

Was sind Kryptowährungen?

ARBEITSVORSCHLÄGE

1. Interpretieren Sie die Karikatur M1.
2. Bilden Sie vier gleich große Gruppen, die sich jeweils mit einem der folgenden Aspekte beschäftigen:
 - Die Technik hinter Kryptowährungen (M2)
 - Wie funktionieren Krypto-Geschäfte? (M3)
 - Das wirtschaftliche und politische Umfeld von Krypto (M4)
 - Kosten und Nutzen der Blockchain-Technologie (M5)

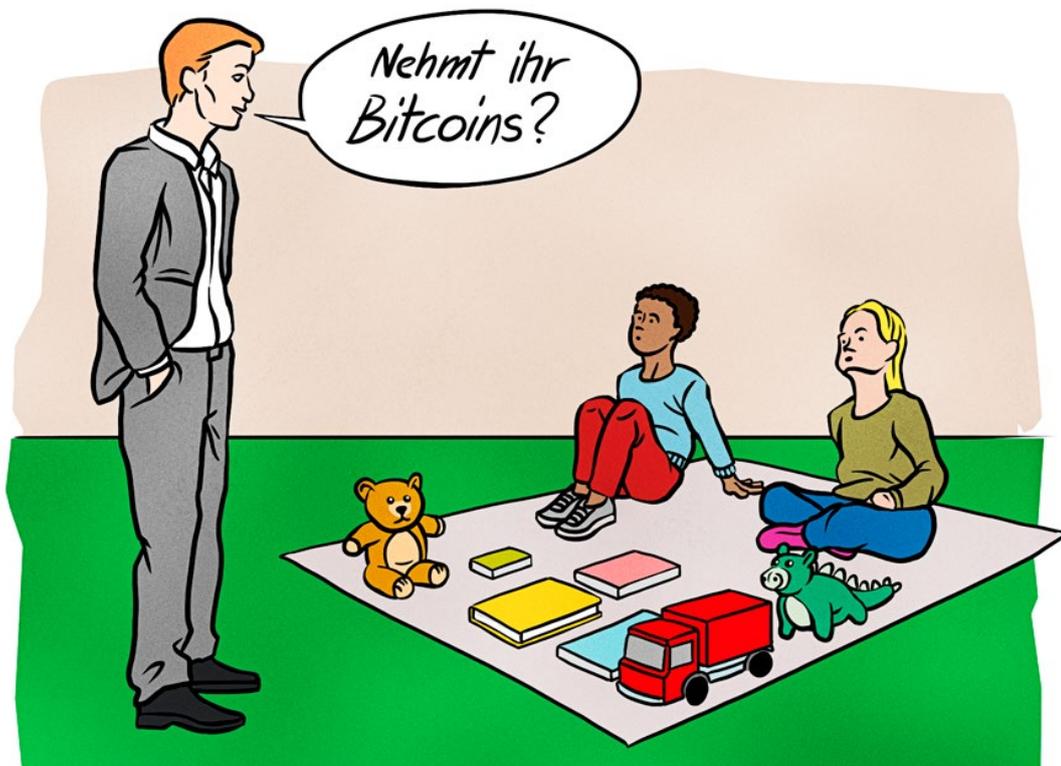
Erarbeiten Sie in den Kleingruppen jeweils ein Plakat und eine mündliche Präsentation dazu, in der Sie die wesentlichen Aspekte des Textes darstellen.

3. Museumsgang: Hängen Sie die Plakate mit möglichst großem Abstand an vier Stellen im Raum aus. Bilden Sie Vierergruppen, in denen aus jeder Plakat-Gruppe eine Person dabei ist (oder zwei, falls es nicht aufgeht). Verteilen Sie die neuen Gruppen auf die Plakate.

Nun präsentieren die jeweiligen Expert*innen aus der Plakatgruppe ihre Arbeitsergebnisse und beantworten Nachfragen. Nach 10 Minuten rotieren die Gruppen im Uhrzeigersinn und die nächsten Expert*innen erläutern ihr Plakat – bis alle Gruppen alle Stationen durchlaufen haben.

4. Erörtern Sie schriftlich: Ist Krypto eine sinnvolle Innovation oder nutzloser Unfug? _____

M1 Karikatur: Bitcoin im Alltag



M2 Die Technik hinter Kryptowährungen

1 Interview mit tante/Jürgen Geuter Teil I

Was ist eine Blockchain?

• Eine Blockchain ist eine spezielle Form von
• Datenbank. Die Besonderheit ist, dass sie nicht
5 wie andere Datenbanken erlaubt, etwas belie-
• big hinzuzufügen, zu verändern oder zu löschen.
• Es ist nur möglich, immer neue Daten hinten
• anzufügen.

• Man muss sich das vorstellen wie eine Perlen-
10 kette und die Perlen sind die sogenannten Daten-
• blöcke. Dadurch, dass ich hinten eine neue Perle
• auffädele, sind die davor miteinander verbunden.
• Ich kann keine in der Mitte rausnehmen, ich
• kann keine mehr verändern, ich habe immer nur
15 die letzte Perle in der Hand.

• Bei Blockchains werden die Datenblöcke mit
• kryptografischen Hashes verknüpft, die ich darauf
• berechne. Was da einmal drin ist, ist drin. Wenn
• ich eine Blockchain habe, dann weiß ich, dass nie-
20 mand diese Daten manipuliert hat, das könnte ich
• sofort sehen.

Was hat die Blockchain mit Kryptowährungen zu tun?

• Die Idee von digitalen Währungen ohne Staa-
25 ten ist schon älter. Blockchains war ein Ansatz,
• wie man sowas umsetzen könnte. Ich könnte
• tante-Coins herausgeben. Dafür brauche ich eine
• Datenbank, wer wieviel Coins hat. Es sollte aber
• nicht eine Bank geben, die alle Konten verwaltet,
30 sondern man sagte, wir brauchen etwas Dezentra-
• les, das nicht kontrollierbar ist. Also brauche ich
• eine dezentrale Datenbank und da darf niemand
• nachträglich etwas ändern, sich Coins hinzufügen
• oder rausnehmen.

35 Theoretisch kann man digitale Währungen
• ohne Blockchains bauen oder Blockchains ohne
• eine digitale Währung benutzen. Allerdings erge-
• ben Public Blockchains (an denen sich theoretisch
• alle beteiligen können) ohne eine Kryptowährung
40 keinen Sinn. Denn um die Dinger zu betreiben,
• muss irgendjemand die Rechner bezahlen, irgend-
• wer muss Strom für die Rechner bezahlen – was
• gebe ich denen dafür? Und wenn ich sie mit etwas
• bezahlen möchte, ich möchte aber, dass alles wei-
45 ter anonym bleibt, muss ich eigentlich auf dieser
• Blockchain eine anonyme Währung haben, in der
• ich ihnen dann diese Tokens gebe. Das heißt ich
• brauche aus ökonomischen und ideologischen
• Grundsätzen bei einer Public Blockchain eine

50 Kryptowährung, um die Leute, die das Netzwerk
• am Laufen halten, dafür zu belohnen, dass sie es
• tun.

Diese Belohnung funktioniert über das sogenannte Mining – richtig? Was muss man sich technisch darunter vorstellen?

55 Mining kennen wir traditionell von Bitcoin und
• das ist eigentlich die einzige größere Kryptowäh-
• rung, die das noch so tut. Wenn jeder einfach so
• Bitcoins erzeugen kann, habe ich sofort Inflatio-
60 on, also brauche ich einen kontrollierten Prozess.
• Gleichzeitig möchte ich Menschen motivieren,
• dieses System am Laufen zu halten. Also hat man
• sich Folgendes überlegt: Wir schreiben ungefähr
• alle 10 Minuten den nächsten Block und beloh-
65 nen die Menschen, die das tun, mit Bitcoins. Die
• suchen sich geplante Überweisungen im System
• zusammen, machen daraus einen Block, berechnen
• einen neuen Hash und werden dafür belohnt.

• Jetzt ist es aber kein zentrales System wo eine*r
70 auf jemanden zeigen und sagen kann »Du kannst
• den nächsten Block bestimmen«, sondern es
• braucht ein anderes Verfahren, wie ich sicherstelle,
• dass nur eine*r diesen Block schreibt. Dafür hat
• man sich dieses Mining überlegt. Das basiert auf
75 dem Konzept Proof-of-Work, das eigentlich aus
• der Spam-Abwehr kommt. Ich weise nach, dass
• ich eine bestimmte Arbeit reingesteckt habe, und
• dafür darf ich die Belohnung einstreichen.

Worin besteht diese Arbeit?

80 Was ich tue, ist Zahlen raten. Wenn der Hash,
• den ich errechne, eine spezielle Eigenschaft hat,
• dann darf ich den nächsten Block schreiben. Ich
• rate Zahlen, die ich hinten an den Block dranhänge,
• dadurch verändert sich der Hash. Wenn ich der
85 Erste bin, der einen gültigen Hash gefunden hat,
• darf ich diesen Block schreiben und bekomme
• dafür die Bitcoins. Dann geht das nächste Rät-
• sel geht los. Die Rätsel hängen von der Menge
• der Teilnehmenden ab, wenn nur zwei Leute da
90 wären, dann wäre das Rätsel sehr leicht. Wenn
• sehr viele Leute mitmachen, dann wird es immer
• schwieriger, so dass es immer ungefähr 10 Minu-
• ten dauert.

■ Jürgen Geuter hat Informatik und Philosophie studiert und arbeitet als Research Director bei den ART+COM Studios an der Erforschung, Implementierung und Erprobung neuer Technologien. Als freier Berater, Autor und Vortragender beschäftigt er sich mit Themen an den Schnittstellen von Technologie, Gesellschaft und Politik. Er ist Gründungsmitglied des transdisziplinären Otherwise Network (ownw.de).

M3 Wie funktionieren Krypto-Geschäfte?

1 Interview mit Beat Weber Teil I

Was ist eigentlich eine Kryptowährung?

Unter Kryptowährungen versteht man Einträge in einer digitalen Datenbank, die nach gemeinsamen Regeln von Freiwilligen verwaltet wird und nur im Internet existiert. Diese Einträge werden von Fans als wertvoll betrachtet und können entweder besessen oder an andere weitergeleitet werden, die sich an diesem Netzwerk beteiligen.

Sind Kryptowährungen Geld?

Ich glaube, dass die Bezeichnung »Währung« für Krypto irreführend ist, weil Währungen beziehungsweise Geld eine ganz spezifische Funktion in einer Wirtschaft erfüllen. Das sind im Wesentlichen drei Dinge: Geld oder Währungen werden gebraucht, um damit Preise von Gütern und Diensten zu messen, die in unserem Wirtschaftssystem auf Märkten entstehen. Die zweite Funktion ist, Güter und Leistungen zu bezahlen. Und die dritte Möglichkeit, die ich mit Geld habe, ist, es zu sparen und damit Wert aufzubewahren.

Von diesen drei Dingen, die normales Geld oder eine Währung auszeichnen, kann man mit Krypto bestenfalls eines machen, nämlich das Aufbewahren. Leute, die Krypto kaufen, bewahren es auf, in der Hoffnung, dass sie es billiger gekauft haben als sie es verkaufen können. Die Spekulation auf eine Wertsteigerung ist das Hauptmotiv, wenn man Nutzer fragt. Kein einziger Preis in Europa ist in Krypto angegeben. Es gibt ein paar Unternehmen, die sagen, du kannst bei mir auch in Krypto zahlen, aber tatsächlich tun wird das kaum ein Konsument.

Was macht Krypto wertvoll?

Ein wirtschaftlicher Wert ist immer das, was andere mir für etwas geben, also der Wert liegt ein bisschen im Auge des Betrachters. Kryptowerte wie zum Beispiel Bitcoin zeichnen sich dadurch aus, dass sie mengenbegrenzt sind. Eine der Grundregeln der Software, die dem zugrunde liegt, ist, dass die Menge begrenzt ist. Damit wird eine Qualität signalisiert, die so ähnlich ist, wie wir das von Sammlerobjekten kennen. Es ist eine Rarität, es ist knapp, es ist begrenzt verfügbar. Das reizt Leute schon seit Ewigkeiten, etwas für wertvoll zu befinden, dass sie etwas haben können, was andere dann nicht haben können, und weckt ihre Bereitschaft, dafür echtes Geld herzugeben.

Wieviel das ist, wird auf Kryptomärkten ausgehandelt, beim Zusammentreffen von Angebot und Nachfrage, also zwischen Leuten, die Krypto kaufen oder verkaufen gegen echtes Geld. Wieviel das ist, schwankt sehr stark, stärker als in vielen anderen Märkten. Das ist ganz anders als bei einer stabilen Währung, wo der Wert von heute auf morgen mehr oder weniger gleichbleibt. Dieses starke Schwanken der Kryptowährungen ist interessant, wenn ich darauf aus bin, auf diese Währungen zu wetten, indem ich versuche, günstig zu kaufen und einen Zeitpunkt abwarte, wo ich die Gelegenheit habe, teurer zu verkaufen.

Wo werden die Kryptowährungen gehandelt?

Es sind in den letzten Jahren viele Kryptofirmen auf den Markt getreten, die anbieten, eine Art Börsengeschäft für Krypto zu organisieren. Die erste bekannte Krypto-Börse hat Mt. Gox geheißen. Die hat ursprünglich mit seltenen Sammelkarten aus Fantasy-Spielen gehandelt und fand im Handel mit Bitcoin eine passende Verlängerung ihres Geschäftsfelds. Das ist, wie ich finde, ein sehr treffender Hinweis auf diese Nachbarschaft, in die sich Krypto auch einreicht. Eine Fantasiewährung im Kontext von Fantasy-Spielen, mit denen handfeste spekulative Geschäfte möglich sind, weil sie sich als Raritäten positionieren.

Demnach ist die Erzählung von Krypto als dezentralem Netzwerk, an dem alle teilhaben können, wenn sie den Rechner anschalten, auch ein Mythos?

Ein machtfreier Raum ist der Krypto-Sektor auf keinen Fall. Es gibt nicht den einen Chef, aber eine Menge sehr große Fische, die in vielen Bereichen einen sehr großen Einfluss haben. Das umfasst viele Aspekte. Das Krypto-Vermögen ist extrem ungleich verteilt. Große Akteure, auch Firmen haben einen großen Einfluss, auf die Vermittlung, auf die Kursbildung und vieles andere. Die Erzeugung – das Mining – ist ebenfalls ein konzentriertes Geschäft. Mit Dezentralität im Sinne von Gleichheit und demokratischer Mitbestimmung hat das nichts zu tun. ■ Beat Weber ist Ökonom mit dem Spezialgebiet Geldtheorie und Mitarbeiter der Oesterreichischen Nationalbank in Wien.

M4 Das wirtschaftliche und politische Umfeld von Krypto

1 Interview mit Beat Weber Teil II

2 Wir haben besprochen, dass der Wert von
3 Kryptos allein darauf beruht, dass Menschen
4 bereit sind, Geld dafür auszugeben, dass sie ei-
5 nen Eintrag in eine Datenbank »besitzen«. Der
6 aktuelle Kurs hängt demnach einfach von An-
7 gebot und Nachfrage an entsprechenden Bör-
8 sen ab, wo solche Einträge gehandelt werden?

9 Ja, und diese Nachfrage ist sehr stark von Stim-
10 mungen abhängig und von Geschichten, die in
11 Sozialen Medien kursieren, viel stärker als bei
12 anderen Anlageobjekten, wo das alles reguliert
13 und ein bisschen eingeschränkt ist. Es werden
14 Gerüchte gestreut, dass es bei diesem oder jenem
15 Kryptowert hinaufginge und man deswegen ein-
16 steigen müsse. Verschiedene Argumente werden
17 da zirkuliert, warum Kryptos toll sind. Dazu zählt
18 unter anderem die Behauptung, es handle sich um
19 Währungen oder technisch bessere Währungen als
20 die, die wir kennen. Da wird oft eine Dynamik in
21 Gang gesetzt, wo Leute über verschiedene Kanäle
22 den Eindruck kriegen, sie müssten da jetzt dabei
23 sein, sonst würden sie was verpassen, zumindest in
24 den letzten Jahren, wo die Kurse ganz stark gestie-
25 gen sind und viele Leute damit auch angeworben
26 wurden, da einzusteigen.

27 **Welchen volkswirtschaftlichen Nutzen ha-
28 ben Kryptowährungen?**

29 Das ist schwer zu erkennen. Vielleicht ist es ein
30 Labor für technische Experimente. Die Block-
31 chain ist eine Technik, um ein gemeinsames
32 Verzeichnis dezentral zu führen. Das hat viele Ex-
33 perimente inspiriert, was man denn außer Krypto-
34 werten noch damit erzeugen könnte und wo man
35 das anwenden könnte. Aber Experimente haben
36 auch Kosten, das müsste man in Balance stellen.
37 Also, die Antwort auf diese Frage ist offen.

38 **Warum konnte sich so etwas ohne unmit-
39 telbaren Nutzen durchsetzen?**

40 Weil die Frage der Durchsetzung nicht daran
41 hängt, ob es einen volkswirtschaftlichen Nutzen
42 hat. Es hat einen privaten Nutzen und das ist ja
43 in unserem Wirtschaftssystem ausreichend. Nie-
44 mand muss sich damit rechtfertigen, was er für
45 die Gemeinschaft bringt, um irgendwas anbieten
46 zu können. Es gab genug Leute, die es interes-
47 siert hat, die dort Unternehmen gegründet haben,
48 die mit Krypto Handel treiben und Kundschaft,
49 die das kauft und verkauft. Nichts davon hat mit
50 volkswirtschaftlichem Nutzen zu tun.

51 »Durchsetzen« könnte auch heißen, dass Krypto
52 nicht verboten wurde und es schrittweise zu staat-
53 licher Anerkennung kam, indem das jetzt reguliert
54 wird. Da würde ich sagen, lange waren sich Be-
55 hörden unklar, wie sie damit umgehen sollen, weil
56 viele dieser Projekte darauf angelegt waren, sich
57 staatlichen Regulierungen zu entziehen. Bei sämt-
58 lichen anderen Finanzinstrumenten gibt es einen
59 Verantwortlichen (Emittent nennt man das), der
60 das herausgibt und in der Verantwortung steht,
61 dass das bestimmte Eigenschaften hat. Bei einer
62 Aktie steht ein Unternehmen dahinter, bei einer
63 Währung ist die Zentralbank verantwortlich. So
64 eine verantwortliche Instanz fehlt bei Krypto. Es
65 gibt keinen Bitcoin-Chef, dem ich Auflagen ma-
66 chen oder den ich ins Gefängnis stecken kann.

67 **Wie sehen die Ansätze zur Regulierung von
68 Krypto aus?**

69 In der EU wurde 2023 ein Regulierungsrahmen
70 verabschiedet und der reguliert den Kryptosektor,
71 indem er bei den Vermittlungsinstanzen ansetzt,
72 zum Beispiel Börsen, die den An- und Verkauf
73 von Krypto organisieren. Diese Privatfirmen
74 werden jetzt Regeln unterworfen, so dass Betrug
75 und Irreführungen im Kryptomarkt weniger
76 wahrscheinlich werden, und sie werden besteuert,
77 so dass ein bisschen von den privaten Gewinnen,
78 die hier erzeugt werden, für die Allgemeinheit
79 abgezweigt wird. Was sich dadurch nicht ändern
80 wird, sind die Wertschwankungen.

81 **Ist es nicht so ein Anzeichen für eine be-
82 stimmte Situation unseres Wirtschaftssystems
83 generell, wenn sich so eine rein spekulative
84 Geschichte wie Krypto so etablieren kann?**

85 Ja, das ist vielleicht ein gutes Beispiel für das,
86 was man »Casino-Kapitalismus« genannt hat. Das
87 Wetten auf Kursveränderung, das früher eine
88 Domäne von hoch professionellen, großen Finanz-
89 akteuren war, wird versucht auch in Privathaushalte
90 zu tragen. Andererseits steht das aber auch in ei-
91 ner ganz alten Tradition von populärer Kleinspe-
92 kulation. Das ist diese Klasse der Raritäten und
93 Sammlerobjekte, also Flohmärkte mit seltenen
94 Sachen. Wo sich Leute nicht nur aus Liebhaberei,
95 sondern auch aus wirtschaftlichen Gründen
96 betätigen. Neu ist, dass es so etwas auch in rein
97 digitaler Form gibt. ■ Beat Weber ist Ökonom mit dem Spezialgebiet

Geldtheorie und Mitarbeiter der Oesterreichischen Nationalbank in Wien.

**M5 Kosten und Nutzen
der Blockchain-Technologie**

1 Interview mit tante/Jürgen Geuter Teil II

Bei der Blockchain als dezentraler Datenbank gibt es das Problem, wer den nächsten Eintrag in die Datenbank (Block) schreiben darf. Bei Bitcoin funktioniert das nach dem Prinzip Proof-of-Work. Ich löse ein kompliziertes Rätsel, darf dann den nächsten Eintrag schreiben und werde dafür mit Bitcoins belohnt. Daran gibt es aber auch Kritik.

Das Verfahren ist sehr energieintensiv, denn ich muss unglaublich viele Berechnungen machen, und alle machen gleichzeitig dieselben, um als Erste das Rätsel zu lösen. Dadurch entsteht bei Bitcoin dieser unglaubliche Energieverbrauch. Die brauchen so viel Strom wie Argentinien.

Dahinter steht die Kalkulation: Wenn ich sehr viel Energie einsetze, dann ist die Wahrscheinlichkeit, dass ich die Blocks schreiben darf, sehr hoch, dadurch bekomme ich ein handelbares Asset (Bitcoins) mit dem ich echtes Geld bekommen kann. Das treibt alle dazu, ein bisschen weniger Geld auszugeben als die Bitcoins, die sie bekommen könnten. Es ist nicht einer, der das tut, sondern es sind theoretisch beliebig viele, die das tun und versuchen durch Proof-of-Work die Coins einzustecken.

Neben Proof-of-Work gibt es aber auch noch das Proof-of-Stake-Verfahren was sind die Unterschiede?

Bei Proof-of-Work kann formal jede*r einfach so teilnehmen, ich stelle mir Rechner hin und die rechnen. Proof-of-Stake bedeutet, du beweist deinen Anteil. Nehmen wir Ethereum mit seiner Kryptowährung Ether als großes Beispiel: Ich muss Ether im Wert von ungefähr 32.000 Dollar hinterlegen, sobald ich das getan habe, habe ich Eintritt bezahlt und kann jetzt an einer Lotterie mitmachen, ob ich den nächsten Block schreiben darf. Es gibt auch noch weitere Verfahren. Bei Proof-of-Space weise ich nach, dass ich riesige Datenmengen auf Festplatten speichere, das ist ein großes Elektroschrott-Thema, weil Festplatten das nicht lange überleben. Bei Proof-of-Authority, gibt es quasi Admin-Accounts die Blocks schreiben dürfen, das ist offensichtlich nicht mehr dezentral.

Welche Folgen hat eine Umstellung von Proof-of-Work auf Proof-of-Stake?

Die erste Folge ist, dass der Energieverbrauch der Chain um rund 99% einbricht. Das wäre natürlich bei Bitcoin ein Riesending. Wie gesagt, so viel Strom wie Argentinien, wenn man das nicht mehr bräuchte, wäre schon geil. Die Kritik der Bitcoin-Akteure ist, dass Proof-of-Stake deutlich zentralisierter ist. Das ist nicht ganz falsch. Bei

Proof-of-Work kann jede*r einfach so mitmachen, abgesehen von dem Schweinegeld für Rechner und Strom. Auch wenn ich nie einen Block schreibe, kann ich immer mitrechnen, ob die anderen es richtig gemacht haben.

Beim Proof-of-Stake musst du dich offiziell einkaufen für viel Geld. Theoretisch wäre es auch möglich, dich von Proof-of-Stake-Mining auszuschießen, weil es halt eine Gruppe aus Accounts ist, die das tun dürfen. Das heißt, die Leute, die sich da gegenseitig kontrollieren, sind jetzt wirklich eine Gruppe und es wird sehr viel leichter, Missbrauch zu organisieren. Ethereum ist diesen Weg gegangen, weil sie den Energieverbrauch loswerden wollten. Es ist um Größenordnungen effizienter, aber anfälliger für Mißbrauch.

Welchen gesellschaftlichen Nutzen hat die Blockchain-Technologie?

Datenbanken sind sehr nützlich und es gibt sehr unterschiedliche Datenbanken für unterschiedliche Probleme. Das Problem, das Blockchains lösen wollen, ist eine gemeinsame Datenbank-Wahrheit zwischen theoretisch beliebig vielen Teilnehmenden, die sich nicht vertrauen können und wollen und die auch keinem Dritten vertrauen können, der das für sie hosten (betreiben) könnte. Deshalb ist es so ineffizient, das ist der Preis, den ich dafür zahle.

Die Frage ist, gibt es in der Realität dieses Problem? Wenn irgendwelche Communities Dinge tun wollen, könnten die sich in der Regel auch auf einen Treuhänder oder eine Genossenschaft einigen, die es für sie tut, oder die Politik schafft Strukturen, die das tun können.

Dazu kommt noch ein großes Problem: Ich habe kein Undo, weil alles dezentral sein soll. Dinge, die drinstehen, können nicht mehr verändert werden. Es gibt keinen Richter, den ich anrufen könnte, um eine Änderung abzusegnet. Das wollen wir aber in der Realität häufig. Wenn da etwas Falsches drinsteht – wenn ich mein Geschlecht wechsele und da steht noch der falsche Name drin –, dann will ich, dass das korrigiert werden kann auf irgendeinem Weg, und das geht mit der Chain nicht. Das heißt, diese sozialen und politischen Kosten sind extrem hoch und ich glaube nicht, dass es in der Realität sehr häufig dieses Problem gibt.

Jürgen Geuter hat Informatik und Philosophie studiert und arbeitet als Research Director bei den ART+COM Studios an der Erforschung, Implementierung und Erprobung neuer Technologien. Als freier Berater, Autor und Vortragender beschäftigt er sich mit Themen an den Schnittstellen von Technologie, Gesellschaft und Politik. Er ist Gründungsmitglied des transdisziplinären Otherwise Network (ownw.de).

