



Donnerstag, 30. Oktober 2025, 17:00 Uhr
~14 Minuten Lesezeit

Das digitale Gefängnis

Der Tod der Freiheit wird weniger mit Handschellen und Polizeiknüppeln als mit Bits und Bytes herbeigeführt werden. Teil 1: Kampf gegen das Bargeld.

von Uwe Froschauer
Foto: Natali _ Mis/Shutterstock.com

Stell dir vor, alles ist auf „digital“ umgestellt – und dann fällt der Strom aus! Dies ist aber nur einer von mehreren Alpträumen, die sich mit der Vorstellung verbinden, wir könnten schon bald in einer

bargeldfreien Welt leben müssen. Neben der Möglichkeit lückenloser Überwachung unseres Zahlungsverkehrs ermöglicht es der Zwang zum Bezahlen mit Karte, Smartphone und Smartwatch auch, den Kauf bestimmter unerwünschter Produkte auf technischem Weg zu verhindern und so den Verbraucher stets am staatlichen Gängelband zu halten. Selbst, wenn die Verhältnisse anfangs noch erträglich erscheinen mögen – es bleibt die Unruhe, der Staat könne mit den einmal etablierten Werkzeugen und mithilfe einer gesellschaftlichen Mehrheit von Innovations-Opportunisten die Falle jederzeit zuschnappen lassen. Nach einem Regierungswechsel oder auch „einfach so“, unter dem Vorwand der Verbrechensbekämpfung. Dabei funktioniert ein Phänomen wie Steuervermeidung schon jetzt auch ganz ohne Bargeld sehr gut. Der Autor setzt sich in seinem zweiteiligen Artikel mit der realistischen Dystopie einer komplett überwachten und manipulierten Menschheit auseinander.

Robert F. Kennedy Jr., US-amerikanischer Minister für Gesundheit und Soziale Dienste, hat Ende September 2025 einen groß angelegten verbalen Angriff auf das digitale Gefängnis gestartet, das die globalen Eliten derzeit im Begriff sind zu errichten. Seine Warnung sollte jeden Menschen zutiefst erschüttern:

„Digitale Währung wird es der Regierung ermöglichen, Sie aus der Ferne zu bestrafen ... Ihre Lebensmittelversorgung zu unterbrechen ... jedes Ihrer Rechte in ein Privileg zu verwandeln, das von Gehorsam

abhängt. Sie wird Sie zu Sklaven machen.“

Blogger wie ich und andere freiheitsliebende Menschen haben schon oft vor dem digitalen Gefängnis gewarnt. Diese Warnung kommt jedoch von jemandem, der mitten im System steht – von einem Menschen, der sich gegen diese totalitären Ambitionen der Macht- und Besitzeliten wehrt, und uns dazu aufruft, das Gleiche zu tun. Wenn jetzt dem Ziel dieser menschenverachtenden Eliten nach der „totalen Kontrolle“ kein Riegel vorgeschoben wird, werden wir uns alle im digitalen Gefängnis wiedersehen. Und es ist fünf vor zwölf. Viel Zeit bleibt nicht mehr.

Der Wirtschaftsjournalist Norbert Häring warnt:

„Wenn es kein Bargeld mehr gibt, wird unser Bankkonto zu einem detaillierten Logbuch unseres Lebens.“

Dieses Zitat stammt aus dem 2025 erschienenen Buch „Krieg gegen das Bargeld“ von Hakon von Holst. Die mit seinem absolut lesenswerten Buch beschriebene Intention hat Hakon von Holst wie folgt **formuliert** (<https://www.amazon.de/Krieg-gegen-das-Bargeld-Geldscheine/dp/3910568211>):

„Man sieht es an so ziemlich jeder Ladenkasse: Immer öfter zücken die Kunden Karte oder Handy, um ihren Einkauf zu bezahlen. Ist das der Zeitgeist, Fortschritt, der Weg in die Zukunft? Die vermeintliche Annehmlichkeit hat jedoch einen Haken: Wer mit Karte bezahlt, bezahlt mit seinen Daten. Nicht nur Zeitpunkt und Ort des Einkaufs sind nachvollziehbar, auch der Warenkorb bekommt ein Gesicht. Die elektronischen Abbuchungen vom Bankkonto werden so zu einem "detaillierten Logbuch unseres Lebens", wie es der Wirtschaftsjournalist Norbert Häring treffend formulierte. Das Zahlen mit Bargeld schützt nicht nur unsere Privatsphäre. Wir behalten auch viel eher den Überblick über unsere Finanzen. Und selbst bei einem

Blackout können wir uns das Nötigste beschaffen. Wer hat ein Interesse an der schleichenden Abschaffung des Bargelds? Geht es tatsächlich um die Bekämpfung von Geldwäsche und Terrorismus, oder steckt viel mehr dahinter? Wer sind die Akteure in Politik und Finanzwirtschaft, und welche Methoden benutzen sie? Was würde die weltweit geplante Einführung staatlicher Digitalwährungen bedeuten? Und: Was können wir gegen die Einschränkung unserer Freiheit tun? Auch wenn es uns privatwirtschaftliche, staatliche und kommunale Einrichtungen immer schwerer machen: Wir haben es vielleicht selbst in der Hand, indem wir weiterhin mit Bargeld bezahlen!“

Chaos durch technische Pannen

Was ist, wenn in der ach so bequemen, von menschenverachtenden Rattenfängern angepriesenen, modernen elektronischen Welt der Strom ausfällt, oder andere Pannen oder Katastrophen verhindern, dass Sie sich lebensnotwendige Güter kaufen können? Beispiele für das dadurch entstehende Chaos gibt es zuhauf.

Die New York Times schrieb am 28. April 2025 von langen Schlangen vor noch funktionierenden Geldautomaten aufgrund eines Stromausfalls in Portugal und Spanien.

Der massive Stromausfall auf der Iberischen Halbinsel erfasste weite Teile des Landes. Unter anderem waren elektronische Zahlungssysteme betroffen: POS-Terminals fielen aus, viele Geldautomaten funktionierten nicht, Mobilfunk und Internet waren gestört, wodurch Kartenzahlungen oder andere digitale Zahlungsmethoden kaum oder gar nicht möglich waren.

Etwa zur gleichen Zeit im April 2025 ereignete sich ein ähnliches Desaster in der Ukraine.

Ein Stromausfall, der im Rechenzentrum von De Novo verursacht wurde, störte Online-Dienste wie die ukrainische Diia-Regierungs-App, lokale Banken, den Postriesen Nova Post und kontaktlose Zahlungssysteme wie Apple Pay und Google Pay. Kiewer Bürger sagten dem Format „Recorded Future News“ des ukrainischen Magazins „The Record“, dass sie während der Störung nicht in der Lage waren, mobile Zahlungen zu nutzen, um die U-Bahn der Stadt zu betreten. Einige Restaurants hatten ebenfalls Probleme mit elektronischen Zahlungssystemen. De Novo benötigte fast sechs Stunden, um die Dienstleistungen für seine Kunden wiederherzustellen.

Im indischen Hyderabad führten am 20. August 2025 ein Kabelschnitt bzw. Aktionen des Stromversorgers dazu, dass große Teile der Internetverbindung ausfielen. Dadurch konnten viele Zahlungen über das meistgenutzte digitale Zahlungssystem UPI in Indien nicht durchgeführt werden. Viele Geschäfte forderten – für viele Kunden ungewohnt – Bargeld. In den sozialen Medien posteten Nutzer Screenshots von fehlgeschlagenen Transaktionen und drückten ihre Frustration über das finanzielle Chaos aus. Ein Großteil der Beschwerden bezog sich auf fehlgeschlagene UPI-Zahlungen, die es den Nutzern erschwerten, Einkäufe, darunter Lebensmittel und andere wichtige Güter, abzuschließen. Ein verärrgerter Kunde, der Schwierigkeiten bei der UPI-Zahlung hatte, sagte dem Magazin *Telangana Today*:

„Ich musste meine Frau anrufen, um die Zahlung von ihrer UPI-ID zu tätigen, da meine nicht durchging. Selbst nachdem sie die Zahlung erfolgreich abgeschlossen hatte, erhielten wir keine Bestätigung. Die Landesregierung und die Energieversorger hätten diese Aktion gut planen müssen.“

Auch in Deutschland gab es vermehrt Fälle, in denen nicht primär ein Stromausfall die Ursache für den Ausfall der digitalen Zahlungsfähigkeit war, sondern Störungen in der IT-Infrastruktur.

Viele Störungen entstehen durch Software- oder Netzwerkfehler bei den Dienstleistern. So kam es am 4. April 2024 zu einer Technikpanne bei der Sparkasse. Tausende Kunden meldeten Ausfälle – betroffen waren unter anderem Supermärkte. Eine Störung der EC-Kartenzahlung in in Filialen großer Einzelhandelsketten wie Lidl und Rewe führten von ca. 7:20 bis 9:50 Uhr zu einem kleinen Chaos. Kartenzahlungen waren nicht möglich. Die Kunden mussten – falls zur Hand – auf Bargeld zurückgreifen.

Am 12. September 2024 ereignete sich eine technische Störung beim IT-Dienstleister Telecash sowie bei an diesen angeschlossenen Anbietern. Von 6 Uhr morgens bis kurz vor 16 Uhr gab es Schwierigkeiten bei der Bezahlung mit Karte. Die Probleme betrafen Debit-, Kredit- und Girokarten.

Wie gut fühlt es sich in solchen Situationen an, ausreichend Bargeld statt Plastik- oder Smartphonegeld in der Tasche zu haben, nicht wahr?

Cyberattacken, die zu einem Ausfall digitaler Zahlungsmöglichkeiten führen können

Viele Störungen werden zunächst als „Cyberangriff“ vermutet, was sich nachträglich meist als Störungen in der IT-Infrastruktur herausstellt. Dennoch sind derartige Fälle bereits vorgekommen. Die Aufsichtsbehörden „Bundesanstalt für Finanzdienstleistungsaufsicht“ (BaFin) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichten seit 2023/2024 von einer steigenden Zahl von Cybervorfällen in der Finanzbranche – darunter auch Angriffe auf Tochterfirmen oder Dienstleister, bei denen Daten abgeflossen oder Prozesse beeinträchtigt wurden. Solche Vorfälle können auch

Zahlungsprozesse stören, weil beispielsweise Back-Office-Systeme abgeschaltet werden müssen, selbst wenn Zahlungsterminals nicht unmittelbar betroffen sind. Auf der Seite der BaFin ist zu **lesen** (https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2025/RIF_4_Cyber_Vorfaellen/RIF_4_Cyber_Vorfaellen_node.html?ljsessionid=E54363F3FC057A1ABAFEBF2AB2287AFA.internet001):

„Risiken aus Cyber-Vorfällen mit gravierenden Auswirkungen

Die Bedrohung durch Cyber-Vorfälle ist weltweit sehr hoch und nimmt weiter zu. Hintergründe sind die fortschreitende Digitalisierung, welche die Angriffsfläche vergrößert, sowie geopolitische Spannungen, die zunehmend in den Cyber-Raum und auf kritische Infrastrukturen ausstrahlen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzte die Bedrohung im Cyber-Raum im Frühjahr 2024 „so hoch wie nie zuvor“ ein.

Fast ein Fünftel aller globalen Cyber-Vorfälle der vergangenen zwanzig Jahre betraf Unternehmen des Finanzsektors. Der Schaden beläuft sich laut Internationalem Währungsfonds (IWF) seit 2004 auf fast 12 Milliarden US-Dollar. Dabei stieg die Zahl der Vorfälle, insbesondere von Cyber-Attacken, in den letzten Jahren stetig an.

Ein Cyber-Vorfall ist ein versehentlich oder böswillig herbeigeführter Vorfall, der sich negativ auf die Vertraulichkeit von Daten und die Verfügbarkeit von IT-Systemen oder Netzwerken auswirken kann oder Sicherheitsrichtlinien, Sicherheitsprozesse oder Nutzungsbedingungen verletzt. Solche Vorfälle können bei den beaufsichtigten Unternehmen selbst, aber auch bei

Auslagerungsunternehmen

(https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2025/RIF_6_Auslagerung_IT_Dienstleistungen/RIF_6_Auslagerung_IT_Dienstleistungen_node.html) entstehen.

Cyber-Vorfälle bei Unternehmen des Finanzmarkts oder bei

Infrastrukturen können die Funktionsfähigkeit des Finanzsystems erheblich beeinträchtigen und im Extremfall zu systemischen Krisen führen. Dies kann insbesondere dann der Fall sein, wenn die enge Vernetzung zwischen Unternehmen des Finanzsektors und Dienstleistern dazu führt, dass viele Unternehmen gleichzeitig von einem Vorfall betroffen sind.

Die Nichtverfügbarkeit von kritischen Systemen und Funktionen, die Verletzung vertraulicher Daten oder hohe wirtschaftliche Verluste können das Vertrauen und die Reputation bei Anlegerinnen und Anlegern sowie Kundinnen und Kunden schädigen. So können Cyber-Vorfälle finanzielle Krisen bei den betroffenen Unternehmen auslösen und das Vertrauen in die Finanzstabilität insgesamt untergraben. Das kann zu Liquiditätsabflüssen führen, beispielsweise in Form von Bank Runs.“

Der niederländische Zahlungsdienstleister Adyen wurde im April 2025 von mehrwelligen DDoS-Attacken (Distributed-Denial-of-Service-Angriff) getroffen. Das führte zu einer mehrstündigen Beeinträchtigung von Zahlungsdiensten in Europa – Online-Checkouts froren ein, Kartenzahlungen bei betroffenen Händlern schlugen fehl oder wurden verzögert. Davon waren auch Händler in Deutschland betroffen, da Adyen viele europäische Händler bedient. Auf der Seite von Adyen war zu lesen

(https://www.adyen.com/knowledge-hub/mitigating-a-ddos-april-2025?utm_source=chatgpt.com):

„Am 21. April 2025 erlebte Adyen einen Distributed-Denial-of-Service-Angriff (DDoS), der sich auf die Verfügbarkeit mehrerer unserer (Zahlungs-)Dienstleistungen in der europäischen Region auswirkte. Dies führte zur Verschlechterung der Leistung unserer Plattform, die sich auf einige unserer Kunden auswirkte.“

(...)

„Der DDoS-Angriff richtete sich speziell an Dienstleistungen in unseren europäischen Rechenzentren, die unsere Transaktionsverarbeitungsdienste und kundenorientierten Anwendungen unterstützen. Infolgedessen verursachte er zeitweilige Ausfälle und Verschlechterung der Leistung in der gesamten EU-Region, wobei die Hauptauswirkungen für die Verarbeitung der E-Commerce- und In-Person-Zahlungstransaktion zwischen 18:51 Uhr MESZ und 19:35 Uhr MESZ lagen. Während dieses Zeitfensters wurden auch unsere Customer Area, Hosted Onboarding und Transfer-API-Dienste abgebaut. Aufgrund unserer bewussten Abschwächung blieben Checkout-Dienste wie Session-Integrationen, Secured Fields und Pay by Link während des gesamten Vorfalls betroffen. Diese Probleme führten zu gescheiterten oder verzögerten Transaktionen für einige Kunden während des betroffenen Zeitrahmens.“

„Verbündete in der Politik“

So überschrieb Hakon von Holst ein Kapitel seines Buches „Krieg gegen das Bargeld“. Die sich stellende Frage lautet: Wer hat ein Interesse an der schrittweisen Abschaffung des Bargelds? Nachfolgend der einleitende Text dieses Kapitels:

„Wir begrenzen den Bargeldfluss, da zumindest große Zahlungen rechtlich gesehen nicht in bar abgewickelt werden dürfen. Was den Rest betrifft: Sorgen wir dafür, dass kleine Zahlungen mit der Kreditkarte attraktiv sind im Vergleich zu Barzahlungen. Zum Beispiel, indem es etwas kostet, Bargeld abzuheben oder mit Bargeld zu bezahlen.“

Romano Prodi (1999–2004 EU-Kommissionspräsident, 2006–2008 Ministerpräsident von Italien)

In Europa existiert ein ‚Anti-Bargeld-Kartell‘ schrieb Yves Mersch 2016 in einem Gastbeitrag für den Spiegel. Der Notenbanker aus dem Direktorium der Europäischen Zentralbank (EZB) unterschied drei Lager: Die ‚Alchemisten‘ wollen das Geld mit einem Verfallsdatum ausstatten, damit die Leute konsumieren und die Wirtschaft in Schwung bleibt. Am einfachsten lässt sich das umsetzen, wenn man Bankkonten mit Strafzinsen belastet und der Bürger nicht ins Bargeld flüchten kann. Die zweite Fraktion ist die „Finanz-Tech-Allianz“. Viele Banken sehen im Bargeld eine kostspielige Bürde. Ihren Ballast würden sie gerne abwerfen und stattdessen an Kartenzahlungen verdienen. Als Letztes im Bunde erwähnt Mersch das ‚Recht-und-Ordnung-Lager‘. Diese Gruppe bringt Bargeld vor allem mit Terrorismus, Steuerbetrug und anderen zwielichtigen Aktivitäten in Verbindung. Ihre Vertreter finden wir zum Teil in der hohen Politik.

Schauen wir uns einmal die Zusammenarbeit zwischen EU-Kommission und Finanzwirtschaft an:

Charlie McCreevy amtierte von 1997 bis 2004 als Finanzminister von Irland. Im Anschluss wurde er EU-Kommissar für Binnenmarkt und Dienstleistungen. Auf einem Kongress der EZB in Frankfurt im November 2006 schmeichelte er dem Banken-Publikum: Man könne Unternehmen oder Verbraucher ‚dazu ermutigen, verstärkt effizientere elektronische Zahlungsmethoden zu nutzen‘. Das könne ‚die Kosten für Bargeld senken – eine Belastung, die oft vom Bankensystem getragen‘ werde. Diesen Punkt führte der EU-Kommissar bereits am 20. September 2005 bei einer Rede in Paris an. Dort sagte er außerdem, dass digitale Zahlungen besser nachvollziehbar, also überwachungsfähig seien. Das nütze der „Bekämpfung von Geldwäsche und Terrorismusfinanzierung“. Am Tag zuvor hatten die Finanzminister der EU-Länder beschlossen: Bei Zahlungen ab 15.000 Euro mit Banknoten und Münzen müssen Unternehmen künftig die Identität ihrer Kunden feststellen.“

So viel zu dem Kapitel „Verbündete in der Politik“ aus dem Buch von

Befürworter behaupten, mit einer digitalen Zentralbankwährung wird es schwieriger, Geld zu verstecken oder Schwarzarbeit zu betreiben. Sie begründen das damit, dass digitale Transaktionen nachverfolgbar sind, und anonyme Bargeldgeschäfte nicht mehr möglich wären. Jede Zahlung könnte automatisch überprüft oder zum Beispiel an die Finanzbehörden gemeldet werden.

Das ist jedoch nicht so einfach, wie meist dargestellt und hängt von der Architektur der digitalen Zentralbankwährungen (CBDC = Central Bank Digital Currency) ab, die sich an unterschiedlichen Datenschutzmodellen orientieren kann. Bei voll-anonymem digitalem Geld werden die Transaktionen nicht gespeichert oder nur lokal in der Wallet. Eine Kontrolle wäre dann – wie beim Bargeld – nicht möglich. Bei pseudonymisiertem digitalem Geld werden die Daten verschlüsselt, und nur bei Verdacht einsehbar. Bei voll-transparentem digitalem Geld werden alle Transaktionen zentral gespeichert und identifizierbar. Das würde eine totale Kontrolle über die finanziellen Tätigkeiten einer Person und einen gravierenden Eingriff in die Privatsphäre eines Menschen bedeuten. Datenschutzrechtlich wäre diese Form meines Erachtens nicht machbar. Aber Gesetze lassen sich aushebeln, wie die Coronazeit gezeigt hat. Durch eine Veränderung des Infektionsschutzgesetzes wurde das Grundgesetz ausgehebelt und mit Füßen getreten.

Wenn beispielsweise der digitale Euro nicht völlig transparent werden soll, um die Privatsphäre zu schützen – wie die Europäische Zentralbank (EZB) behauptet –, würde er nicht automatisch Steuerbetrug verhindern. Das oftmals angeführte Argument, dass Steuerbetrug durch digitale Zahlungen erschwert würde, lässt sich damit nicht halten. Die EU-Kommission selbst schrieb 2018, dass „Steuerbetrug in signifikantem Umfang über bargeldlose Transaktionen“ erfolge, „wobei komplexe Rechtsstrukturen und oft

multinationale Vorgänge genutzt“ würden (EU-Kommission, 12. Juni 2018, COM (2018) 483 final).

Ein großer Teil von Steuervermeidung oder -hinterziehung findet bereits jetzt nicht in bar, sondern über Offshore-Konten, Briefkastenfirmen, kreative Buchhaltung oder digitale Kryptowährungen außerhalb staatlicher Kontrolle statt.

Eine CBDC würde nur die kleinen, alltäglichen Formen von Steuerbetrug wie zum Beispiel Schwarzarbeit oder Barverkäufe ohne Rechnung erschweren, nicht aber die strukturelle oder internationale Steuerflucht.

Die Kleinen würden wieder einmal gehängt, und die Großen laufen gelassen — ganz im Sinne der Macht- und Besitzeliten. CBDCs erschweren den Steuerbetrug für den Normalbürger, große Unternehmen dagegen können ihre Gewinne weiterhin legal verschieben, und reiche Menschen komplexe Steueroptimierungsstrategien nutzen. Legale Steuerhinterziehung. Eine CBDC trifft primär den Otto-Normalverbraucher und kleine Unternehmen, nicht aber die globale Steuervermeidung der Großunternehmen.

Der gläserne und steuerbare Bürger

Klar, digitale Zahlungen sind besser nachvollziehbar und damit überwachungsfähig. Im Fokus steht jedoch nicht, dass digitale Zahlungen der „Bekämpfung von Geldwäsche und Terrorismusfinanzierung“ nützen, wie Charlie McCreevy in den Vordergrund stellte — das ist nur ein Vorwand der Eliten und ihrer politischen und medialen Handlanger —, sondern die Überwachung der Bürger, wie auch Robert F. Kennedy Jr. richtig erkannte. Digitales Zentralbankgeld möchte das Bargeld — und damit die

Möglichkeit anonymer Zahlungen – verdrängen. Jede Zahlung wäre digital dokumentiert, wodurch die Bürger keine Privatsphäre bei finanziellen Transaktionen mehr hätten.

Digitale Zentralbankwährungen können so gestaltet sein, dass jede Transaktion transparent und nachverfolgbar ist. Der Staat, die Zentralbanken und Geschäftsbanken, IT-Konzerne, Zahlungsabwickler wie Visa, Mastercard oder SWIFT, Supranationale oder internationale Institutionen wie der Internationale Währungsfonds (IWF), die Bank für Internationalen Zahlungsausgleich (BIZ), die Europäische Union und so weiter, könnten genau sehen, wer wann, wo und wofür Geld ausgibt – und so ein detailliertes Verhaltensprofil der Bürger erstellen. Auch Regulierungs- und Sicherheitsbehörden wie Finanzaufsichten, Steuerbehörden, Geheimdienste oder Strafverfolgungsstellen könnten über gesetzliche Regelungen Zugriff auf Transaktionsdaten verlangen, zum Beispiel mit dem Vorwand, Geldwäsche oder Terrorismusfinanzierung bekämpfen zu wollen. All diese Institutionen bekämen erheblich mehr Zugriff auf sensible Finanzdaten, als es heute bei Bargeld oder dezentralen Kryptowährungen der Fall ist. Wenn jemand beispielsweise regelmäßig an alternative Plattformen spendet oder Produkte kauft, die als politisch sensibel gelten, könnte dies registriert und gegen ihn verwendet werden.

Digitale Zentralbankwährungen (CBDCs) könnten „programmiertes Geld“ entwickeln, das mit Bedingungen verknüpft ist, bis wann es ausgegeben sein muss und wofür es ausgegeben werden darf. Der Staat könnte etwa festlegen, dass bestimmte Käufe nicht erlaubt oder nur unter bestimmten Umständen möglich sind, wie zum Beispiel der Kauf von Alkohol, Zigaretten oder Benzin.

So könnte einer Person verboten werden, ihr digitales Geld für Benzin oder Flugtickets zu verwenden, weil ihr CO₂-Limit erreicht

ist.

Zentralbanken hätten durch eine CBDC direkten Zugriff auf alle digitalen Konten. Zentralbanken oder der Staat könnten Konten einfrieren, Guthaben beschränken oder negative Zinsen erzwingen, damit man sein Geld schneller ausgibt. Der Staat könnte zum Beispiel meine Blogtätigkeit als „unerwünschtes Verhalten“ ansehen und mir den Zugriff auf digitale Gelder sperren. In China läuft diese unsägliche Massensteuerung und -überwachung bereits im Rahmen des „Social Credit System“.

Wenn du nicht parierst, drehen sie dir den Geldhahn zu.

Auch einige deutsche Politiker schielen bereits auf das chinesische Modell.

CBDCs – verknüpft mit der ebenfalls angestrebten digitalen Identität – würden ein integriertes Kontrollsystem entstehen lassen, das Finanzdaten, Identität, Gesundheitsstatus, Reisedaten usw. der Bürger zusammenführt. In Verbindung mit einem „sozialen Kreditsystem“ könnten die Menschen in die von den Macht- und Besitzeliten gewünschte Richtung dirigiert werden. Wir wären diesen Monstern praktisch hilflos ausgeliefert. Regierungen könnten Zahlungen verweigern, wenn zum Beispiel bestimmte Bedingungen wie Impfstatus oder Steuerstatus nicht erfüllt sind.

Fazit

Sollte das Geldsystem komplett digital werden, ist es anfällig für technische Störungen, Hackerangriffe oder Missbrauch. Ein zentraler Ausfall oder gezielte Manipulation könnten ganze Volkswirtschaften lahmlegen. Die Menschen wären machtlos und der Willkür ihrer Peiniger ausgeliefert.

Durch die digitale Kontrolle des Geldflusses verliert der Bürger ein großes Stück seiner wirtschaftlichen Selbstbestimmung. Wir würden durch digitales Geld stärker an politische Entscheidungen oder staatliche Regeln gebunden werden, und so im Sinne der eliteninstruierten Politiker gesteuert werden.

Gehorsame würden belohnt, und Ungehorsame bestraft werden — moderne Sklaverei! Wollen Sie das?

Im Grunde ist das jetzt schon so, wie die Corona-Zeit gezeigt hat.



Uwe Froschauer hat an der Ludwig-Maximilians-Universität München Betriebswirtschaft studiert und abgeschlossen. Sein besonderes Interesse galt der Wirtschaftspsychologie. Er arbeitete als Unternehmensberater, gibt Seminare bei Berufsbildungsträgern, ist Autor mehrerer Bücher und betreibt den Blog **wassersaenge.com** (<https://wassersaenge.com/>). Seine Leidenschaft für weltweite Reisen machte ihn sensibel für Kulturen und Probleme anderer Völker. Er ist naturverbunden und liebt Tiere und Pflanzen.