-Key-Kryptografieanwendung. Jede einzelne Transaktion musste jedoch, um ein Double Spending zu verhindern, von zentralen Servern bestätigt werden.<sup>5</sup>

<sup>3</sup> Alles Wichtige zum NSA-Skandal, <http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal> von Patrick Beuth (Abruf: 03.09.2015).

<sup>4</sup> Phil Zimmermann war der erste, der die asymmetrische Kryptografie (auch Public-Key-Kryptografie genannt) als Software der Allgemeinheit leicht zugänglich machte. <https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html> (Abruf: 03.09.2015).

<sup>5</sup> The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order, Paul Vigna und Michael J. Casey, St. Martin's Press (January 27, 2015), Pos 1140.

- Hashcash, ein Proof-of-Work-System, wurde im Mai 1997 von Adam Back, einem britischen Kryptografen ursprünglich entwickelt, um E-Mail-Spam und Denial-of-Service-Angriffe zu begrenzen. Computer müssen nach diesem Konzept kostspielige Arbeit verrichten, ehe sie Informationen versenden dürfen, sodass für jeden, der ein Netzwerk mit Nachrichten überfluten will, erhebliche Kosten anfallen.<sup>6</sup>
- Die Idee eines Hauptbuches bzw. einer Datenbank mit einer nachvollziehbaren chronologischen Erfassung aller darin gespeicherten Transaktionen datiert bereits aus 1991 und stammt von Haber und Stornetta.<sup>7</sup> Das Konzept von Haber und Stornetta sah dabei einen zentralen Server vor, der ein erhaltenes Dokument zusätzlich zu einem Zeitstempel auch mit einem Link zu dem vorhergehenden erhaltenen Dokument versieht und so eine vollständige chronologische Dokumentenerfassung ermöglicht. In der Folge erweiterten Harper und Stornetta ihr Konzept, indem nicht mehr einzelne Dokumente verknüpft wurden, sondern Dokumente in Blöcke zusammengefasst wurden. Einerseits wurden dabei innerhalb der Blöcke die Dokumente miteinander verlinkt und andererseits wurden die Blöcke verknüpft und in Form einer Kette aneinandergereiht.
- Das Konzept des *b-money*, entwickelt von Wei Dai 1998, sah sowohl die Möglichkeit des Schaffens einer Kryptowährungseinheit als Hashcash-Funktion als auch ein Peer-to-Peer-Netzwerk vor.
- Zwischen 1998 und 2005 entwickelte Nick Szabo das digitale Währungssystem *Bit-Gold*. Auch BitGold basierte bereits auf dem Proof-of-Work-Ansatz von Adam Back und löste eines der offenen Punkte des Hashcash-Konzepts: Im System von Adam Back konnte jede Hashcash-Einheit nur einmal verwendet werden. Das System von Nick Szabo kreierte digitale Werteinheiten, die wiederholt genutzt werden konnten.
- Im Jahr 2005 stellte Hal Finney (der später auch eine wichtige Rolle in der Verbreitung des Bitcoin-Systems spielen sollte) das *Reusable Proof-of-Work*-Konzept vor, dass die Ansätze des b-moneys von Wei Dai verwendete und mit den von Adam Back entwickelten Hashcash-Puzzles ergänzte, um einen Vorschlag für eine Kryptowährung zu schaffen.

All diese Konzepte erforderten jedoch durch das ungelöste Double Spending-Problem (unbeschränkte Möglichkeit der Reproduktion eines digitalen Gutes) des digitalen Geldes einen vertrauenswürdigen Dritten in welcher Form auch immer.

Das von Satoshi Nakamoto am 31. Oktober 2008 an den E-Mailverteiler der Kryptografiegruppe (cryptography@metzdowd.com) versandte neunseitige Konzept mit dem Titel *Bitcoin: A Peer-to-Peer Electronic Cash System* unterschied sich insbesondere in zwei Aspekten von den bisher diskutierten Ideen:

---

<sup>6</sup> <https://en.wikipedia.org/wiki/Hashcash> (Abruf: 03.09.2015).

<sup>7</sup> [https://en.wikipedia.org/wiki/Linked\\_timestamping](https://en.wikipedia.org/wiki/Linked_timestamping) (Abruf: 19.02.2016)

- Im Ausmaß des dezentralen Netzwerks und der Auslagerung der Bestätigung der Transaktionen an die Teilnehmer des Netzwerks.
- In der Form des Mining-Belohnungsalgorithmus, der eine Weiterführung des b-money-Konzepts von Wei Dai darstellte.

Die Kombination der Nutzung des Proof-of-Work-Konzepts zur Generierung von digitalem Geld mit dem Konzept von Harper und Stonetta (Zeitstempel und Verlinkung der Transaktionen/Blöcke) und der dadurch entstehenden Bitcoin-Blockchain zur Vermeidung des Double Spending-Problems erfolgte damit auf diese Weise erstmals durch ein dezentrales Computernetzwerk.

Die Bitcoin Architektur verwendet kryptografische Verschlüsselungstechniken zur Regelung des Geldschöpfungsprozesses und zur Verifizierung der durchgeführten Transaktionen. Das Netzwerk basiert auf einer dezentralen Struktur, die aufbaut auf der Anonymität der Nutzer damit auch die Gleichheit der Teilnehmer sicherstellt und durch den Proof-of-Work-Ansatz die Möglichkeit für Manipulationen Dritter beseitigt.

Mittels des Proof-of-Work-Konzeptes bestimmt sich das Ausmaß der möglichen Einflussnahme auf den Algorithmus durch den wirtschaftlichen Aufwand, den man bereit ist, in das System zu investieren (z. B. in Form von Mining-Hardware).

---

## 2.2 Definitionen

**Automated Clearing Houses (ACH-Systeme)**<sup>8</sup> Elektronisches U.S. Clearing-System, in dem vorrangig über Telekommunikationsnetzwerke übermittelte Zahlungsaufträge zwischen Finanzdienstleistern in einem Rechenzentrum des Betreibers verrechnet und ausgetauscht werden. Die Verrechnung der Zahlungen erfolgt brutto (je Datei) oder netto (nur Saldo) zu vorgegebenen Zeitpunkten über Konten der teilnehmenden Finanzdienstleister bei der Zentralbank oder einer privaten Settlement-Bank. Es handelt sich meist um eine große Anzahl von Überweisungen bzw. Lastschriften. Die Abwicklung erfolgt in Form der Stapelverarbeitung (Zusammenfassung in Dateien).

**Bitcoin-Blockchain** ist die öffentlich einsehbare Datenbank, die von den Nutzern des Systems, die sich einen Bitcoin Core heruntergeladen haben (auch Nodes genannt), dezentral auf ihren Computern gehostet wird. Die Bitcoin-Blockchain kann öffentlich eingesehen werden auf Internetseiten wie [www.blockchain.info](http://www.blockchain.info), hier kann man den Transaktionsstrom durch Eingabe einer Bitcoin-Adresse nachverfolgen.

**Blocks** sind Transaktionen, die in Transaktionsgruppen zusammengefasst sind und die sequentiell in der Blockchain erfasst werden.

---

<sup>8</sup> Springer Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, Stichwort: Automated Clearing House (ACH), online im Internet: <http://wirtschaftslexikon.gabler.de/Archiv/5035/automated-clearing-house-v9.html>, (Abruf: 01.01.2016).

**Bitcoin 1.0 (Blockchain 1.0)** meint die Nutzung der Bitcoin-Architektur als Zahlungsabwicklungssystem.

**Bitcoin 2.0 (Blockchain 2.0)** umfasst die Nutzung dezentraler Kryptotransaktionssysteme als Erfassungs- und Abwicklungssysteme für Verträge über Vermögensgegenstände aller Art, beispielsweise Aktien, Anleihen, Kredite, Smart Property, Smart Contracts usw.

**Bitcoin 3.0 (Blockchain 3.0)** umfasst die Nutzung der Blockchain-Technologie über den Finanzbereich hinaus im Gesundheitswesen, in der öffentlichen Verwaltung, im öffentlichen Kulturbereich, in der Literatur usw.

**Eine Bitcoin-Adresse** ist der Hash eines öffentlichen Schlüssels im Bitcoin-System.

**Bitcoin Improvement Proposal (BIP)** Für wesentliche technische Verbesserungsvorschläge des Bitcoin-Protokolls gibt es ein spezielles Verfahren auch BIPs genannt.

**BTC/XBT** stehen für Abkürzungen für die Währungseinheit des Bitcoin-Systems.

**Cloudmining**<sup>9</sup> Beim Cloudmining bilden Nutzer einen Rechenleistungspool. Im Basismodell stellt der Anbieter Mining-Hardware zur Verfügung, überwacht und kontrolliert auch deren ordnungsgemäßes Arbeiten. Meist werden alle 24 h die geminten BTC proportional an die beteiligten Teilnehmer des Pools ausgeschüttet (durch Überweisung in die jeweiligen Wallets). Je nach konkreter vertraglicher Ausgestaltung der Pools sind auch gesellschaftsrechtliche Implikationen denkbar, die komplexe Fragestellungen aufwerfen.

**Cryptocurrency/Kryptowährungen** sind digitalisierte Wertmarken, auch als Token bezeichnet (ein *bitcoin*, oder ein Litecoin), die online auch als Tauschmittel/Zahlungsmittel akzeptiert werden. Jede Kryptowährung basiert auf einem Peer-to-Peer-Netzwerk und einem entsprechenden Protokoll. Manche Kryptowährungen haben eine eigene Blockchain, manche nutzen die Bitcoin-Blockchain – beispielsweise nutzt Counterparty für die Erfassung der Transaktionen ihrer Währung (XCP) die Bitcoin-Blockchain.

**Dapps**<sup>10</sup> meint dezentrale Applikationen. Dezentrale Applikationen werden häufig wie folgt definiert:

- Es handelt sich um eine Open-Source Anwendung.
- Die Anwendung arbeitet autonom ohne zentrale Autorität.
- Jegliche Änderung des Anwendungsprotokolls muss konsensbasierend sein.

<sup>9</sup> <http://www.jurpc.de/jurpc/show?id=20140104>, Moritz Schroeder, Bitcoin: Virtuelle Währung – reelle Problemstellungen (Abruf: 01.01.2016).

<sup>10</sup> <https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md> (Abruf: 02.10.2015).

- Daten und Aufzeichnungen über den Anwendungsbetrieb müssen kryptografisch in einer dezentralen Blockchain lagern, um etwaige zentralen Points-of-Failure zu vermeiden.
- Die Nutzung der DAPP erfordert kryptografische Tokens.

**Dezentrale autonome Organisationen (Decentralized Autonomous Organisation [DAO])** Diese – auch bezeichnet als dezentrale autonome Konsensplattformen (Decentralized Autonomous Consensus Platforms [DCAP]) – sind virtuelle Einheiten, die mit einer Blockchain/Cryptolledger interagieren und spezielle, vorprogrammierte Aufgaben ausführen. In ihrer einfachsten Ausprägung handelt es sich nur um einen Agenten, der programmiert wurde, um eine spezielle Transaktion auszuführen. Diese DAO kann die Aufgaben einer Organisation, eines Unternehmens oder eben eines Agenten übernehmen.

**Distributed Ledger** dezentrale Datenbanken nutzen typischerweise Kryptowährungstechnologien unterscheiden sich jedoch in der Form des Konsensus-Algorithmus (Proof-of-Work; Proof-of-Stake, usw.). Der angewandte Konsensus-Algorithmus ist dabei auch bestimmt dadurch ob es sich bei den Nodes des Netzwerkes um anonyme und/oder identifizierte Teilnehmer des Netzwerkes handelt.<sup>11</sup>

**Double Spending-Problem** Die zweimalige Verwendung eines Tokens/einer Wertmarke wird in herkömmlichen Wirtschaftssystemen durch Involvierung der Finanzsysteme gelöst (eine dritte Partei verwaltet und kontrolliert). In den Kryptowährungssystemen wird das Double Spending-Problem durch Bildung der dezentralen und fälschungssicheren Blockchain gelöst. Technisch wird bei einem Double Spending-Versuch eine Bitcoin-Transaktion initiiert und in der Folge – bevor die erste Transaktion bestätigt wurde – wird mit denselben *bitcoins* eine weitere Transaktion initiiert. Der Trick ist eine betrügerische Transaktion auf dem Bitcoin-Netzwerk als erstes bestätigt zu bekommen, sodass die erste Transaktion nicht durchgeführt wird<sup>12</sup> (Double-Spend-Race-Attacke).

**Dust** Das Dust-Limit wurde 2010 eingeführt, um zu vermeiden, dass die Bitcoin-Blockchain mit winzigen Transaktionen überflutet wird. Das Limit von 0,01 *bitcoin* entsprach damals einem verschwindend geringen Euro-Betrag. Wer Transaktionen mit weniger als 0,01 *bitcoin* sendete, musste eine Gebühr zahlen. Da das Limit inzwischen mehrere Euro wert wäre, wurde der Code mittlerweile geändert und das Dust-Limit erhöht.

**Fork** Ein Fork ist das Resultat einer Änderung des Protokolls eines Kryptotransaktionssystems durch die Kernentwickler. Ein Fork teilt die Blockchain und das Protokoll in zwei

<sup>11</sup> Consensus-as-a service: a brief report on the emergence of permissioned distributed ledger systems, erschienen im Blog, <http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>, S. 4, verfasst von Tom Swanson, am 6. April 2015 (Abruf: 15.08.2015)

<sup>12</sup> What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability, <http://www.coindesk.com/Bitcoin-bug-guide-transaction-malleability/> (Abruf: 26.09.2015).

Versionen – eine, die den neuen Regeln folgt und eine, bei der die alten Regeln weiterhin gelten und die Neuerungen nicht akzeptiert werden. Welche sich durchsetzt, entscheiden die Nutzer – diejenigen, die den Client updaten oder nicht updaten, diejenigen, die mit ihm minen oder nicht minen, und diejenigen, die die neue Blockchain herunterladen oder nicht.<sup>13</sup>

**Forth**<sup>14</sup> ist eine von Charles H. Moore um 1970 entwickelte einfache Script-Sprache. Forth kommt mit sehr wenig Speicher aus. Forth bzw. eine Forth-ähnliche Sprache wird zur Programmierung von Mikrocontrollern genutzt und ist die Programmiersprache der bitcoin-Scripts.

**HardFork**<sup>15</sup> Eine HardFork tritt auf, wenn eine Änderung des Bitcoin-Protokolls ein Update der Knoten erfordert. Wird dieses Update nicht durchgeführt, arbeiten die „alten“ Knoten an der „alten“ Blockchain weiter und die „neuen“ an einer neuen Blockchain.

**Halving** Für jeden generierten und bestätigten Block wird eine Belohnung von 25 *bitcoins* ausgezahlt. Im Laufe der Jahre wird sich diese Belohnung aufgrund des vorgesehenen Algorithmus jedoch immer wieder halbieren (**Halving**), wodurch die Rate der erzeugten *bitcoins* verringert wird.

**Hash** ist das Ergebnis eines Verschlüsselungsvorgangs. Ein Hash-Algorithmus, wie die im Bitcoin-System verwendeten SHA-256 und ECDSA, verwandelt eine nicht zufällige Zeichenfolge in eine weitgehend zufällige Zeichenfolge. Die im Internet allgegenwärtige Verschlüsselung von Informationen dient der Sicherheit und wäre ohne Hash-Funktionen nicht möglich.

**Hashcash Proof-of-Work** Das Hashcash Proof-of-Work-Konzept wurde von Adam Back 1997 entwickelt. Das Konzept bedeutet, dass Rechner eine gewisse Arbeit nachweisen müssen, um eine Aktion auszuführen. Um beispielsweise einen Kommentar auf einem Blog abzugeben oder eine E-Mail abzuschicken, muss der Computer einige Sekunden Rechenaufgaben lösen.

**Hashrate** meint die gesamte Rechenleistung, die im Bitcoin-Minen investiert wird. Von ihr hängt ab, wie schwierig die zu berechnenden Hashes sind. Genauer: Die geschätzte Zahl der Giga-Hashes pro Sekunde (Milliarden von Hashes pro Sekunde), die das Bitcoin-Netzwerk ausführt.<sup>16</sup>

---

<sup>13</sup> Nach dem Hack ist vor dem Hack, von Christoph Bergmann, <http://Bitcoinblog.de/2014/07/28/nach-dem-hack-ist-vor-dem-hack/> (Abruf: 05.08.2015).

<sup>14</sup> [https://de.wikipedia.org/wiki/Forth\\_%28Programmiersprache%29](https://de.wikipedia.org/wiki/Forth_%28Programmiersprache%29) (Abruf: 01.01.2016).

<sup>15</sup> On consensus and forks, <https://medium.com/@octskyward/on-consensus-and-forks-c6a050c792e7#7b5fbc10c> (Abruf 09.04.2016).

<sup>16</sup> <https://blockchain.info/de/charts> (Abruf: 09.04.2016).

**Hacking**<sup>17</sup> Wahrscheinlichkeit, einen privaten Schlüssel zu knacken: Es gibt (potenziell) 1.461.501.637.330.902.918.203.684.832.716.283.019.655.932.542.976 Bitcoin-Adressen. Jeder zufällig generierte private Schlüssel kann nur eine dieser Adressen öffnen. Das bedeutet: Die Chance, eine Adresse zu knacken, liegt bei 1 zu 1.461.501.637.330.902.918.203.684.832.716.283.019.655.932.542.976.

**Internet of Things (IoT)** Internet-of-Things (IoT) ist die Vision, dass jedes Ding der physischen Welt mit dem Internet und anderen Dingen vernetzt wird und so in der Lage ist, Daten über seinen Zustand und die Umwelt zu erfassen, und sich aus dem Internet Daten zu holen und Befehle zu empfangen.<sup>18</sup>

**Maleability-Problem** Eine Transaktion wird mithilfe eines privaten Schlüssels signiert, wobei nur der kritische Teil der Transaktionsdaten von der Signatur abgedeckt wird. Daneben kann man eine Hashsumme über die gesamte Transaktion erstellen. Da die Signatur nur einen Teil der Transaktionsdaten abdeckt, kann man die restlichen Daten ändern und damit eine gleichwertige Transaktion mit unterschiedlicher Hashsumme erstellen. Wird nun diese zweite Transaktion in einen Block aufgenommen, ist die Transaktion abgeschlossen und verbucht. Die erste Transaktion wird als Double-Spend verworfen. Wenn nun nur die Hashsumme der ersten Transaktion als Indikator für die erfolgreiche Transaktion genutzt wird, wird das Transaktionsergebnis nie sichtbar.<sup>19</sup>

**Mikropayment** Kleinbetragszahlung bzw. Mikrozahlung bezeichnet ein Zahlungsverfahren geringer Beträge (meist unter 1 USD/EUR), die vor allem beim Kauf von „Paid Content“, also digitalen Gütern, wie Musikstücken und Zeitungsartikeln online anfallen.

**Netzwerkeffekt** Ein Netzwerkeffekt beschreibt, dass der Nutzen an einem Standard oder Netzwerk wächst, wenn dessen Nutzerzahl größer wird. Wenn der Nutzen für alle bei steigender Nutzerzahl weiter anwächst, spricht man von positiver Rückkopplung. Wird eine kritische Masse erreicht, so steigt die Nutzerzahl exponentiell an.<sup>20</sup>

**Nodes** Nodes, auch Peers genannt, sind Knoten im Netzwerk; ein voller Bitcoin-Node (Full-Node) hat den Original-Client und damit die gesamte Blockchain heruntergeladen und sichert so das dezentrale Netzwerk.

---

<sup>17</sup> <http://www.blockchaincenter.de/fragen/wie-viele-Bitcoin-adressen-gibt-es/> Wie viele Bitcoin-Adressen gibt es? (Abruf: 01.01.2016).

<sup>18</sup> <http://Bitcoinblog.de/2016/01/09/denn-ein-parkplatzsensor-bekommt-kein-bankkonto/> (Abruf: 13.01.2016).

<sup>19</sup> <https://Bitcointalk.org/index.php?topic=490965.0> (Abruf: 25.09.2015).

<sup>20</sup> Definition Netzwerkeffekt, übernommen von Wikipedia; <https://de.wikipedia.org/wiki/Netzwerkeffekt>, (letzter Abruf: 11.08.2015).



**Nonce**<sup>21</sup> Die Nonce in einem Bitcoin-Block ist ein 32 Bit (4-Byte)-Feld, dessen Wert so eingestellt ist, dass der Hash-Block eine Serie von Nullen enthält. Der Rest der Felder sollte nicht geändert werden, da sie eine definierte Bedeutung haben. Jede Änderung der Daten des Blocks (so wie die Nonce) verändert den Hash-Block komplett. Da es unmöglich ist, vorherzusagen, welche Kombination von Bits das richtige Ergebnis des Hashs liefert, werden unterschiedliche Nonce-Werte solange durchprobiert, bis der Hash die richtige Anzahl an 0 Bits hat. Da diese Berechnungen Zeit und Ressourcen erfordern, ist die Veröffentlichung des Blocks ein Nachweis für die geleistete Arbeit (Proof-of-Work).

**On-chain** Bitcoin-Transaktionen werden auf der Blockchain durchgeführt und erfasst.

**Off-chain** Bitcoin-Transaktionen werden nicht auf der Blockchain, sondern auf Side-chains oder bei den diversen Bitcoin-Dienstleistern durchgeführt.

**Peer-to-Peer-Netzwerke bzw. Peer-to-Peer-Marktplätze** Im Internet gibt es zwei Arten von Netzwerken bzw. Marktplätzen. Die am häufigsten anzutreffenden Netzwerke sind zentral organisiert, beispielsweise Google, Facebook, T-Online usw. Ein dezentrales Netzwerk hingegen besteht ausschließlich aus gleichberechtigten Teilnehmern (Peers) und benötigt keinen zentralen Server, um zu funktionieren. Der Peer-to-Peer-Ansatz zeichnet sich dadurch aus, dass die gewünschte Funktionalität durch die Kooperation aller vorhandenen Teilnehmer (Peers) weitgehend gemeinsam erbracht wird, anstatt wie bisher bei klassischen Internetanwendungen eine strenge Unterteilung in einen zentralen Dienstgeber (Server) und eine Vielzahl von Dienstnehmern (Clients) zu haben. Die Grundidee der Kooperation und Selbstorganisation aller Teilnehmer kann genutzt werden, um mittels Peer-to-Peer-Technologie bestehende Anwendungsszenarien kostengünstiger umzusetzen. Die notwendige Infrastruktur wird durch die Kooperation aller Marktteilnehmer gemeinsam bereitgestellt, womit eine Reihe von Vorteilen für die Marktteilnehmer entsteht. So bietet ein verteilter Marktplatz eine hohe Verfügbarkeit und Robustheit, da die bereitgestellte Infrastruktur nicht von einzelnen zentralen Komponenten abhängig ist, wie dies bei bisherigen Marktplätzen unter Aufsicht eines einzelnen Marktplatzbetreibers üblicherweise der Fall ist. Gleichzeitig fallen aufgrund des fehlenden zentralen Marktplatzbetreibers keine bzw. nur geringe Transaktionskosten für das Agieren auf dem verteilten Marktplatz an, sodass sich solche Marktplätze auch gut dafür eignen, kurzlebige oder immaterielle Güter von geringem Wert zu handeln.<sup>22</sup>

**Permissioned and Permissionless Systems** Regulierte Systeme (**Permissioned System**) erfassen ihre Nutzer, in dem die Identität dieser durch irgendeine Art eines KYB- (Know your Business) oder KYC- (Know your Customer) Verfahrens verifiziert werden, ähnlich

<sup>21</sup> <https://de.Bitcoin.it/wiki/Nonce> (letzter Abruf: 28.07.2015).

<sup>22</sup> Verfahren und Protokolle für sicheren Rechtsverkehr auf dezentralen und spontanen elektronischen Märkten, von Michael Conrad, Dissertation, Karlsruher Institut für Technologie Fakultät für Informatik, 2009, KIT Scientific Publishing 2010.

den Erfordernissen der traditionellen Finanzsysteme. Dagegen sind in einem unregulierten System (**Permissionless System**) die Identitäten der Teilnehmer nicht bekannt. Das Bitcoin-System wurde als unreguliertes System entwickelt. Inzwischen führen jedoch viele der Unternehmen in der Bitcoin-Ökosphäre bereits verpflichtend KYC- oder KYB-Prüfungen durch, daher spricht man auch von einem *permissioned on a permissionless system*.

**Pooled Mining** ist ein Mining-Konzept, bei dem sich mehrere Miner zur Validierung eines Blocks zusammenschließen und die erhaltenen *bitcoins* nach verschiedenen Verteilungsschlüsseln (z. B. beigetragene Rechenleistung) aufgeteilt werden.

**Seigniorage**<sup>23</sup> ist der reale Ertrag, der einer staatlichen oder privaten Institution dadurch entsteht, dass sie in der Lage ist, Geld zu produzieren, dass sie im Tausch gegen Faktorleistungen, Sach- oder Finanzaktiva in Umlauf bringen kann. Der Begriff Seigniorage wird aber überwiegend enger gefasst und als realer Gewinn der Geldschöpfung des Staates bzw. seiner Zentralbank verwendet.

**Sidechains** sind Blockchains, die parallel zur Bitcoin-Blockchain laufen und die miteinander und/oder mit der Bitcoin-Blockchain interagieren und so versuchen, neue Technologien zu realisieren und bestimmte Verhaltensregeln abzubilden.

**Smart Property** ist Vermögen, dessen Eigentum und Besitz über kryptografisch gesicherte Datennetzwerke und intelligente Verträge verwaltet und übertragen wird.

**Smart Contract** Der Begriff wurde bereits 1994 von Nick Szabo<sup>24</sup> geprägt, intelligente Verträge sind Computerprogramme, mittels derer Vertragsbestimmungen automatisch ausgeführt werden. Diese Computerprogramme basieren auf If-then-Anweisungen und interagieren mit realen Vermögenswerten: Tritt eine vorprogrammierte Bedingung ein, löst das Computerprogramm entsprechend der festgeschriebenen Vertragsklausel eine Reaktion aus. Erst durch die Möglichkeit der Verbindung mit einem Zahlungsabwicklungssystem erlangt die Idee der intelligenten Verträge Bedeutung.

**Simplified Payment Verification (SPV)** wird genutzt von Thin-/Light-Clients, z. B. Electrum, Multibit, Bitcoin Wallet für Android, Mycelium und mehr. Diese Clients speichern nicht die komplette Blockchain, sondern synchronisieren in der Regel mit einem Netzwerk von Servern und stimmen eingehende Transaktionen nur mit den Block-Headern oder den letzten Transaktionen ab. In Zukunft, wenn – wie erwartet – das Transaktionsvolumen weiter zunehmen wird, wird es vermutlich eher die Regel sein, leichte

<sup>23</sup> <http://www.wirtschaftslexikon24.com/d/seigniorage/seigniorage.htm> (Abruf: 06.09.2015).

<sup>24</sup> Nick Szabo is a computer scientist, legal scholar and cryptographer known for his research in digital contracts and digital currency. He graduated from the University of Washington in 1989 with a degree in computer science. Übernommen von [https://en.wikipedia.org/wiki/Nick\\_Szabo](https://en.wikipedia.org/wiki/Nick_Szabo) (Abruf: 21.01.2016).

Clients zu verwenden, da normale Rechner von der Kapazität der Festplatten überfordert werden.

**SoftFork** Bei einer SoftFork müssen die Knoten ihre Software auch nach eine Änderung des Bitcoin-Protokolls nicht updaten. Trotz der Programmänderung wird an derselben Blockchain weitergearbeitet.

**Sybil-Attacke**<sup>25</sup> Bei einer sogenannten Sybil-Attacke versucht der Angreifer eines Peer-to-Peer-Netzwerks, möglichst viele eigene Knoten (viele eigene Identitäten) zu erzeugen und damit das System zu korrumpieren bzw. die Abfolge der Transaktionen zu ändern, um ein Double Spending möglich zu machen. Durch den erforderlichen Proof-of-Work bei Validierung der Transaktionen und Finden der Blöcke ist eine Sybil-Attacke, die die Reihenfolge der Transaktionen rückwirkend manipulieren will, um ein Double Spending durchzuführen nur mit unverhältnismäßigen Kapitaleinsatz möglich.

**SWIFT (Society for Worldwide Interbank Financial Telecommunication)**<sup>26</sup> ist eine 1973 gegründete, in Belgien ansässige Organisation, die ein internationales standardisiertes Kommunikationssystem für weltweit mehr als 10.400 Banken über sichere Telekommunikationsnetze (das SWIFT-Netz) in zwei Rechenzentren betreibt. Über diese Rechenzentren schicken sich pro Tag rund 10.500 angeschlossene Geldinstitute aus mehr als 200 Ländern etwa 20 Mio. Nachrichten. Rund 90 % aller internationalen Banktransaktionen werden über dieses Meldesystem abgewickelt. 2013 waren das täglich etwa 20 Mio. internationale Zahlungsaufträge mit einem Gesamtvolumen von 7,5 Bio. Euro. SWIFT ist eine Genossenschaft im Besitz der Banken und dem EU-Recht unterworfen. In diesen SWIFT-Nachrichten teilt beispielsweise eine Bank einer anderen mit, dass für deren Kunde ein Überweisungsauftrag vorliegt, dessen Gegenwert sich die Empfängerbank bitte zu folgendem Termin von dem genannten Verrechnungskonto holen möge und an den Zahlungsempfänger weitergeben soll.

**TOR (the Onion Routing)** Das TOR-Projekt vermischt die IP-Adressen von Internetbenutzern. So ist es nicht mehr feststellbar, wer welche Seiten besucht hat. TOR wird häufig genutzt, um im Netz seine Privatsphäre zu wahren.

**Turing-Vollständigkeit**<sup>27</sup> Mit der Turing-Vollständigkeit eines Systems wird seine universelle Programmierbarkeit beschrieben. Für die Adjektivform turingvollständig wird synonym häufig auch turingmächtig verwendet. Der Name ist abgeleitet vom englischen Mathematiker Alan Turing, der das Modell der universellen Turing-Maschine eingeführt

---

<sup>25</sup> <https://de.wikipedia.org/wiki/Sybil-Attacke> (Abruf: 15.10.2015).

<sup>26</sup> <https://de.wikipedia.org/wiki/SWIFT> (Abruf: 01.01.2016).

<sup>27</sup> <https://de.wikipedia.org/wiki/Turing-Vollst%C3%A4ndigkeit> (Abruf: 01.01.2016).

hat. Eine turing-vollständige Programmiersprache kann verwendet werden, um jede andere Computersprache (nicht nur seine eigene) zu simulieren – es ist ein Satz von Anweisungen, die Bedingungen enthalten, Schleifen und Schreib-/Lesespeicher. Das Bitcoin-Protokoll aus dem Jahre 2009 umfasst die Programmiersprache Script, das (absichtlich) nicht turing-vollständig ist.

**Trustless Asset Management**<sup>28</sup> definiert die Möglichkeit, Vermögensgegenstände wie digitalisierte Werte mittels mathematischer Algorithmen – ohne die Involvierung einer dritten Vertrauensperson – durch Nutzung eines dezentralen Hauptbuches zu verwalten.

**UTXO** Unspent Transaction Outputs<sup>29</sup>

**Wallets** Als Wallets werden sowohl Bitcoin-Clients als auch die Dateien bezeichnet, in denen die Adressen und privaten Schlüssel des Bitcoin-Anwenders gespeichert sind. Der aufsummierte Wert der Adressen steht dem Nutzer als verwendbares bitcoin-Guthaben zur Verfügung. Der Nutzer hat immer die alleinige Kontrolle über seine diversen privaten Schlüssel. Das Wallet dient weiter dazu, Adressen zu generieren und ermöglicht in der Regel auch den Import von Adressen, die von anderen Wallets generiert wurden, sofern der private Schlüssel zu der entsprechenden Adresse bekannt ist.<sup>30</sup>

---

<sup>28</sup> <http://www.ofnumbers.com/2014/02/14/presentation-covering-smart-contracts-smart-property-and-trustless-asset-management/> (Abruf: 01.01.2016).

<sup>29</sup> <https://github.com/ethereum/wiki/wiki/White-Paper> (Abruf: 17.01.2016).

<sup>30</sup> Bitcoin, kurz & gut, Jörg Platzer, O'Reilly Verlag GmbH & Co. KG; 1. Aufl. (Abruf: 29. 09. 2014).

Bitcoins und andere dezentrale Transaktionssysteme

Blockchains als Basis einer Kryptoökonomie

Sixt, E.

2017, XIV, 195 S. 17 Abb., Softcover

ISBN: 978-3-658-02843-5