Schriftliche Stellungnahme für den Finanzausschuss des Deutschen Bundestages
Öffentliche Anhörung zum digitalen Euro am 19.02.2024

Professor Dr. Rainer Böhme
Universität Innsbruck, Institut für Informatik

Der digitale Euro kann eine Chance für die Eurozone sein, die Institution des frei nutzbaren öffentlichen Geldes im digitalen Zeitalter zu erhalten.

Ob dies gelingt, hängt maßgeblich von der ökonomischen, rechtlichen und insbesondere technischen Ausgestaltung ab. Während ein Gesetzesvorschlag vorliegt und die wirtschaftswissenschaftliche Literatur unter Einbeziehung von Universitäten, Forschungsinstituten und den Forschungsabteilungen der Zentralbanken mögliche ökonomische Aspekte untersucht, sind über die technische Ausgestaltung des digitalen Euros bislang sehr wenige verbindliche Informationen verfügbar. Eine Beurteilung der Chancen und Risiken eines digitalen Euros ist erst dann seriös möglich, wenn das technische Konzept des Gesamtsystems[1] vorliegt, am besten unterstützt durch eine Referenzimplementierung.

Die Entwicklung und erfolgreiche Einführung einer Zentralbankdigitalwährung für einen großen Währungsraum ist technisch sehr anspruchsvoll. Insbesondere wenn Ziele der Datensparsamkeit, Sicherheit, Effizienz und Benutzungsfreundlichkeit gleichzeitig erreicht werden sollen, unterscheidet sich die Technik erheblich sowohl von bekannten elektronischen Zahlungssystemen, als auch von aktuellen Entwicklungen im Bereich der Krypto-Assets, die seit der Erfindung von Bitcoin oft als Inspiration herangezogen werden. Ich glaube, dass sich der digitale Euro technisch grundlegend von bisherigen IT-Projekten unterscheidet, welche die Zentralbanken im Eurosystem regelmäßig unter Einbeziehung von privaten Dienstleistungsunternehmen umsetzen. Zur Verdeutlichung: Ein Zahlungsverkehrssystem wie TARGET2 kombiniert bestehende Elemente unter Nutzung von Konzepten und Werkzeugen aus dem Silicon Valley. Für den digitalen Euro braucht es gänzlich neue Konzepte und Werkzeuge. Technisch wird hier Neuland betreten. Das Eurosystem muss die Köpfe gewinnen und halten, die sonst im Silicon Valley arbeiten würden.

Bislang ist Bargeld die einzige Form, in der alle Menschen direkte Forderungen gegenüber der Zentralbank halten und im Zahlungsverkehr austauschen können, ohne dabei Datenspuren zu hinterlassen. Mir ist keine Technik bekannt, welche diese Eigenschaften von Bargeld exakt digital abbilden könnte. Also sollte das Ziel eines digitalen Euros sein, Bargeld zu ergänzen und seine Eigenschaften so gut wie möglich nachzubilden. In einem Aufsatz bezeichnen mein Koautor und ich dies als die „Suche nach einer minimalinvasiven Technologie“[2]. Diese Suche erfordert die Erforschung neuer Techniken sowie einen auf wissenschaftliche Befunde aufbauenden öffentlichen Diskurs über den bei der Annäherung an die Eigenschaften von Bargeld zu findenden Kompromiss.

Ambitionierte Ziele beim Datenschutz sollen ein Alleinstellungsmerkmal des digitalen Euros gegenüber bestehenden elektronischen Zahlungssystemen, bekannten Krypto-Assets und

[1] Unverbindliche Architekturskizzen der EZB aus dem Jahr 2023 sehen verschiedene Komponenten vor. Selbst wenn die zentrale Datenbank nur pseudonyme Werte speichert, ist zu untersuchen, ob bspw. die IT-Sicherheit und der Datenschutz in allen Komponenten gewährleistet ist, wie z.B. im geplanten Verzeichnisdienst, welcher menschenlesbare Identifikatoren der Zahlungsparteien auf 14-stellige, eindeutige Kontonummern auflösen soll.
[2] Auer, R. and Böhme, R. Digitales Zentralbankgeld: Auf der Suche nach einer minimalinvasiven Technologie. In J. Beermann, ed., *20 Jahre Euro. Zur Zukunft unseres Geldes*. Siedler, München, 2022, S. 437–464.

den Zentralbankdigitalwährungen anderer Länder werden. Grundsätzlich kann jedes digitale System im Prinzip zu einem Überwachungsinstrument derjenigen werden, die die Technik entwerfen und betreiben. Tatsächlich ist es oft einfacher, ein überwachbares System zu entwickeln als ein datenschutzfreundliches. Es erfordert erheblichen Mehraufwand, um Überwachung und Missbrauch – auch durch die Betreiber selbst – technisch zu verhindern. Aber es ist möglich: Informatikerinnen und Informatiker erforschen Techniken zur Gewährleistung eines nutzerüberprüfbaren Datenschutzes seit circa 40 Jahren. In ihren Vorschlägen werden in der Regel neuartige kryptographische Verfahren, vertrauenswürdige Hardware und die Verteilung von Aufgaben auf unabhängige Parteien kombiniert. Selbst wenn Datenspuren nicht vollständig vermeidbar sein sollten, kann Technik so gestaltet werden, dass der Zugriff auf personenbezogene Daten nicht unbeobachtet erfolgen kann und Betreiber somit rechenschaftspflichtig sind. Dies ist meistens leichter realisierbar als maximale Datensparsamkeit. In vielen Fällen kann dabei auf wohl untersuchte kryptographische Verfahren zurückgegriffen werden, welche mehr Sicherheit versprechen und effizienter sind als neuartige kryptographische Verfahren. In einem an ein globales Publikum gerichteten Aufsatz, der das Spannungsfeld zwischen Privatsphäre und einer effizienten Prävention und Verfolgung von Straftaten beleuchtet, empfehlen wir diesen Ansatz für Zentralbankdigitalwährungen.[3]

Ich möchte an dieser Stelle die Bedeutung von Datensparsamkeit betonen. Zahlungsdaten zeichnen ein detailliertes Bild über das Verhalten fast jeder Person. Sie offenbaren zum Beispiel Vermögensverhältnisse, Gesundheit, Aufenthaltsorte und Interessen. Während eine datenschutzrechtliche Rechtmäßigkeit formell durch Schaffen von Rechtsgrundlagen für die Verarbeitung personenbezogener Daten relativ einfach herstellbar ist, reicht dies möglichweise nicht aus, um Bedenken vollständig auszuräumen und das Vertrauen der Menschen zu gewinnen. In einem verteilten System ist es sehr kompliziert, Daten, die einmal erhoben wurden, vollständig zu löschen. Noch schwieriger ist es zu gewährleisten, dass Betroffene sich von der Löschung selbst überzeugen können. Daten, die zu einem bestimmten Zweck erhoben wurden, könnten durch technische und menschliche Fehler – „Datenpannen“ – unberechtigt weitergegeben oder gar öffentlich werden. Gesetzliche Regelungen zum Umgang mit gespeicherten Daten könnten neu interpretiert oder in Zukunft geändert werden. Diese abstrakten Risiken schaffen Unsicherheit, können Nährboden für Spekulationen geben und in Folge Menschen dazu veranlassen, ihr Verhalten an eine gefühlte Bedrohung anzupassen, was mutmaßlich mit einem Verlust von Freiheit einhergeht.

Selbst eine glaubhafte Zusicherung, es würden lediglich notwendige Daten gesammelt, ist meiner Meinung nach unzureichend, solange die technische Ausgestaltung des digitalen Euros nicht bekannt ist. Denn es kommt auf die konkrete technische Architektur an, welche Daten tatsächlich zum Betrieb notwendig sind. Beispielsweise ist die Durchsetzung von Haltelimits[4] nicht datensparsam und effizient realisierbar, da jede Person eindeutig identifiziert und alle ihr zugeordneten Aufbewahrungsorte für digitale Euros europaweit miteinander synchronisiert werden müssten. Es ist also bereits bei der Wahl der Architektur auf Datensparsamkeit zu achten und es sind Anstrengungen nötig, dies über den gesamten

[3] Auer, R., Böhme, R., Clark, J., and Demirag, D. Mapping the Privacy Landscape for Central Bank Digital Currencies. *Communications of the ACM*, 66, 3 (2023), 46–53.

[4] Haltelimits wurden zur Begrenzung der Wertaufbewahrungsfunktion vorgeschlagen. Eine Begrenzung ist ökonomisch sinnvoll, allerdings kann sie mit anderen Mitteln erreicht werden. Die fehlende Verzinsung sowie eine geringere Chance auf Aufklärung und Erstattung im Falle eines Verlustes können den digitalen Euro diesbezüglich bargeldähnlicher machen.

Entwurfs- und Entwicklungsprozess hinweg glaubhaft zu vermitteln. Ein Bekenntnis zu Peer Review und Open Source, Wertschätzung von konstruktiven Beiträgen aus der Open-Source-Community, Transparenz über die Beteiligung der Finanz- und IT-Industrie, Offenheit im Umgang mit Schwachstellen, die Etablierung eines Bug-Bounty-Programms, Feldtests mit diversen Benutzerinnen und Benutzern, technische Stresstests und Krisensimulationen sind Maßnahmen, die Vertrauen schaffen können, insbesondere wenn sie fachlich versierte Meinungsführerinnen und Meinungsführer erreichen. Dies bekräftigt meine Empfehlung zu einem öffentlichen Diskurs über die technische Ausgestaltung des digitalen Euros unter Einbeziehung von Wissenschaft, Wirtschaft und Zivilgesellschaft.

Datenschutz bei Zentralbankdigitalwährungen hat viele Dimensionen. Er beginnt im Privaten – sollen Zahlungen mit dem digitalen Euro Belege auf dem Endgerät hinterlassen, auf die ein Partner potenziell zugreifen kann? Eine Geldbörse hat kein Gedächtnis. Als nächstes betrifft er die Beziehung zwischen Zahlenden und Zahlungsempfängern – sollen die Kassensysteme Kundinnen und Kunden anhand ihrer Endgeräte oder Kontonummern wiedererkennen und potenziell Profile bilden können? Im Moment funktioniert das technisch bei (Kunden-)karten. Wie viele Informationen über das Zahlungsverhalten erhalten Finanzinstitute und wie dürfen sie und Dritte diese kapitalisieren? Selbst wenn Nutzung und Weitergabe formell von einer Einwilligung abhängen, lehrt uns die Erfahrung mit datenschutzrechtlichen Einwilligungen im Internet, wie sorglos Menschen damit umgehen. Schließlich bleibt das Verhältnis zu staatlichen Stellen. Unter welchen Voraussetzungen und von welcher Stelle stehen der Strafverfolgung Transaktionsdaten aus dem Betrieb des digitalen Euros zu Verfügung? Ist rückwirkender Zugriff technisch möglich, oder sollen lediglich einzelne Konten bei hinreichendem Verdacht ab dem Zeitpunkt einer Anordnung beobachtet werden können? Wie schützt man Bestands- und Transaktionsdaten vor dem Zugriff durch staatliche Stellen anderer Staaten bzw. unter welchen Voraussetzungen werden Daten ins Ausland übertragen? Für alle diese Fragen kann man Analogien bei der Bargeldnutzung suchen, aber die Antworten sind aus konzeptionellen oder technischen Gründen oft nicht übertragbar. Dies unterstreicht, dass mit der Entwicklung des digitalen Euros die Verantwortung einhergeht, wesentliche Bestandteile des Geld- und Währungssystems neu zu denken.

Geld und Information gehen im digitalen Zeitalter ineinander über. Es wird schwieriger, die Neutralität des Geldes in jeder Hinsicht sicherzustellen. Der digitale Euro ist eine Chance, die Eurozone zukunftssicher zu machen und im Standortwettbewerb mit Wirtschaftsräumen gleichzuziehen, die ebenfalls an Zentralbankdigitalwährungen arbeiten. Eine Umkehr erscheint mir kaum möglich. Wenn der digitale Euro nicht kommen sollte – oder eingeführt und von der Bevölkerung nicht angenommen werden sollte – dann ist es gut möglich, dass wir Zeugen der gleichen Entwicklung werden, jedoch mit privatem Geld. Das bedeutet den Verlust der Möglichkeit gestaltend einzugreifen, den Verzicht auf Gewinne aus Seigniorage, den Kontrollverlust über Zahlungsdaten, die Aufgabe eines wesentlichen Stücks digitaler Souveränität und birgt die Gefahr, dass nicht alle Menschen gleichen Zugang zu Geld haben.

Ich glaube, Erfolgsfaktoren für einen digitalen Euro sind, dass er für alle Menschen zugänglich sowie im Alltag bequem, sicher und frei nutzbar ist, und sie davon überzeugt sind, dass sein Wert stabil und private Zahlungen anonym bleiben.

gez. Univ.-Prof. Dr. Rainer Böhme