

Jour fixe vom 25.10.2021

Bitcoin – „freies Geld“ für freie Bürger (GS 3-21)

Im Vorspann bezieht sich der Artikel darauf, wie man sich in der bürgerlichen Welt von der kryptographischen Welt der Verschlüsselung beeindruckt zeigt. Was da beeindruckt, das sind erst einmal die großen Dollarsummen.

— *Für den bürgerlichen Sachverstand ist es selbstverständlich, dass auf einem Euroschein 100 Euro steht und der auch so viel wert ist oder dass Aktienwerte an der Börse steigen. Worüber stolpert er beim Bitcoin? Ohne näheren Gedanken nimmt er den als eine im Internet beheimatete digitale Währung, über die der Staat nicht seine Hand hält. Das sieht er skeptisch. Andererseits kriegt er mit, dass Bitcoins schon an der Börse gehandelt werden und es da um Millionen geht. Das versöhnt ihn wieder: Wenn etwas zu so viel Reichtum führt, kann es so verkehrt nicht sein!*

Der Bitcoin gilt als ein Phänomen, das eigentlich nicht zu der Welt passt, wie man sie in Gestalt von Währungen, Kultur usw. kennt. Ohne sich groß um eine Erklärung zu kümmern, wird dieses neue Phänomen aber in die eigene Vorstellungswelt eingemeindet. Das ist von vorneherein eine affirmative Einstellung zu den Verhältnissen, wie sie sind. Zu klären ist, was da eigentlich eingemeindet wird.

— *Die öffentliche Meinung in Form von SZ-Kommentaren im Wirtschaftsteil etc. schlägt eine Kurve vom negativen Urteil über ein Geld, von dem man sich nichts kaufen kann, hin zu dem Imperativ, man solle von so einem Kunstgeld, das doch eigentlich nichts wert sein sollte, nichts halten. Dieses anfängliche Urteil wird dann revidiert angesichts der vielen Leute, die auf das Ding spekulieren. Im Ergebnis verbeugt er sich vor der Realität und vor der gesellschaftlichen Praxis und anerkennt das Ding.*

Zur Verbeugung vor der Realität: Einerseits weiß man nicht so recht, was man von dem Ding halten soll und womit man es da zu tun hat, andererseits wird es von Vielen benutzt und geschätzt – also muss man sich dem anschließen. Dass etliche Menschen durch die Spekulation damit und darauf reich geworden sind und dass es sich damit erfolgreich bewährt hat, wird zum Argument gemacht: Dann kommt man um das Ding nicht herum.

*

— *Zu **Punkt 1.** (S. 69): Nakamotos kritische Diagnose lautet: Das Geld taugt nicht ordentlich für den darauf angewiesenen Bürger als Zahlungsmittel. Das merkt er an zwei wesentlichen Punkten: Es gibt eine Inflation, die der Staat nicht nur zulässt, sondern von sich aus auch betreibt. Und die Banken verlangen Gebühren, neuerdings sogar Negativzinsen und spekulieren mit dem Geld der Bürger. Alles Dinge, die Nakamoto für untauglich hält. Vor diesem Hintergrund hat er sich seine digitale Währung ausgedacht.*

Bevor man zu seiner Lösung kommt, muss man klären, inwiefern er das Geld für nicht tauglich hält. Von welchem Standpunkt aus sind Bankgebühren und Inflation überhaupt kritikabel?

— *Nakamoto nimmt den Standpunkt des Geldbenutzers ein. Von dessen Betroffenheit aus beurteilt er, was Geld zu leisten hätte und hält für das Eigentliche am Geld, dass es zum Kaufen, Verkaufen und Aufbewahren da ist. Vom Standpunkt der Nützlichkeit für den Konsumenten beurteilt er die Qualität des Geldes und zieht eine negative Bilanz. Das Geld wird missbräuchlich benutzt, indem Staat und Banken es für ihre eigenen Geschäfte benutzen, es darüber entwerten und deshalb das Vertrauen, das man ihnen als den Verwaltern dieses Geldes entgegenbringen muss, nicht verdienen.*

Die zwei Sachen gehören zusammen: Erst einmal bezieht sich Nakamoto auf bestehende Verhältnisse, in denen es ein Geld gibt, mit dem alle Subjekte der Ökonomie umgehen und von dem sie wollen, dass es gut funktioniert. So bezieht er sich *positiv* auf das Geld als etwas Nützliches. Von daher sagt er im zweiten Schritt, das Dumme am Geld sei, dass die Zentralbank, der Staat und die Banken das eigentlich gute Geld in seiner Tauglichkeit ständig mindern, indem sie es missbräuchlich verwenden. Erst dann kommt der Übergang dazu, dass Nakamoto eine andere Währung will. Vorher sagt er vom Geld nur, dass man es braucht, es funktionieren muss und das Schlechte daran ist, dass man es den Banken anvertrauen muss. Dadurch funktioniert es nicht so, wie es eigentlich funktionieren sollte, müsste oder könnte. An diesem Punkt setzt er ein und entwickelt Alternativen für ein

besseres Funktionieren des Geldes.

— *Mit der Diagnose, Geld werde in seinem Nutzen gemindert, weil sich andere Instanzen dazwischen schalten, kommt er ja auch ganz funktionalistisch zu dem Schluss, dass ohne Dazwischentreten dieser Instanzen das Geld ein viel besseres Geld wäre. Das ist der Bauplan für seine Therapie und für seine Konstruktion eines Geldes, das ohne diese Vertrauensverhältnisse mit Staat und Banken funktionieren kann, also ungeschmälert seinen Dienst tut.*

Er legt den Maßstab des Funktionierens an die Welt des Geldes an: Das Geld soll für den Menschen konstruiert sein, der mit dem Geld einkaufen geht. Über das echte Geld, das es gibt, hat er das falsche Urteil, eigentlich sei es *dafür* da, werde aber von den Instanzen missbraucht und leide deshalb in seiner Funktion. Diesen theoretischen Unsinn konstruiert er schon im Hinblick auf das, worauf er damit hinaus will.

— *Die Mängel macht er nicht am Geld fest, sondern an den Instanzen, die damit schlecht umgehen.*

— *Er fasst es prinzipieller: Dass beim Tausch überhaupt eine Drittpartei notwendig ist, sieht er als prinzipiellen Mangel für die Funktionen des Geldes. Für ihn ist das Kernproblem das „Ausmaß an Vertrauen“, das erforderlich ist. Weil für ihn das eigentliche Problem ist, dass jemand anderer dazwischentritt, widmet er sich kritisch dem, was bei diesen Drittparteien seiner Meinung nach im Hinblick auf die Funktion des Geldes alles schiefgehen kann. Dagegen erfindet er gewissermaßen eine Missbrauchsverhinderungskonstruktion.*

Diese Argumente widersprechen sich nicht: Er macht alle Mängel so am Geld vorstellig, dass da eine dritte Partei zwischen die zahlungswilligen Figuren tritt und das eröffnet des Feld des Missbrauchs. Diese dritten Parteien verdienen daher das Vertrauen nicht und deswegen ginge es darum, dass die Zahlungswilligen sich selber ein Geld schaffen, das alle Dritten aus ihrem Zahlungsverkehr ausschließt und damit von Betrug, Übervorteilung oder Gebühren frei ist.

— *In seinem ersten Zitat bemängelt er am Geld, dass damit Kredit geschöpft wird: „Sie verleihen es in Wellen von Kreditblasen mit einem kleinen Bruchteil an Deckung“. Sein Geld dagegen kann man nicht mehrfach verwenden, eine Geldschöpfung durch Kredit will er mit seinem Geld unterbinden.*

Das ist eine nähere Ausführung zu dem, wie Nakamoto den Missbrauch des Geldes durch die Banken bestimmt. Von seinem Standpunkt aus ist das Geld eine Einrichtung, die in dem Dienst aufgeht, den sie Austauschwilligen fürs Bezahlen leistet. Mit dieser Funktion ist das Geld für ihn fertig bestimmt. Wo die Banken mit ihrem Kreditgeschäft ein ganz anderes Interesse am Geld praktisch machen, ist das für ihn ein Missbrauch des Geldes für ihre eigennützigen Zwecke und das macht das Geld für seinen eigentlichen Zweck schlecht tauglich. So macht er sich an die Konstruktion eines Geldes, das allen schädlichen Einfluss Dritter ausschließt.

— *Das ist dann das elektronische Zahlungsverfahren, das er in die Welt gesetzt hat. Da gibt es keine dritten Parteien mehr, denen man vertrauen muss, sondern durch das Internet wird eine direkte Zahlung zwischen Gebern und Empfängern ermöglicht. An der Stelle kann man schon den Widerspruch festhalten, den sich Nakamoto leistet: Durch das Verfahren sollen Waren bezahlt werden. Das unterstellt allerdings, dass die Waren an sich einen Wert haben. Dafür ist das Geld in der realen Welt ja da: Maß der Werte zu sein, das den Wert der Waren bezeichnet. In Nakamotos Vorstellung soll das Geld als solches aber keine Rolle mehr spielen.*

Seine Konstruktion lebt nicht davon, dass er weg will vom Geld, sie lebt davon, dass er weg will vom *Vertrauen* in das Geldwesen. Dass er dabei das, was Geld der Sache nach ist, um die Ecke bringt, ist eine Konsequenz seiner Diagnose und seiner Konstruktion. Das Zitat auf S. 70 ist eine Auskunft über das von ihm identifizierte Kernproblem, man brauche eine vertrauenswürdige Partei. Hierfür bietet er den Zahlungswilligen eine Konstruktion, die das Vertrauen in eine Partei ersetzt durch einen kryptographischen Nachweis, also ein mit Verschlüsselungstechnik konstruiertes Zahlssystem, das in Übertragung von Datenketten von ‚Gleich zu Gleich‘ (peer to peer) besteht. Das ist sein Angebot.

Er konstruiert also eine *andere* Art von Zahlungsverfahren. Dieses Vorhaben enthält in seinem Ausgangspunkt schon den Widerspruch, dass das im Prinzip keine andere Art und Weise des Umgangs mit dem Geld ist, das es gibt. Er jedoch macht sich getrennt davon an einem Verfahren zu schaffen, das Dritte ausschließt und sicherstellt, dass genau das übertragen wird, was übertragen werden soll. Dieses *Verfahren* identifiziert er dann mit einem gut funktionierenden Geld. Vom Ausgangspunkt her moniert er, dass das existente Geld schlecht funktioniert. Seine Verbesserungen desselben münden darin, dass sein zu entwerfendes und zu praktizierendes Zahlungsverfahren ein Geld schafft, das all diese Probleme nicht mehr macht. In diesem Sinne ist der oben genannte Widerspruch zu verstehen: Er löst sich los von dem Geld, um das sich in dieser Gesellschaft alles dreht, um es perfekter funktionieren zu lassen.

— *Wenn er sich an die Verbesserung des Geldes als Mittel des Zahlungsverkehrs macht, bringt er den Stoff, um den es geht, um die Ecke, während er vorher (S. 71 unten) bei allen Transaktionen, die er für unzulänglich befindet, unterstellt, dass es ein Geld gibt, um dessen Verbesserung man sich bemühen muss.*

*

Das erste Zitat unter **Punkt 2.** auf S. 72 unten führt aus, wie dieses Zahlswesen, die Coins funktionieren sollen und macht die Verabschiedung Nakamotos von seinem Ausgangspunkt noch einmal deutlich: Perfektioniert werden sollen ja Kaufen und Verkaufen, vertragsmäßige Erfüllung von Tausch und Zahlung. Sein Endpunkt ist die Definition seiner elektronischen Münze als Kette digitaler Signaturen. Das ist natürlich der Sache nach kein Geld. Was der im Zitat genannte Zahlungsempfänger erhält, ist nämlich nichts anderes als diese Kette digitaler Signaturen. Es ist nur der Anspruch, das soll mit Zahlung verwechselt werden; also der Anspruch darauf, dass dieses Verfahren, diese Coins Eigentum übertragen, wenn nur der Übertragungsweg sicher gemacht ist. In seiner Konstruktion aber kommt das Eigentum gar nicht vor.

— *Inwiefern nimmt Nakamoto seinen eigenen Ausgangspunkt zurück und was genau ist der Widersinn dieser Ersatzgelddefinition?*

Er entfernt sich von der *Sache*, um die es beim Geld geht – von dem Geld, in Form von Münzen und Scheinen, auf das der Staat die Menschheit als *das* gültige Geld der Gesellschaft verpflichtet. Das ja auch irgendwie anders gestaltet sein könnte. Es ist der Sache äußerlich, welche Form das Geld hat, das der Staat als das verbindliche Zahlungsmittel dieser Gesellschaft garantiert. Über die festgelegte Form ist aber nicht zu vergessen, was das Geld der Sache nach ist: ein ganzes gesellschaftliches Produktionsverhältnis. Das Geld *ist* Eigentum, genauso wie es Eigentum an Sachen und Produktionsmitteln gibt. Es ist Eigentum in dem Sinn, dass man erstens exklusiv darüber verfügt und es zweitens durch den Staat die garantierte Macht hat, auf den stofflichen Reichtum eines anderen zuzugreifen. Es sind also nicht bloß beliebige Zettel, die man als Geld verwendet. Der Witz des Geldes, diesem durch den Staat in die Welt gebrachten Quantum, ist, dass es gesellschaftliche Verfügungsmacht über und Zugriff auf den Reichtum der Gesellschaft darstellt.

Im Zitat auf S. 72 kommt der Zugriff auf den materiellen Reichtum der Gesellschaft, der Ausschluss oder Zugriff auf Waren, die getauscht werden sollen, nicht mehr vor. Da findet gar kein Austausch statt. Das Einzige, was bei Nakamoto hin- und hergeschoben wird, ist die sorgsam protokollierte Übertragung von exklusiven Eigentumsrechten an Datenmengen von Person A auf Person B. Worüber da exklusiv verfügt werden soll, ist nichts anderes als das Protokoll darüber, dass etwas, was vorher A gehört hat – diese eine Datenkette –, jetzt B gehört, und der, solange es ihm gehört, ausschließlich *darüber* verfügen kann. Das ist hier der ganze Inhalt von Eigentum. Ein Verhältnis zum stofflichen Reichtum der Gesellschaft, also Eigentum im Sinne der Privatmacht der exklusiven Verfügung *über etwas*, ist das nicht. Eigentum ist es nur ganz formell, dass niemand außer man selbst über dieses Konstrukt verfügt. Das ist die Art und Weise, sich von dem, was Geld in dieser Gesellschaft, was Tausch, Kauf und Verkauf ist, zu verabschieden.

Die Konstruktion Nakamotos soll die ideale Form der Übertragung von Eigentum sein. Er spricht zwar von Zahlung und Eigentumsübertrag, der Eigentumsübertrag besteht aber nicht im Übertrag von Zugriffsmacht. Das Einzige, was hier an Eigentum übertragen wird, ist das

Protokoll der Transaktionen.

— *Die Konstruktion ist also rein formell. Er nennt es Geld, an dem man ein Eigentum hat, und überträgt das als diese Zugriffsmacht auf einen anderen, der dann der Besitzer dieses Datenhaufens ist und das dann auch Geld nennt. Die wirkliche Qualität von dem Geld, auf das man vom Staat verpflichtet ist, Zugriffsmacht auf den gesellschaftlichen Reichtum zu sein, wird damit nicht erfüllt. Er beschränkt sich auf die formelle Seite: Es ist ein Zettel, auf dem Geld steht, den kann man digital übertragen. So etwas konstruiert er jetzt selbst.*

Es geht allein darum, dass derjenige, der als Eigentümer eines Coins geführt wird, wirklich der Eigentümer ist. Der Empfänger bekommt die exklusive Verfügung darüber, diesen Datenhaufen wieder an den Nächsten zu übertragen. Das Internet verlässt der Datenhaufen nicht, er bewegt sich immer nach dem Kommando dessen, der aktuell das Zugriffsrecht auf ihn hat. Mehr wird da nicht übertragen. Das ist das *Selbstreferenzielle* an dem Ganzen: Es wird immer wieder aufs Neue darauf Bezug genommen, dass das, was transportiert wird, auch wirklich das ist, was transportiert wird.

— *Welche Eigentumsvorstellung herrscht in diesen Transaktionsprotokollen vor?*

Die bleibt ganz bei der Formalie des Ausschlusses: Eigentum ist, dass man ausschließlich darüber verfügt. Daher muss so sorgfältig protokolliert werden, dass, wenn A an B etwas weg gibt, damit das Eigentumsrecht von A erlischt. Es ist dann bei B und kann nicht gleichzeitig von A an C übertragen werden. Diese Eigentumsvorstellung zeichnet sich dadurch aus, dass die Protokolle vor Manipulation sicher sind.

— *Wie ist das mit dieser Kette zu verstehen?*

Die Kette ist das Verschlüsselungsverfahren, das die korrekte Übertragung gewährleistet und den aktuell Verfügungsberechtigten dokumentiert.

— *Ist das eine Art Transparenz?*

Es ist ein Verschlüsselungsverfahren, das das Verhältnis der beiden gerade an einer Übertragung Beteiligten und die Autonomie der Übertragung sicherstellt. Der Erhalt eines Coins wird penibel festgehalten, damit jeder nur über das verfügt, was erklärtermaßen seiner Verfügung unterliegt. Der Übertrag soll fälschungssicher, anonym und nicht änderbar sein. Die Beteiligten sollen direkt miteinander interagieren in einer verschlüsselten Form, sodass die Privatsphäre nicht preisgegeben werden muss. Alles muss verschlüsselt und kodifiziert sein. Zugleich soll für jedermann ersichtlich sein, dass alles ordnungsgemäß ist, weil sonst der Schlüssel des einen nicht zum Schlüssel des anderen passt. Ein solches Protokoll, diese Art Kassenbuch zu führen ist eine ziemlich aufwendige Angelegenheit und erfordert erheblichen Rechenaufwand.

Nakamoto richtet das Übertragungswesen als dezentrales Netzwerk von Teilnehmern ein, die alle sein Programm verwenden. Als gemeinsame, dezentrale und für jeden Teilhaber einsehbare Datenbank existiert das, was bereits angesprochen wurde: Jeder kann die Richtigkeit des gesamten Hin und Hers verfolgen und es ist klar zugewiesen, worüber jeder verfügen kann. Im Text wird das als „virtueller Geldbeutel“ bezeichnet. Die sichere Übertragung geht so, dass immer eine Blockchain fortgeschrieben wird, in der alle Übertragungen nacheinander aufgelistet und damit auch nicht mehr veränderbar sind.

— *Die Blockchain soll willkürliches Kopieren und Vervielfältigen des digitalen Geldes im Prinzip ausschließen. Es soll keine falschen Coins geben und ein Vervielfältigen, also eine nach oben offene Geldmenge soll nicht möglich und darüber der Wert des Kunstgeldes gesichert sein. Die gerade genannte große Rechenleistung ist für die Übertragung Pizza gegen Coin nicht nötig, das betrifft doch vielmehr das Schöpfen neuer Coins.*

Eine Übertragung von Bitcoin gegen z.B. eine Pizza ist gerade nicht Inhalt und Gegenstand einer Blockchain. Hier wird keine Pizza bestellt, sondern es werden digitale Datenhaufen hin und her geschoben, die als Coins bezeichnet werden. Diese Transaktionen werden protokolliert und eindeutig ihren Eigentümern zugeordnet. Dafür wird ein erheblicher Rechenaufwand betrieben. Die Art und Weise, wie die Information verschlüsselt und abgespeichert wird, soll verhindern, dass sich jemand in den Besitz von Bitcoins bringt, die er nicht auf dem vorgeschriebenen Übertragungsweg erhalten hat. Dafür muss dieses dezentrale Kassenbuch fälschungssicher sein und es muss ausgeschlossen sein, dass dort

jemand willkürlich kopieren und vervielfältigen kann. Die Auflistung der erfolgten Transaktionen, die ihrerseits das Eigentum ausmachen, das transportiert werden soll, wird ständig in verschlüsselter Form fortgeschrieben. Das heißt Blockchain, weil die verschlüsselte Form so aussieht, dass immer ein gewisser Teil der Transaktionen in einem Block zusammengefasst wird und dann – wie in einer Kette – ein neuer Block angehängt wird.

— *Wenn sich diese Aktionen in der digitalen Community verbreiten, kann es doch dabei nicht stehen bleiben, nur Datensätze hin und her zu schieben. Es kommt doch darauf an, dass der Bitcoin tatsächlich die Funktion eines Zahlungsmittels erhält und den Austausch von Eigentum anstoßen kann?*

Im Text ist dazu von einem „Disneyland im Cyberspace“ die Rede. Damit wird auf den Irrsinn hingewiesen, dass ein umfangreiches Datennetz mit diversen Teilnehmern aufgebaut wird, die heftig hin und her transferieren, codieren und verschlüsseln – ohne dass irgendwas von dem passiert, was bei Tausch und Verkauf in der realen Welt vorkommt. Was bei diesen Leuten aber sehr wohl vorkommt, ist der Standpunkt, dass Eigentum das ist, worauf es ankommt; und dass darauf geachtet werden muss, dass es gesichert, bewahrt und nicht gefährdet wird.

— *Es geht um den Fanatismus, das Eigentum mit einem enormen Aufwand an elektronischer Sicherheit nach seiner formellen Seite hin abzusichern. Das resultiert aus dem Urteil, dass das wirkliche Geld nicht richtig gesichert ist. Dritte missbrauchen es für eigene Zwecke, anstatt mit ihm das Tauschverhältnis abzusichern.*

— *Der Ausgangspunkt von Nakamoto war, für die Bürger die Zahlung mit Geld sicher zu machen. Gelandet ist er in diesem Disneyland, in dem man Bitcoins hin und her schiebt, die für sich keinen Wert darstellen.*

— *Warum sollten die Beteiligten einfach so Datensätze hin und her schieben, was soll das für einen Zweck haben? Unterstellt ist doch, dass derjenige, der die Bitcoins verschoben hat, irgendwas dafür bekommt. Warum sollte er das sonst tun? Er will doch nicht einfach wertlose Bitcoins bei sich auf den Computer sammeln. Das kommt einem wie eine Farce vor, weil sie mit ihrem Hin- und Herschieben der Daten, das minuziös protokolliert wird, dem Kauf und Verkauf den ganzen gesellschaftlichen Inhalt rauben.*

Es geht nicht darum, ob deren Programm gut, schlecht oder gar nicht als Geld funktioniert. Hier sollte ein Argument gegen den Inhalt des Treibens dieser Leute vorgebracht werden. Als Mitglieder einer funktionierenden Marktwirtschaft ist ihnen nichts so selbstverständlich wie der Umgang mit Geld. Aus ihrer Unzufriedenheit heraus, wie das Geld für sie funktioniert und wie sie über Wertverlust und Kosten klagen, leisten sie sich diese wertlose Veranstaltung im Internet. Hier können sie ganz fälschungssicher und anonym ihr Eigentum ohne Eingriff von Dritten hin und her schieben – ganz ohne wirkliches Eigentum. Sie organisieren im Internet in dieser inhaltslosen Form eine Nachbildung gesellschaftlicher Verhältnisse, in denen es Eigentum braucht, um auf fremdes Eigentum zugreifen zu können. Diese Absurdität leisten sie sich von ihrem Bedürfnis her, eine eigene, selbst kontrollierte, nicht von Dritten abhängige, nur ihrem Interesse als ausschließende Eigentümer dienende Veranstaltung zu machen.

Dafür müssen sie gar nicht persönlich unter einer Inflation leiden. Für die Teilnehmer ist das eine sehr frei gewählte Betätigung: Sie beweisen (sich), dass sie das im Internet viel besser beherrschen als die Leute im wirklichen Leben mit dem wirklichen Geld.

*

In Nakamotos Software ist auch eingebaut, wie man zu Coins kommt. Wenn man sich um dieses gemeinschaftliche Netzwerk verdient macht, indem man sich mit dem entsprechenden Rechenaufwand an dieser Buchführung beteiligt, dann gibt es – nachdem man mit noch mehr Rechenaufwand erfolgreich sinnfreie Rechenaufgaben gelöst hat – als Lohn dafür eine entsprechend definierte Anzahl oder auch Bruchzahl von (neuen) Coins, die man sich selber gutschreiben kann.

— *Auf S. 75 unten steht, wer als erster mit dem Block anfängt und ihn fortschreibt, erhält aus dem Nichts die dafür ausgelobte Menge an Bitcoins. Fällt das unter die im Zitat erwähnte Konvention, dass sie das unter sich ausgemacht haben?*

„Durch Konvention“ heißt, dass Nakamoto das so festgelegt und programmiert hat. Das betont das Willkürliche daran. Von Nakamotos Standpunkt aus soll das ein Anreiz dafür sein, sich mit Rechenleistung, für die ja Stromkosten in echtem Geld anfallen, an dem dezentralen Netzwerk zu beteiligen und es damit überhaupt zu ermöglichen.

— *Geht es beim 'Mining' darum, wie man überhaupt an Bitcoins kommt? Wird man in der virtuellen Welt der Bitcoins dadurch reicher, dass man diese Rechenaufgaben löst?*

Das 'Mining' ist der einzige Weg, wie neue Bitcoins ins Internet gelangen. Jemand muss den Rechenaufwand, der nötig ist, um einen neuen Block zu erstellen, als erster erledigen.

— *Dabei muss jemand ein kryptographisches Rätsel lösen und bekommt als Belohnung neue Bitcoins. Liegt darin nicht eine neue Bestimmung? Bisher ging es dem Erfinder darum, ein Zahlungsverfahren in die Welt zu setzen, das 'Mining' zielt nun darauf, zusätzliche Zahlungsmittel zu bekommen – mit der Besonderheit, dass es für sich keinen Wert hat, sondern im Verfahren aufgeht.*

Das ist ein gewisser Übergang. Ausgangspunkt war, Eigentum sicher zu übertragen. Durch die Verschlüsselung und die Art und Weise der Speicherung im Internet kann Eigentum in dieser absurden Form übertragen werden. Der Form nach ist es Eigentum, der Sache nach die Dokumentation seiner eigenen Übertragung. Zweck ist ja eine Verbesserung des Zahlungssystems und des Austauschs. Mit dem 'Mining' wird deutlich, dass es auch bei dieser Sorte Reichtum denjenigen, die damit hantieren, nicht nur auf seine Übertragung und Dokumentation ankommt. Daran anknüpfend hat Nakamoto dieses ‚Mining‘-Konstrukt so ausgelegt, dass es den Teilnehmern einen Weg aufzeigt, wie sie sich diese Sorte Eigentum in erweitertem Ausmaß beschaffen können: Indem sie sich verdient machen um die Codierung und an die vorhandenen Ketten einen neuen Block anhängen. Das ist als Wettbewerb organisiert: Wer als erster weiß, wie der aussehen soll, bekommt als Lohn dafür neue Bitcoins.

— *Was nur eine sichere Übertragung sein soll, wird so verfälscht. Indem sich jemand um diese komplizierte Übertragung verdient macht, geht das über die Übertragung hinaus und es wird ein Mehr erzeugt.*

— *Warum soll das verfälscht sein? Der Abschnitt zeigt doch, dass sie das Tauschen weniger interessiert als der Zugriff auf das Eigentum anderer.*

„Verfälschung“ trifft das nicht. Es ist die einzige Art und Weise, wie man überhaupt ohne Tausch an Bitcoins kommt: Man macht sich auf die genannte Art und Weise verdient um das Zirkulieren des Geldersatzes und so verdient man sich die neuen Coins. Das ist der Weg, wie der Geldersatz als jemandes Eigentum auf die Welt kommt. Offensichtlich geht es denen darum, sich selber in die Verfügung über Bitcoins zu bringen und diesen Geldersatz bei sich aufzuhäufen. Ganz wie in der analogen Welt des Geldes, geht es da nicht einfach bloß um das Zirkulieren der vorhandenen Bitcoins, sondern um ihre Vermehrung.

— *Sie kriegen mit, dass es in der realen Welt des Geldes darum geht, dass es mehr werden muss. Das kopieren sie und bringen mit dem 'Mining' immer neue Bitcoins in Umlauf.*

Natürlich sind diejenigen aus dieser Gemeinde, die sich um den Bitcoin verdient machen, auch am Zugriff auf mehr Eigentum davon interessiert. Das ist aber zu unterscheiden vom Zweck der Konstruktion, die Nakamoto mit seinem 'Mining' in die Welt setzt. Ihm geht es nicht um die *unendliche* Vermehrung, seine Sorge gilt *bei* der Vermehrung der *Beschränkung* der Masse seines Ersatzgeldes.

— *Wichtig ist es, festzuhalten, dass die Community ihre Bitcoins selber schöpft, also ohne Dritten zwischen diesen Akteuren. In dieses Programm ist die Generierung neuer Coins eingeschrieben. So verwirklichen sie ihre Kritik am realen Geld, nämlich, dass da durch das Dazwischentreten Dritter, Banken etc. eine Verfälschung des Geldes stattfindet. Alle Konstruktionsmomente des Bitcoin sind der Ausfluss der falschen Theorie Nakamotos über das Geld.*

Auf S. 76 oben ist davon die Rede, dass der Staat Maßnahmen ergreift, um sein Geld fälschungssicher zu machen. Analog dazu baut Nakamoto in sein Programm ein, dass niemand sich einfach Bitcoins beschaffen kann. Es gibt dafür nur den einen im System eingebauten Weg. Zur Analogie gehören auch immer die Vergleiche Nakamotos mit dem

Geld der realen Welt wie der mit dem Goldgräber auf S. 75.

— *Beim Vergleich des 'Minings' mit Goldgräbern, den sie bemühen, liegt eine falsche Analogie vor: Wenn nach Gold gegraben wird, ist bereits unterstellt, dass dieses Metall zur Geldware geworden ist. Diese Leistung ist keine natürliche Eigenschaft, sondern Werk des Staates. Nakamoto tut so, als erschaffe man durch die Beteiligung am 'Mining' die Geldqualität des Bitcoins.*

Der Aufwand beim Goldgraben führt zum Besitz eines Gegenstands, den man entweder in Geld umtauschen kann oder der selber den Zugriff auf den materiellen Reichtum gewährt, weil Gold das Geld der Gesellschaft ist. Beim Bitcoin wird zwar auch einiger Aufwand getrieben, aber das Resultat ist kein Geld, kein Zugriffsmittel auf den Reichtum der Gesellschaft. Es bleibt bei dem Formalismus der ausschließlichen Verfügung über das Eigentum, der nur darin besteht, dass protokolliert wird, wie es transportiert wird. Das, was man da sein Eigentum nennt, sind Daten, die hin und her wandern und deren Transaktionen dann in einer Art Kassenbuch dokumentiert werden.

*

Zur eingebauten Knappheit: Warum legt Nakamoto so viel Wert auf die absolute Beschränkung der Masse seiner Coins und baut entsprechende Hürden in sein Programm ein? Evident ist, dass er dabei auf bürgerliche Inflationstheorien zurückgreift. Worin liegt der Unterschied?

— *Das Stichwort von der Knappheit, das Nakamoto aufgreift, hat seine Grundlage in der verkehrten bürgerlichen Vorstellung, dass, wenn zu viel Geld unterwegs ist, das 'richtige' Verhältnis von Geldmenge und bestehendem Warenberg beeinträchtigt werde und so zur Inflation führe. Nakamotos Bemühen um Beschränkung und Seltenheit seines Ersatzgeldes ist insofern ein Irrwitz, als er das Verhältnis von Ware und Geld in ein Verhältnis des Bitcoin zu sich selbst verwandelt. Mit der Einprogrammierung willkürlich gesetzter Schranken sollen all die Gefahren, die er dem „Fiatgeld“-Verkehr beimisst, beseitigt sein. Er macht durch seine Vorschrift Seltenheit und Knappheit praktisch wahr.*

Mit diesem Formalismus soll die Wertbeständigkeit und Transfersicherheit des Bitcoin, den er aus dem Nichts geschöpft hat, gewährleistet sein. Nakamoto sucht nicht wie bürgerliche Ökonomen nach dem 'richtigen' Verhältnis von Warenmenge und Geldmenge. Sein Rezept heißt, einfach den Zuwachs der Bitcoin-Menge beschränken. Er definiert dazu Grenzen sowohl nach der absoluten Menge – bei 21 Mio Bitcoins ist Schluss – als auch nach der Seite der Geschwindigkeit seiner Vermehrung und schreibt sie in sein Programm. Der Sache nach sind diese Grenzen vollkommen willkürlich und unbestimmt.

*

Der nächste Termin findet am **8. November 2021** statt. Weiter geht es mit dem Artikel über den Bitcoin im GS 3-21 ab Seite 78. Das nächste Thema wird auf der Website des GegenStandpunkt-Verlags bekannt gegeben – voraussichtliches Thema am 22.11. sind die Russland betreffenden Artikel im GS 3-21: Ukraine, Gipfeltreffen Biden-Putin, Rüstungsdiplomatie.