Einige Erläuterungen zu Geld, Bitcoin und Blockchain

Dr. Makarius Wenzel
https://sketis.net

April 2018

Geld

Was ist überhaupt Geld?

Substanz:

- Bedruckte Papierzettel?
- Geprägte Metallscheiben?
- Besondere Metalle: Kupfer, Silber, Gold?
- Mammon? (Gottheit eines globalen Kultes — ursprünglich phönizisch)

Eigenschaften:

- Schwer zu beschaffen? (Schürfen, Bergbau, Metallurgie, . . .)
- Ergebnis von Arbeit?
- Selten?
- Wertvoll?
- Magisch?

Das Wesen des Geldes

Definition: Geld ist *beglaubigte Rechtsbeziehung* von Wirtschaftsteilnehmern

Rechtsbeziehungen durch Transaktionen:

$$A \xrightarrow[10\ell \text{ Bier}]{\text{liefert an}} B \qquad C \xrightarrow[\text{6h im Garten}]{\text{arbeitet für}} D$$

Unpersönliche Rechtsbeziehungen:

$$E \xrightarrow[\text{100 Credits}]{\text{schuldet}} \qquad \xrightarrow[\text{100 Credits}]{\text{beansprucht}} F$$

Darstellungsformen von Geld

Bargeld: bzw. “Briefgeld”

- Beglaubigung der Rechtsbeziehung auf Papier: durch Verbriefung
- Erzeugung durch Zentralbanken (halb-öffentlich)

Giralgeld: bzw. “Buchgeld”

- Beglaubigung der Rechtsbeziehung auf Konto: durch Verbuchung
- Erzeugung durch Geschäftsbanken (privat, genossenschaftlich, halb-öffentlich)

Bitcoin: bzw. “Kryptogeld”

- Beglaubigung durch Blockchain-Eintrag mit Energieverbrauchsnachweis: durch Verheizen von Rechenleistung
- Erzeugung durch Peers im globalen Wettbewerb (anarchisch)

Buchführung

Geschichte:

Mittelalter: einfache Buchführung auf Basis persönlichen Vertrauens (bzw. Hausgewalt des Herrschers)

Neuzeit: doppelte Buchführung zur Kontrolle (lat. "contra-rotulum") im Unternehmen (u.A. Jacob Fugger und Matthäus Schwarz)

Post-2008 Finanzkrise: Versuche einer globalisierten Peer-to-Peer Buchführung, ohne Vermittler, d.h. keine Banken, Finanzinstitute, Finanzämter, Staaten

Peer-to-Peer:

- wörtlich: jeder Teilnehmer ist den anderen völlig gleich
- typisch: einige Teilnehmer sind noch gleicher
- historisch: Bezeichnung für Mitglieder des französischen Adels

Bitcoin

Was ist Bitcoin?

Primärquelle: von 2008

- Satoshi Nakamoto (Pseudonym, evtl. Mensch aus dem Silicon Valley?)
- Papier: *Bitcoin: A Peer-to-Peer Electronic Cash System*
  https://bitcoin.org/bitcoin.pdf

Prinzipien:

- Mathematik (Kryptographie) und Informatik (Software)
  statt Vertrauen in Institutionen, Recht und Gesetz, staatliche Ordnung
- global verteilte Buchhaltung über Blockchain
- unveränderliche signierte Transaktionen mit Zeitstempel
- leistungsorientiertes Peer-to-Peer Abstimmungsverfahren
- Pseudonyme Teilnehmer: keine Namen sondern asymmetrische Krypto-Keys

Offizielle Darstellung

Website: https://bitcoin.org/de

Werbesprüche:

- Sofort-Peer-to-Peer Transaktionen
- weltweite Zahlungen
- geringe bis keine Transaktionskosten
- keine zentrale Autorität, sondern globales Kollektiv
- öffentliches Design mit Open-Source Implementierung
- gehört niemandem und wird von niemandem kontrolliert
- jeder kann teilhaben

Probleme von Bitcoin

- Transaktionen zu langsam und zu teuer
- unpraktisch für täglichen Einkauf
- hohe Anforderungen an Computer-Sicherheit: Software und Benutzer
- Zentralisierung des Mining: Spezialrechner und Rechenzentren
- Dienstleister:
  - doch notwendig
  - Glücksritter, Raubritter
  - technologische Zusammenbrüche
- keine Währung sondern Spekulationsblase (virtuelle Tulpenzwiebeln), siehe z.B. https://bitcoinmagazine.com/markets

Der Bitcoin-Blockchain Goldrausch

Typische Mitspieler:

- Bitcoin (ab 2008) mit vielen Clones, Forks, Variationen
- Ethereum (ab 2013): Blockchain für "Smart Contracts",
  d.h. Buchungsvorgänge die sich bei Fälligkeit selbsttätig ausführen
- Hunderte Dienstleister bei https://bitcoinmagazine.com/industry/blockchain

Achtung: man unterscheide sorgfältig . . .

1. Technologie
2. Soziologie
3. Ökonomie
4. Idiotie

Blockchain

Bedeutung der Kryptographie

- Wichtige Grundlage für Sicherheit in der Informationstechnik
- Harte mathematische Verfahren auf Basis von Wahrscheinlichkeiten
- Oft politisch stark umkämpft und umstritten: Beteiligung von NSA und NIST an der Entwicklung und Standardisierung

Anwendungen:

- Sicherer Zugang zu Websites über `https` (aber nicht `http`)
- Verschlüsselung von E-mail, z.B. GNU Privacy Guard (GPG), Enigmail
- Merkle-Baum zur Organisation kryptographisch signierter Daten (Ralph Merkle, 1979)
- Blockchain als besonders strukturierter Merkle-Baum (Satoshi Nakamoto, 2008)

Kryptographische Hashes

Prinzip:

- Dokument im Klartext $\rightarrow$ Hash Digest
- Einwegfunktion: Umkehrung bzw. Kollision (fast) unmöglich

z.B. `md5 "Ente"  = "46a991394b46157bb5d369914b54cd58"`
z.B. `md5 "Enter" = "f1851d5600eae616ee802a31ac74701b"`

Einige Standards: mit natürlichem Verfall

MD-5 (Ronald Rivest): 1991 bis 2008, völlig veraltet
SHA-1 (NSA): 1995 bis 2010/2017, teilweise veraltet
SHA-2 (NSA): ab 2001, noch aktuell
SHA-3 (Keccak Team): ab 2015, mögliche Alternative zu SHA-2

Proof-of-work — Energieverbrauchsnachweis

Prinzip

- Quasi-Umkehrung der Hash-Funktion, etwa:
  Gib mir $text$, so dass der Hash mit einer Anzahl Nullen beginnt,
  z.B. `sha1` $text$ = "0000000b2c63ac8b45cccefe27425422ee0d66d0"
- Das einzige bekannte Verfahren: brute-force (alles Durchprobieren)
- Die Mathematik der Wahrscheinlichkeiten bestimmt den Rechenaufwand
- Aber: fortschreitende Computer-Technologie verringert den Zeitaufwand
  tendenziell durch mehr Energieeinsatz und mehr Rechen-Knoten (CPUs, GPUs)

Anwendungen:

- "Hash-Cash" SPAM Filter (1992): Pseudo-Bezahlung für Mail-Zustellung
- Bitcoin (2008): Nebenbedingung für Blocks in der Blockchain

Blockchain als verteilte Buchführung

Prinzip:

- Kette von Datensätzen (Blocks) als linearer Merkle-Baum
- Jeder Block bestätigt den Vorgänger-Block über kryptographischen Hash
- Jeder Block enthält kryptographisch signierte Nutzlast (z.B. Buchungsvorgang)
- Abstimmung der Peers über fortschreitendes Wachstum in *eine* Richtung, ohne Verzweigung

Folgen:

- Unveränderlichkeit: akzeptierte Blöcke können nicht zurückgenommen werden
- Gleichheit der Peers: nach Rechenleistung (Energieverbrauch!)
- Gelegentliches Raubrittertum: Ausnutzung von Fehlern in der Software