H. Wedekind

Bitcoin: Kryptologisches Geld und Währung

Kontinuativa (mass nouns) und Individuativa (count nouns)

„Geld fließt in die Erhaltung eines überzogenen Lebensstandards“ heißt es u.a. in den vielen Kommentaren zur Griechenlandhilfe. Das Politische interessiert uns hier nicht. Wichtig für uns ist die Erkenntnis, dass „Geld“ sprachlich in vielen Fällen auch als *Kontinuativum*, als Stoffname (mass noun) verwendet wird, wobei es völlig gleichgültig ist, welche Einheiten zugrunde liegen. Wenn Einheiten angeben werden können z.B. Euro (€), Dollar ($) etc., dann spricht man von einem *Individuativum* (count noun) oder von einer Währung. Mit Bitcoin (BTC), der kryptologischen Einheit für das Internet-Geld, ist ein neues Individuativum, ein neues „count noun“, in die Welt gesetzt worden, das uns beschäftigen soll.

Der Übergang vom „mass noun“ zum „count noun“ ist in den Wissenschaften gang und gäbe. Denken wir zunächst an den vorbildlich herausgearbeiteten Begriff „Energie“ der Physik als „mass noun“. Wenn wir abstrakt fragen, was Energie sei, bekommen wir konkret zur Antwort, dass es verschiedene Energieformen gäbe. Wärmeenergie, mechanische Energie, Atomenergie, chemische Energie, photo-voltaische Energie usw. werden uns in Erinnerung gebracht. Gleichzeitig wird aber darauf hingewiesen, dass es Äquivalente zwischen den Energieformen gibt, die den Energiebegriff als Abstraktum rechtfertigen. Wohlbekannt ist das mechanische Wärmeäquivalent, dass die Wärmeeinheit Kilokalorie (kcal) mit den mechanischen Meter-Kilopond (mkp) in Äquivalenz setzt. Die Äquivalenz, noch aus der Schule bekannt, lautet: 1 kcal = 427 mkp. Es waren die bedeutenden Wissenschaftler Julius Robert Mayer (1814-1878) und Hermann von Helmholtz (1821- 1894), die im Rahmen ihrer Studien zum ersten Hauptsatz der Wärmelehre diese wunderbare Äquivalenz herausfanden. Helmholtz insbesondere ist durch seine Invarianz-Forschungen in die Abstraktionsgeschichte der Naturwissenschaften als Pionier eingegangen. Energie als „mass noun“, als Begriff ist invariant (unveränderlich) bezüglich der Energieformen, nicht nur von Wärme und mechanischer Energie, sondern auch bezüglich aller anderen Formen.

Nach dem Vorbild Energie, ist der Übergang vom mass noun „Geld“ zum count noun „Geld“ als Geldform einfach. Geldformen in Euro €, in Dollar $ ... haben als Konkreta auch Äquivalenzen untereinander. Als erheblicher Nachteil gegenüber naturwissenschaftlichen Äquivalenzen, die den Rang von Naturkonstanten haben, muss angesehen werden, dass Geldäquivalenzen durch Normierung (also politisch) entstehen, durch Angebot und Nachfrage, die frei sein können, oder auch politisch manipuliert werden. In summa kann gesagt werden, dass Geldäquivalenzen im politischen Raum stehen, damit arbiträr sind und an Exaktheit zu wünschen übrig lassen. Die Zahl 427 im Wärmeäquivalent galt schon, scherzhaft gesprochen, zu meiner Schulzeit vor 65 Jahren und wird weiter gelten. An die damalige Umrechnung DM in $ erinnern sich nur noch vereinzelt einige wenige.

Anmerkung: „mass nouns“ und ihre „count nouns“ gibt es im täglichen Leben in Hülle und Fülle. Nehmen wir das Beispiel „Wasser“ als Kontinuativum. Gezählt wird Wasser als Individuadivum in Form von „Tropfen Wasser“, „Eimer Wasser“, etc.

„Mining“, die Erzeugung von Bitcoins im Internet

Für die Geldform eines Staates hat der Staat das Erzeugungsmonopol. Das war im Altertum auch schon so. Weil Geld im güterwirtschaftlichen Handel gebraucht wird und Güter knapp sind, ist die „Knappheit des Geldes“ und ihre Kontrolle (scarcity of money) zu einem Prinzip erhoben worden. Prinzipien stehen immer ganz am Anfang einer Lehre. Also befassen wir uns mit dem knappen Erzeugen von Bitcoins im sog. „Mining“. So wie man früher mühevoll nach Silber und Gold graben musste, um knappes Geld zu erzeugen, so muss man heute in Analogie eine große Computerleistung aufbieten, um einigermaßen ertragreich zu sein. Das ist die Pointe, und die ökonomische Idee von Bitcoin. Nicht Geldmengenpolitiker der Zentralbanken sollen Knappheit erzeugen, sondern Knappheit wird erzeugt und kontrolliert durch Rechenkapazität und Erzeugungsalgorithmen. Das Notebook vor mir langt nicht; das ist allenfalls Schaufel und Sieb zum Auswaschen von Gold am Yukon-Fluss in Alaska. Würden Notebooks langen, wäre ganz Griechenland mit Notebooks unterwegs zum Yukon. Wir wollen hier, ohne auf die technischen Einzelheiten einzugehen, die oben im Link stehen, nur mal abschätzen, wie hoch der Aufwand z.B. in USD($) ungefähr für eine Bitcoin ist. Man kann heute Bitcoins z.B. mit USD kaufen. Ich könnte heute am 13.09. 2015 um 11:48 ein Bitcoin für 233,68 USD($) kaufen. Der Bitcoin/USD-Hebel (Leverage) liegt nach Internet zwischen 1:2 und 1:4.

Wir nehmen einen Leverage von 1:3 an, so dass hinter $ 233 rund $ 80= € 70 reale Computer-Leistung steckt. Da der Bitcoin-Kurs stark schwankend ist, sollte man von einem Kauf absehen, was ja auch dringend empfohlen wird. Wer sich unglücklich machen will, sollte Bitcoins kaufen. Gäbe es ein Hebeln auch in den Naturwissenschaften, wäre das Perpetuum Mobile schnell erfunden. Unsere Banken hebeln mit etwa 1:10 (Eigenkapital/Gesamtkapital). Auch das wird beanstandet. Heute gibt es weltweit 12 Millionen Bitcoins. Nach Vorhersage wird es 2033 insgesamt 21 Millionen Bitcoins geben. Das heißt doch im Shakespeare‘schen Sinne: “Much ado about nothing“ (Viel Lärm um nichts)? Vergleichen wir 21 $x10^6$ Bitcoins im Jahre 2033 einmal mit der „Dicken Berta“ (Draghi Mining) zur Euro-Stützung der EZB, € 500 x 10^9, die die EZB so aus dem Ärmel schüttelt, auch wenn 1 Bitcoin weiter rund 70 € wert sein sollte, dann sieht die Bitcoin-Währung gegenüber der „Dicken Berta“ doch aus wie eine Spielzeugkanone für Kinder.

Asymmetrische Verschlüsselung: Public Key, Private Key

Die ökonomische Idee von Bitcoin ist die Erzeugung von Knappheit durch Rechner mit ihren Algorithmen. Die technische Idee von Bitcoin steckt im RSA-Verfahren der Computer-Kryptografie, benannt nach den berühmten Erfindern Rivest, Shamir und Adleman (1978), die für ihre Leistung mit dem Turing Award (auch genannt der Nobel-Preis für Informatiker) erst 2002 geehrt wurden. Der Aufsatz war die Geburtsstunde der modernen Computer-Kryptografie. Erfunden hat den Bitcoin 2008 ein Japaner namens Satoshi Nakamoto.

Geld ist ein hochsensibles, universelles Gut und hochgradig unlauteren Begehrlichkeiten ausgesetzt. Diebe klauen am liebsten Geld. Die Sicherheitsstandards müssen sehr hoch sein, so hoch wie bei „top secret“-Angelegenheiten im politischen, wie auch im unternehmerischen Geschäft. Man muss verschlüsseln, also eine Information für Unberechtigte in eine nicht lesbare Form bringen. Der Haken ist der Schlüssel, mit dem man verschlüsselt. Er wird klassisch symmetrisch zum Verschlüsseln wie

auch zum Entschlüsseln benutzt und dürfte eigentlich gar nicht über angreifbare Verbindungen kommuniziert werden. Ein Schlüssel ist das sensibelste in unserem Geschäft und sollte prinzipiell eigentlich nicht über Leitungen geschickt werden.

Geht das überhaupt? Antwort: Ja, wenn man einen Verschlüsselungs-Schlüssel (public key) von einem Entschlüsselungs-Schüssel (private key) trennt. Beim „public key“ wird die Festung „key“ von vornherein aufgegeben, wie der Name „public“ schon sagt. Das Wort ist streng genommen ein Widerspruch in sich. Der „private key“ bleibt geheim beim Sender. Er verschickt den „public key“ des Empfänger, die Nachricht, hier der Geldbetrag in Bitcoins und eine Signatur als Authentifikation, mit der der Empfänger die Nachricht entschlüsseln kann. Was hier so leicht erklärt wird, ist aber beachtlich kompliziert. Mathematiker-Herzen erfreut das. Es wird sogar ein Primzahlsatz von Euler herangezogen. Ungewöhnlich, dass die mathematische Zahlentheorie eine praktische Verwendung gefunden hat. Die Theorie darzustellen, würde unseren Rahmen sprengen. Wir verweisen aber für den mathematischen Laien auf Christoph Bergmann „Bitcoins für Anfänger“.