

Bankstil – Spezial

Der Digitale Euro



Autor: Ralf Keuper

August 2023

INHALTSVERZEICHNIS

EINLEITUNG.....	3
DEFINITIONEN	4
Digitales Zentralbankgeld (CDBC).....	4
Digitaler Euro.....	4
Zeitschiene	5
DIE ROLLE DER BANKEN	6
EINSATZFELDER EINES DIGITALEN EURO.....	6
Zahlungsverkehrsabwicklung	7
Maschinenökonomie	7
Unternehmensfinanzierung	7
Programmierbar oder nicht programmierbar?.....	8
Digitaler Euro ohne Blockchain	10
IDENTIFIZIERUNG / ANONYMITÄT / DATENSCHUTZ.....	12
Wie identitätsbasiert soll Digitales Zentralbankgeld sein?.....	14
Digitaler Euro in Kombination mit digitalen Identitäten für Personen und Maschinen.....	18
EUDI	19
SICHERHEIT DES DIGITALEN EURO.....	20
SCHLUSSBETRACHTUNG.....	23

EINLEITUNG

Wenn es nach den Vorstellungen der EU-Kommission geht, dann wird der digitale Euro dazu beitragen, die Effizienz bei der (grenzüberschreitenden) Zahlungsabwicklung zu steigern, die Inklusion zu fördern und die digitale Souveränität der EU zu sichern. Die fortschreitende Digitalisierung, die Bestrebungen privater Unternehmen und Organisationen, Stablecoins herauszugeben und die Pläne anderer Regionen in der Welt, ein eigenes digitales Zentralbankgeld zu emittieren, machen die Einführung eines digitalen Euro zwingend.

Für die Verbraucherinnen und Verbraucher ist der digitale Euro, sofern er überhaupt bekannt ist, kaum zu greifen. Begriffe wie Retail CDBC, Wholesale CDBC, tokenbasiert oder kontobasiert in Kombination mit der Blockchain lassen das Thema abstrakt erscheinen. In der Tat ist es alles andere als einfach, sich einen Überblick über die Thematik zu verschaffen.

Ungeachtet dessen sind die Planungen für die Einführung eines digitalen Euro schon weit fortgeschritten. Aktuell kursiert als Einführungstermin das Jahr 2027. Der digitale Euro ruft in den verschiedenen gesellschaftlichen Gruppen ein geteiltes Echo hervor. Während die Banken und die Wirtschaft im Prinzip keine gravierenden Einwände haben, sind Datenschützer da weniger entspannt. Es drohe die Einführung eines Überwachungsstaates lautet einer der Kritikpunkte. Andere machen den Erfolg davon abhängig, ob ein Blockchain eingesetzt wird oder nicht. Pessimisten halten das Vorhaben schon jetzt für gescheitert¹.

Der vorliegende Report verfolgt die Absicht, für mehr Übersichtlichkeit zu sorgen, ohne dabei den Anspruch auf Vollständigkeit zu erheben. Vorgestellt werden zunächst die verschiedenen Begriffe, die in der Diskussion um Digitales Zentralbankgeld besonders häufig verwendet werden. Im Anschluss daran werden, nachdem die Rolle der Banken kurz beleuchtet wird, die verschiedenen Einsatzfelder des digitalen Euro diskutiert. Großen Raum nimmt die Frage der Identifizierung ein, die nicht zuletzt durch die geplante Einführung der EUID-Wallet an Aktualität gewonnen hat.

¹ [Der digitale Euro hat keinen Sinn](#)

DEFINITIONEN

Nachfolgend nun die Definition der wesentlichsten Begriffe.

DIGITALES ZENTRALBANKGELD (CDBC)

Die Einführung von Digitalem Zentralbankgeld, wie es momentan in zahlreichen Ländern unter dem Begriff Central Bank Digital Currency (CDBC) diskutiert und z.T. schon getestet wird², soll die Digitalisierung im Finanzsektor und in den anderen Bereichen der Wirtschaft beschleunigen.

Eine Central Bank Digital Currency (CDBC) wäre eine Alternative zum Giralgeld der Banken. Liquiditäts- und Gläubigerrisiken wären damit ausgeschlossen.

Unterschieden wird bei einer Central Bank Digital Currency (CBDC) zwischen Wholesale CBDC und einer Retail-CBDC. Bei der Wholesale CBDC werden die digitalen Zentralbankreserven nur Finanzinstituten zugänglich gemacht. Bei einer Retail-CBDC bekommen natürliche Personen, Unternehmen und staatliche Behörden den direkten Zugang zum Zentralbankgeld. Die Retail-CBDC würde laut ihren Befürwortern zu deutlichen Effizienzgewinnen bei der Zahlungsabwicklung sowie zu mehr Finanzstabilität führen. Die Insolvenz einer Geschäftsbank hätte in dem Szenario keine negativen Auswirkungen auf die Kunden. Während eine Wholesale-CBDC verzinst werden kann, gilt das für eine Retail-CBDC nicht.

Dennoch bleiben einige Herausforderungen bzw. offene Fragen: Sollen CDBC's zinstragend sein oder einer Art zinslosem Bargeld entsprechen? Soll es Token-/Value-based und von Person zu Person übertragbar sein oder von Bankkonto zu Bankkonto transferiert werden können? Soll es sich dabei um eine 100%ige Deckung handeln, wie beim Vollgeld? Soll sie programmierbar oder nicht programmierbar sein?

DIGITALER EURO

² [2022 BIS survey on central bank digital currencies and crypto](#)

DIGITALER EURO

Der Digitale Euro zählt zur „Familie“ der Central Bank Digital Currency. Der Digitale Euro soll das Bargeld nur ergänzen, nicht ersetzen. Darüber hinaus soll der digitale Euro die strategische Autonomie Europas sichern und dem Zahlungsverkehrssystem einen erheblichen Digitalisierungsschub geben³. Angestrebt wird weiterhin, den Digitalen Euro so zu gestalten, dass damit anonyme Zahlungen möglich sind, so wie heute mit dem Bargeld⁴.



Die Transaktionskosten würden deutlich sinken, das Kontrahentenrisiko sich fast auflösen. Viele Intermediäre, wie Korrespondenzbanken, wären nicht mehr nötig⁵.

ZEITSCHIENE

Momentan führt die EZB eine Untersuchungsphase für die mögliche Einführung eines digitalen Euro durch. Die EZB hat angekündigt, nach Abschluss der Untersuchung im Herbst 2023 über die Fortsetzung weiterer vorbereitender Arbeiten zu entscheiden. Stimmt der EZB-Tat dem Vorhaben zu, könnte mit der Einführung eines Digitalen Euro ab 2027 begonnen werden⁶.

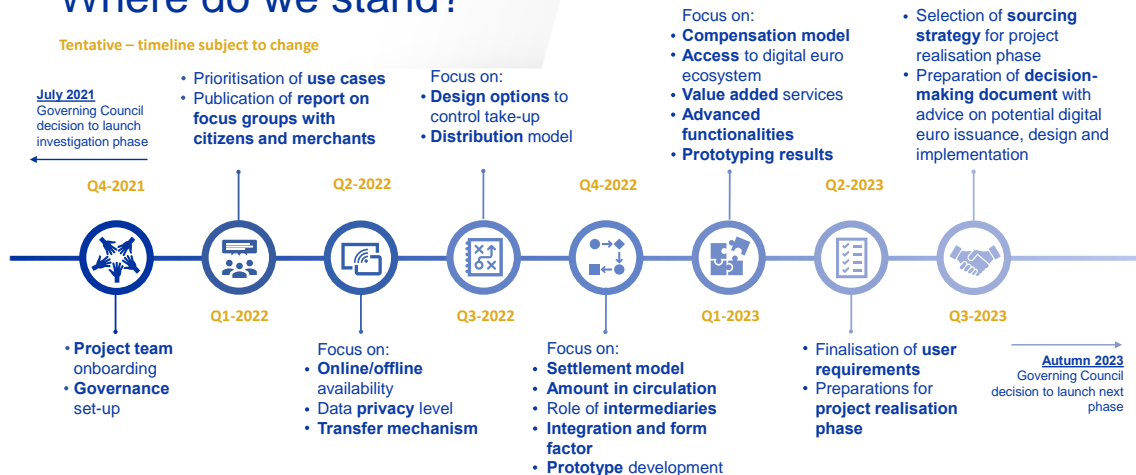
³ [Digitaler Euro](#)

⁴ Vgl. dazu: [Digitales Zentralbankgeld und der digitale Euro](#)

⁵ Vgl. dazu: [Digitales Geld: Optionen für den Zahlungsverkehr](#)

⁶ [Nächste Schritte: Digitaler Euro](#)

Where do we stand?



DIE ROLLE DER BANKEN

Der aktuelle Vorschlag der EU-Kommission sieht folgende Rollenverteilung vor⁷:

- Banken und Sparkassen sollen im Rahmen des Digitalen Euro das Onboarding von Kunden übernehmen (Identifizierung des Kunden, Registrierung der Kundenauthentifizierung etc.)
- Banken und Sparkassen sollen wichtige Dienstleistungen rund um die Abwicklung von Zahlungen anbieten, bspw. das Aufladen des Digitalen Euro über Bargeld oder Konten bei Banken und Sparkassen
- Die EZB setzt zudem einen Fokus darauf, dass der Digitale Euro mit sog. „Waterfall-“ und „ReverseWaterfall“ Funktionen mit einem Geschäftsbankkonto verbunden sein soll. Diese Funktionen ermöglichen das Auslösen oder Empfangen von Zahlungen oberhalb des Haltelimits.

EINSATZFELDER EINES DIGITALEN EURO

Wie bereits erwähnt, ist die Erwartung, dass der Digitale Euro die Effizienz bei der Abwicklung von Finanztransaktionen deutlich verbessert. Der digitale Euro wird

⁷ [Einordnung der EZB-Designprinzipien für einen Digitalen Euro und Beschreibung der Auswirkungen auf unser zweistufiges Geldsystem](#)

DIGITALER EURO

demnach die Entwicklung europaweiter und interoperabler Lösungen für den Massenzahlungsverkehr, einschließlich der vollständigen Einführung von Sofortzahlungen, erleichtern. Weitere Einsatzfelder sind die Maschinenökonomie und die Unternehmensfinanzierung.

ZAHLUNGSVEREKEHRSABWICKLUNG

Die Europäische Kommission fordert, dass Händler- oder Inter-PSP-Entgelte werden reguliert werden müssen, um sicherzustellen, dass sie sich an den relevanten Kosten der Zahlungsdienstleister, einschließlich einer angemessenen Gewinnspanne orientieren und nicht höher sind als die für das effizienteste vergleichbare Zahlungsmittel verlangt⁸. Um eine effektive Nutzung des digitalen Euro als gesetzliches Zahlungsmittel zu gewährleisten sollte die EZB Empfehlungen aussprechen, kann aber auch eine verbindliche Höhe dieser Gebühren oder Entgelte festlegen. Die Gebühren oder Entgelte sollten nicht zu übermäßigen Belastungen Händler führen, sondern auch einen ausreichenden Ausgleich für die Kosten bieten, die den Zahlungsdienstleistern bei der Verbreitung des digitalen Euro entstehen.

MASCHINENÖKONOMIE

Ebenfalls einen großen Effekt hätte der digitale Euro auf die sog. Machine Economy und hier insbesondere auf die Machine-to-Machine-Zahlungen. Autos, Maschinen und andere technische Geräte könnten ihre Dienste auf Pay-per-use – Basis im großen Stil anbieten. Profitieren würde davon u.a. das Leasing- und Absatzfinanzierungsgeschäft. Wenn jede Maschine einen eigenen Computerchip und Geldbeutel (Wallet) erhält, dann wäre sie in der Lage, Zahlungen zu empfangen, Geld zu überweisen und Buchungen in den ERP-Systemen anzustoßen⁹.

UNTERNEHMENSFINANZIERUNG

⁸ [Entwurf zum Digitalen Euro \(EU-Kommission\)](#)

⁹ [Der digitale Euro auf der Blockchain \(Bitkom-Infopapier\)](#)

DIGITALER EURO

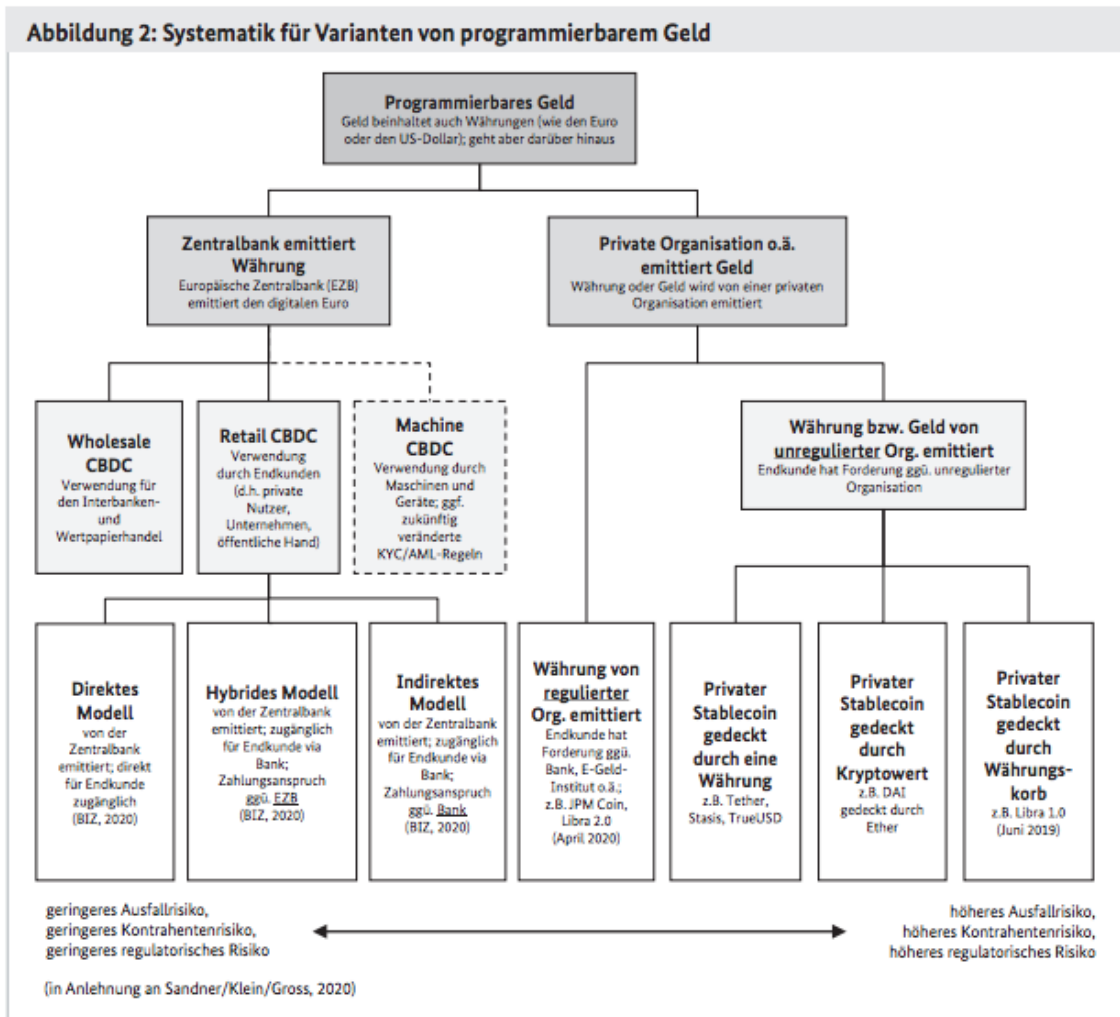
Unternehmen hätten die Möglichkeit, den digitalen Euro für die Kapitalbeschaffung oder Emission von digitalen Wertpapieren zu nutzen. Dies könnte dazu beitragen, die Effizienz und den Zugang zu Finanzierungsmöglichkeiten für Unternehmen zu verbessern¹⁰.

PROGRAMMIERBAR ODER NICHT PROGRAMMIERBAR?

Die Befürworter eines programmierbaren Digitalen Euros verweisen auf die zahlreichen Vorteile. Nur ein programmierbarer Euro könne die strukturellen Schwächen der heutigen Transaktionsabwicklung überwinden. Diese ist geprägt von einer Trennung der Geschäftsvorfälle in den Liefer- und den Bezahlprozess. Da beide Teilprozesse verschiedene IT-Systemen durchlaufen, kommt es zu zeitlichen Verzögerungen, Medien- und Systembrüchen sowie zu aufwändigen Abstimmungen. Mit der Blockchain könnten die beiden separaten Teilprozesse synchronisiert und automatisiert werden. Eine Schlüsselrolle übernehmen dabei Smart Contracts, d.h. Verträge, die beim Eintreten bestimmter Ereignisse automatisch ausgeführt werden

¹⁰ [Digitaler Euro: Einführung, Funktion und Risiken](#)

DIGITALER EURO



„Smart Contracts ermöglichen hierbei die korrekte und automatisierte Ausführung von Vertragsvereinbarungen. Mit der Erfüllung der Vereinbarungen sind häufig auch Bezahlvorgänge verbunden. Damit diese unabhängig von der Betragshöhe vollautomatisiert erfolgen können, ist der Euro in programmierbarer Form erforderlich“¹¹

Für den Fall, dass die Maschinenökonomie Realität wird, könnte die Einführung einer Machine CBDC sinnvoll sein. Sobald die rechtlichen Fragen geklärt sind und jede Maschine über eine sichere Digitale Identität verfügt, stünden M2M-Zahlungen und Zahlungen zwischen Menschen und Maschinen (technologisch) nichts mehr im Weg. Nach den Vorstellungen der EU-Kommission wäre der digitale Euro kein programmierbares Geld und könnte daher nicht dazu verwendet werden, seine Ausgaben zu begrenzen oder auf bestimmte Waren oder Dienstleistungen zu lenken: Als digitale Form der einheitlichen Währung sollte er vollständig fungibel sein. Der

¹¹ [Der digitale, programmierbare Euro \(FinTechRat beim Bundesministerium der Finanzen\)](#)

DIGITALER EURO

digitale Euro sollte für digitale Euro-Zahlungstransaktionen sowohl offline als auch online verfügbar sein.

Ein digitaler Euro könnte auch europäische Unternehmen für künftige Anwendungsfälle in der Industrie 4.0 und im Web 3 (d.h. dezentrales Internet) unterstützen Internet) unterstützen, indem er ihnen eine öffentliche Alternative zu programmierbaren Zahlungen bietet, die möglicherweise von CBDCs ausländischer Länder und Stablecoins von Technologieunternehmen stammen oder von ihnen kontrolliert werden.

Der digitale Euro sollte jedoch die Programmierung von bedingten digitalen Euro-Zahlungen durch Zahlungsdienstleister unterstützen. Die Zahlungsdienstleister könnten verschiedene Logik entwickeln, um den Nutzern des digitalen Euro eine Reihe von bedingten Zahlungsvorgängen anzubieten, einschließlich automatisierter Zahlungstransaktionen für das Einzahlen oder Abheben von digitalen Euro, Daueraufträge, die automatische Zahlungen eines bestimmten Betrags zu einem bestimmten Datum auslösen, und Zahlungen zwischen Automaten, die so programmiert sind, um automatisch Zahlungen für ihre eigenen Ersatzteile bei deren Bestellung auszulösen, für das Laden und Bezahlen von Strom zu den günstigsten Marktkonditionen, für das Bezahlen von Versicherung sowie Leasing- und Wartungsgebühren auf Nutzungsbasis.

DIGITALER EURO OHNE BLOCKCHAIN

Es gilt für viele als ausgemacht, dass digitales Zentralbankgeld ohne Blockchain nicht realisiert werden kann. Möglich ist es dennoch.

Beim Banknotenhersteller G+D ist man davon überzeugt, dass der digitale Euro sehr gut ohne Blockchain auskommt. Zwar sei die Blockchain *“eine hervorragende Technologie für bestimmte Anwendungsfälle. Da eine CBDC jedoch von einer vertrauenswürdigen Institution ausgegeben wird, ist der Einsatz von Blockchain hier nicht notwendig. Manche Designkriterien einer CBDC könnten durch Blockchains und Distributed-Ledger-Technologie (DLT) erfüllt werden. Allerdings hat G+D Anforderungen ermittelt, die damit nur schwer umzusetzen sind. Dazu gehören sichere fortlaufende Offline-Zahlungen, die Möglichkeit, Datenschutz und Transparenz optimal*

DIGITALER EURO

aufeinander abzustimmen, und die Garantie größtmöglicher Stabilität ohne einen Single Point of Failure im CBDC-Ökosystem¹²“.

Um die Sicherheit digitaler Zentralbankwährungen gewährleisten zu können, sei ein ganzheitlicher Ansatz unabdingbar. Die Zentralbanken und Geschäftsbanken übernehmen dabei die Schlüsselrollen.

Programmierbare Zahlungen lassen sich sehr gut ohne Blockchain durchführen, wie im Internet der Dinge bzw. der Machine Economy. So könnten programmierbare Machine-to-Machine-Payments es *“ermöglichen, dass Maschinen eigenständig Teile und Materialien bestellen, wenn die Lagerbestände knapp werden. Elektrofahrzeuge könnten Ladevorgänge ganz einfach mit einem vorprogrammierten Smart Contract bezahlen – ganz ohne menschliches Zutun. In der Welt des IoT könnten programmierbare Zahlungen völlig neuen Geschäftsmodellen den Weg ebnen sowie die Automatisierung von Zahlungen für den B2B-Bereich ermöglichen”*.

Bei G+D hat man mit Filia eine Lösung entwickelt, bei der der monetäre Wert durch ein Datenelement repräsentiert wird. Die Zahlung erfolgt durch die Übermittlung dieses Datenstücks von einer Person zur anderen, analog zu Barzahlungen, die durch die Übertragung von physischen Banknoten oder Münzen von Person A zu Person B abgewickelt werden (wertbasierter Ansatz).

In der Praxis sähe das dann so aus, dass die Erstellung und Ausgabe der Dateien, die den Geldwert repräsentieren, *“in einer hochgesicherten Offline-Umgebung bei der Zentralbank erfolgt, während die Distribution von Geschäftsbanken oder anderen Finanzdienstleistern übernommen wird. Zahlungsdienstleister können Filia – als Teil eines größeren Bezahlsystems – in ihre eigenen Angebote integrieren, um neue Geschäftsmodelle zu ermöglichen sowie Wachstum und Innovation in einem offenen System fördern”*.

Nach Ansicht des Chefvolkswirts der Schweizerischen Nationalbank, Carlos Lenz, ist die Blockchain für digitales Zentralbankgeld ungeeignet. Eine dezentrale Lösung auf Blockchain-Basis sei sehr ineffizient. Der Leiter der Zahlungsverkehrsanalyse bei der Deutschen Bundesbank, Diehl, ist ebenfalls der Auffassung, dass die Blockchain-

¹² [Digitales Zentralbankgeld ohne Blockchain](#)

DIGITALER EURO

Technologie für CBDC nicht wirklich notwendig ist, wobei er auf CBDC-Initiativen wie Chinas digitalen Yuan und Schwedens e-krona verweist, die beide keine Blockchain einsetzen. Öffentliche oder erlaubnisfreie Blockchains für CBDC-Systeme zu implementieren, ergäbe keinen Sinn, so Diehl.

IDENTIFIZIERUNG / ANONYMITÄT / DATENSCHUTZ

Bei der Einführung digitaler Zentralbankwährungen (CBDC) stehen verschiedene Alternativen zur Verfügung. Eine wichtige Frage ist dabei, welche Rolle der private Sektor spielen soll. Von nicht geringerer Bedeutung ist, wo die Zahlungsdaten und digitalen Identitäten verwaltet werden sollen und wer darauf Zugriff hat.

Fast alle Zentralbanken, so die Autoren von [Central bank digital currencies: motives, economic implications and the research frontier](#), die ein CBDC in Erwägung ziehen, gehen davon aus, dass der private Sektor in einem CBDC-System eine wichtige Rolle spielen wird, insbesondere bei der Versorgung von Haushalten und Unternehmen. Sowohl Geschäftsbanken als auch Nicht-Banken-Payment Service Provider (PSPs) müssen in der Lage sein, verbrauchernahe Dienste anzubieten, sodass die Nutzer Geld von einem Bankkonto, einer Kreditkarte oder anderen Zahlungsdiensten auf eine CBDC-Geldbörse überweisen können. Die Nutzer sollten außerdem die Möglichkeit haben, mit einer Vielzahl von Zahlungsmitteln zu bezahlen, z. B. mit Prepaid-CBDC-Geräten, Karten mit Offline-Funktionen oder Smartphone-Geldbörsen, die eigenständig sind oder in Bank- oder Big-Tech-Apps integriert sind.

Demnach gibt es stichhaltige Argumente dafür, warum ein einstufiges System, das vollständig von der Zentralbank betrieben wird, nicht wünschenswert ist. Direkte CBDCs würden eine weitgehende Verlagerung der operativen Aufgaben (und Kosten) vom privaten auf den öffentlichen Sektor bedeuten. Die Zentralbanken streben weder danach, den privaten Sektor bei diesen verbrauchernahen Tätigkeiten zu ersetzen, noch sind sie in der Lage, dies zu tun.

Eine Alternative ist eine operative Architektur, in der der private Sektor alle Massenzahlungen durchführt, während die Zentralbank eine Backup-Infrastruktur betreibt. Diese Klasse von "hybriden" CBDC-Architekturen kombiniert die Glaubwürdigkeit einer direkten Forderung an die Zentralbank mit dem Komfort der Zahlungsdienste des privaten Sektors. Wenn ein PSP ausfällt, muss die Zentralbank in der Lage sein, Forderungen eindeutig zu erfüllen und im Idealfall die

DIGITALER EURO

Zahlungen für die Kunden des ausgefallenen Zahlungsdienstleisters ohne große Verzögerung wieder aufnehmen. Diese Fähigkeit erfordert, dass der Zentralbank ausreichende Informationen über Privatkundenkonten (oder Pseudonyme bei anonymen Konten) zur Verfügung stehen.

Einige Zentralbanken scheuen möglicherweise davor zurück, einen Datensatz mit allen Kundendaten zu führen, zum Beispiel aufgrund von Bedenken hinsichtlich des Datenschutzes und der Datensicherheit. Eine weitere Option ist daher eine Konstruktion, bei der die Zentralbank keine Informationen über Massentransaktionen hat, so wie es bei den heutigen Zahlungssystemen der Fall ist. Eine Variante ist eine "vermittelte" Architektur, bei der die Zentralbank nur die Großhandelsalden der einzelnen Zahlungsverkehrsdienstleister erfasst. Der Nachteil ist, dass die Zentralbank Forderungen einlösen muss, über die sie nicht direkt verfügt.

Um die Glaubwürdigkeit von Bargeld zu gewährleisten, müssten die Zahlungsverkehrsdienstleister daher genau überwacht werden, um jederzeit sicherzustellen, dass die der Zentralbank gemeldeten Großkundenbestände der Summe aller Privatkundenkonten entsprechen.

Der größte Konflikt besteht zwischen der Privatsphäre der Nutzer und der Integrität des Zahlungssystems. Eine vollständig anonyme CBDC-Konstruktion könnte analog zum Bargeld schwerwiegende Nachteile für die Integrität des Zahlungssystems haben und illegale Transaktionen, Geldwäsche, Terrorismusfinanzierung usw. ermöglichen. Jedoch bringt die vollständige Aufzeichnung der Transaktionen, die mit den Identitäten der Nutzer verknüpft sind, eigene Herausforderungen mit sich, insbesondere im Bereich der Cybersicherheit, da die Zentralbank zu einem attraktiven "Honigtopf" für Hacker werden könnte. Dies ist ein weiterer Grund für einige Zentralbanken, eine intermediäre Architektur zu bevorzugen.

Zentralbanken können ihre Systeme so gestalten, dass sie einen höheren Datenschutz bieten als Systeme des privaten Sektors. Das ist allerdings mit Kosten verbunden. Überdies erfordert eine angemessene Gestaltung eine öffentliche Überprüfung und Aufsicht. Ein Vorschlag ist die Verwendung von Zero-Knowledge-Proofs in einem softwarebasierten CBDC-System. Außerdem können die Anwendungsprogrammierschnittstellen (APIs) in einem CBDC-System den Datenaustausch auf die für eine bestimmte Transaktion erforderlichen Informationen

DIGITALER EURO

beschränken und den Benutzern eine größere Kontrolle über die von ihnen erzeugten Daten geben.

WIE IDENTITÄTSBASIERT SOLL DIGITALE ZENTRALBANKGELD SEIN?

Die entscheidende Frage bei der Einführung des digitalen Euros ist, wie eng das digitale Zentralbankgeld mit der Identität des Kontoinhabers, der Kontoinhaberin verknüpft werden soll. Gehören anonyme Zahlungen, wie heute noch mit dem Bargeld, bald der Geschichte an?

Eine Central Bank Digital Currency (CDBC) kann entweder Token-/Value-based oder Account-based sein. Im ersten Fall wird das Geld bzw. ein Wertgutschein von Person zu Person übertragen, während im zweiten Fall der Transfer von Bankkonto zu Bankkonto vollzogen wird. Die meisten Zentralbanken, wie die EZB, bevorzugen den kontobasierten oder den identitätsbasierten Ansatz.

Bereits heute übernehmen die Geschäftsbanken die Aufgabe der Identifizierung (KYC) bei der Kontoeröffnung. Ein Geldsystem, das sich weitgehend außerhalb der staatlichen ID-Systeme bewegt, gilt als nahezu ausgeschlossen. Daraus folgt, dass das digitale Zentralbankgeld an die personenbezogenen Daten, die Kredithistorie und weitere Informationen des Kontoinhabers, der Kontoinhaberin gekoppelt wird. Wenn Geld identitätsbasiert sein soll, führt dies zu einer ganzen Reihe von ethischen Dilemmas und sozialen Fragen. Wie viel personenbezogene Daten sollen an das Konto und die jeweilige Transaktion gekoppelt werden? In welchen Fällen haben die Kontoinhaberinnen und Kontoinhaber das Recht, den Zugriff auf die personenbezogenen Daten und die Kontodaten zu verweigern? Welche (zentrale) Instanz soll die Daten verwalten? Was geschieht im Falle eines Hacks? Wenn die Banken die Aufgabe der Identifizierung übernehmen - wie werden die dabei entstehenden Kosten verrechnet?

Es existieren einige Alternativen, wie das digitale Zentralbankgeld weitgehend anonym ausgestaltet werden könnte.

Der Banknotenhersteller Giesecke + Devrient hat eine eigene Lösung entwickelt: G+D Filia: Dabei *“stellt eine von der Zentralbank erzeugte Datendatei den Geldwert dar, genau wie Banknoten und Münzen in physischen Brieftaschen. Die Datei wird gemäß dem heutigen Geldkreislauf über Geschäftsbanken verteilt. Einzelpersonen können die*

DIGITALER EURO

Datendatei dann mit Smartphones, Smartcards, Smartwatches oder anderen elektronischen Geldbörsen nutzen“.

Die deutschen Banken und Sparkassen liebäugeln derzeit mit dem Konzept der selbstbestimmten Digitalen Identitäten.

Wie kann ein Mindestmaß an Anonymität beim digitalen Euro erreicht werden? Dieser Frage geht das Forschungsnetzwerk der EZB, EUROchain, in [Exploring anonymity in central bank digital currencies](#) nach. Das Forscherteam hat dazu ein Proof of Concept erstellt¹³.

Wesentliche Erkenntnisse daraus:

Das vom ESZB entwickelte Konzept zeigt, dass es möglich ist, ein vereinfachtes CBDC-Zahlungssystem zu entwickeln, das den Nutzern ein gewisses Maß an Privatsphäre für Transaktionen mit geringem Wert bietet und gleichzeitig sicherstellt, dass Transaktionen mit höherem Wert den obligatorischen AML/CFT-Kontrollen unterzogen werden.

Eingesetzt wurde mit Unterstützung von Accenture die in Banken schon relativ weit verbreitete Blockchain-Variante R3 Corda. Transaktionen können in dem Proof of Concept anonym durchgeführt werden. Zu diesem Zweck müssen die Nutzer sog. “anonymity vouchers” erwerben, die sie dazu berechtigen, bis zu einer bestimmten Höchstgrenze anonym zu bezahlen. Geht der Bedarf darüber hinaus, muss ein weiterer “anonymity voucher” beantragt werden.

Das Konzept sieht vier Instanzen vor:

- Zwei Finanzintermediäre
- eine Zentralbank und
- eine Instanz für die Überwachung von Geldwäsche (AML Authority)

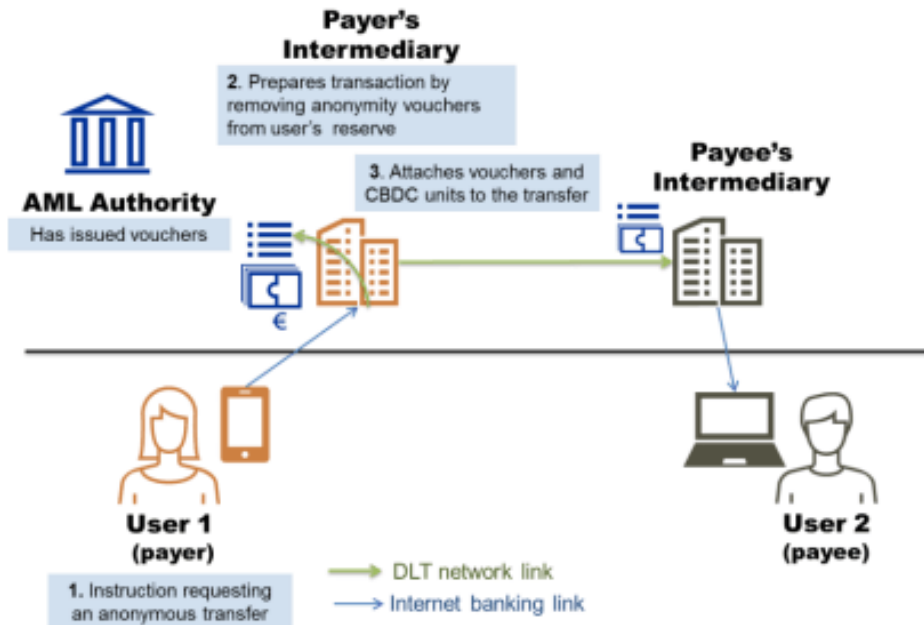
Die Intermediäre versorgen die Kunden mit digitalen Euros, die sie von der Zentralbank beziehen. Die Intermediäre führen im Auftrag ihrer Kunden die Transaktionen durch.

¹³ [Wie anonym ist ein digitaler Euro?](#)

DIGITALER EURO

Solange die Transaktionen der Kunden von den "anonymity vouchers" abgedeckt sind, werden die Zahlungen ohne AML-Check automatisch ausgeführt.

Transfer with anonymity vouchers



Source: ECB

Weiterhin übernimmt der Intermediär das Onboarding der Kunden:

Jeder Nutzer wird von einem Vermittler aufgenommen, der seinen Kunden pseudonyme Identitäten zur Verfügung stellt, die als Netzwerkadressen für CBDC-Zahlungen verwendet werden.

Die Zentralbank darf als einzige Instanz digitale Euros ausgeben und einziehen. Die AML Authority überprüft die Identitäten der Nutzer/Kunden, die großvolumige Zahlungen vornehmen. Ihre weitere Aufgabe besteht darin, wie schon erwähnt, die "anonymity vouchers" auszustellen, sofern die Bedingungen dazu erfüllt sind. Das Modell sieht darüber hinaus die Rolle eines digitalen Notars, eines "non-validating notary" vor.

Im Konzeptnachweis ermöglicht ein spezieller Knoten, der als "nicht validierender Notar" bezeichnet wird, den Vermittlern, die Gültigkeit von Zuständen zu überprüfen, indem er ein Register aller derzeit gültigen UTXOs führt. Um die Privatsphäre der Nutzer zu schützen, hat der Notar keinen

DIGITALER EURO

Zugang zu Daten wie Transaktionswerten, Nutzeradressen oder Zustandsverläufen.

Das Modell enthält momentan noch einige Lücken.

Ein Problem:

Ungeachtet des Datentrennungsmodells von Corda kann ein Teilnehmer daher einen Wissensgraphen auf der Grundlage der Informationen aufbauen, die er im Laufe der Zeit von den CBDC-Einheiten erhält. Dies bedeutet, dass Details vergangener Transaktionen von Vermittlern neuer Inhaber eingesehen werden können, die nicht an diesen Transaktionen beteiligt waren. Dennoch hat kein Intermediär zu einem bestimmten Zeitpunkt einen vollständigen Überblick über alle Netzwerkaktivitäten. Die Zentralbank kennt den aktuellen Umlauf, erhält aber nur dann Informationen über die einzelnen CBDC-Einheiten und die Pseudonyme ihrer Inhaber, wenn diese Einheiten zurückgegeben werden.

Eine mögliche Lösung:

Bis zu einem gewissen Grad lässt sich diese Herausforderung durch das Abschneiden der Historie eines Staates - das so genannte "Chain Snipping" - lösen. Dabei handelt es sich um ein technisches Verfahren, bei dem ein Intermediär die Rücknahme aller CBDC-Einheiten auf den Konten seiner Nutzer veranlasst und die Ausgabe der entsprechenden CBDC-Menge für jeden Nutzer auslöst. Indem ein Intermediär die Historie der Einheiten eines Nutzers zurücksetzt, reduziert er die Menge an Informationen, die für andere Teilnehmer sichtbar ist. Dies hat jedoch keine Auswirkungen auf die Privatsphäre des Nutzers gegenüber der Zentralbank, die nach wie vor alle Informationen über die eingelösten Einheiten erhält.

Eine weitere Möglichkeit, die Anonymität und Privatsphäre der Nutzer zu schützen, sind rotierende Public Keys, Zero-knowledge proof und Enclave Computing. Die Verwendung rotierender Schlüssel, bei denen die Nutzer regelmäßig neue Pseudonyme generieren, würde die Fähigkeit der Knoten einschränken, Transaktionen mit einzelnen Nutzern zu verknüpfen, da die Nutzer im Laufe der Zeit verschiedene Pseudonyme verwenden würden.

DIGITALER EURO

Der Europäische Datenschutzbeauftragte warnt vor einer kontobasierten Identifizierung des digitalen Euro. Dies könne „dazu führen, dass alle Transaktionen des Endnutzers identifiziert und möglicherweise nachverfolgt werden.“ Stattdessen wird ein digitaler Euro auf Basis von Tokens bevorzugt. Dabei erfolgt der Nachweis der Inhaberschaft des Geldes über einen privaten Schlüssel. Damit lasse sich die Anonymität der Zahlung sicherstellen¹⁴.

DIGITALER EURO IN KOMBINATION MIT DIGITALEN IDENTITÄTEN FÜR PERSONEN UND MASCHINEN

Vor einiger Zeit forderte Philipp Sandner, den Euro und die digitalen Identitäten auf die Blockchain zu bringen. In ähnlicher Weise plädierte daraufhin der Bankenverband in seinem Positionspapier [Jenseits von Libra: Warum die Wirtschaft einen digitalen Euro braucht](#).

Eine Forderung:

Die Identität des Nutzers eines digitalen Euros – ob Mensch oder Maschine – muss eindeutig zuzuordnen sein. Hierfür ist ein [europäischer Identitätsstandard notwendig](#), besser noch ein globaler Standard. Bei jeder Form von Digitalgeld sollten Kunden nach einem genauso strengen Standard identifiziert werden müssen, wie ihn Banken oder andere Verpflichtete nach den geltenden geldwäscherechtlichen Bestimmungen heute selbstverständlich zu berücksichtigen haben. ... Damit auch im IoT Werte direkt zwischen Maschinen übertragen und rechtssicher abgebildet werden können, sollte dieser Identitätsstandard auch eine eindeutige Zuordnung von Maschinen zu deren rechtlichen Inhabern ermöglichen.

Das nächste Ziel ist der Bereich IoT oder IIoT. Wie in der von Identity Economy zusammen mit Bankstil durchgeführten Studie [Maschinenidentitäten – Schlüssel zum Internet der Dinge](#) bereits herausgestellt wurde, fehlen nicht nur europäische Standards im Bereich der Identifizierung – schon allein in Deutschland dominiert ein Flickenteppich an Lösungen bzw. Allianzen. Die US-amerikanischen und asiatischen Internetkonzerne werden versuchen, dieses Vakuum für sich zu nutzen und Quasi-

¹⁴ [Expert:innen warnen vor Überwachungspotential](#)

DIGITALER EURO

Standards, wie schon heute im kommerziellen Internet gängige Praxis, durchzusetzen¹⁵.

EUDI

Vor einigen Wochen wurde der [Entwurf der EU-Kommission zum Digitalen Euro](#) im Internet zugänglich gemacht. Aus dem Dokument geht hervor, dass die EUDI-Wallet dabei eine zentrale Rolle übernehmen soll.

Hier nun einige Auszüge:

Die EU-weit interoperable Europäische Geldbörse für digitale Identitäten (EUID) ermöglicht den Nutzern auf freiwilliger Basis bei Zahlungen eine starke Kundenauthentifizierung und Zahlungen vorzunehmen, wie in Artikel 97 der PSD2 gefordert. Die gleichen Funktionalitäten sollten auch den Nutzern des digitalen Euro angeboten werden.

Europäische Geldbörsen für digitale Identitäten könnten digitale Transaktionen erleichtern, indem sie Folgendes ermöglichen: Authentifizierung, Identifizierung und den Austausch von Attributen, einschließlich Lizenzen und Zertifikaten. Die Europäische Geldbörsen für digitale Identitäten sollten zum universellen Zugang zum digitalen Euro und zu dessen Verwendung beitragen. Die Mitgliedstaaten sollten europäische Geldbörsen für digitale Identitäten auf der Grundlage gemeinsamer Standards und Praktiken ausgeben, die in den Durchführungsvorschriften festgelegt sind. Die Europäische Geldbörse für digitale Identitäten sollte über strenge und spezifische Schutzmaßnahmen zur Gewährleistung des Datenschutzes und des Schutzes der Privatsphäre sowie eine hochrangige Sicherheits-Zertifizierung verfügen. Die von der Europäischen Zentralbank zu entwickelnden Front-End-Lösungen sollten daher die technischen Spezifikationen für die europäischen Geldbörsen für digitale Identitäten berücksichtigen. Dies würde die entsprechende Interoperabilität mit den Europäischen Geldbörsen für digitale Identitäten ermöglichen, die es erlauben würden, diese Vorteile zu nutzen.

Eine vollständige Anonymität bietet der digitale Euro nicht:

¹⁵ [Digitaler Euro in Kombination mit digitalen Identitäten für Personen und Maschinen](#)

DIGITALER EURO

Durch die Beachtung eines risikobasierten Ansatzes, der dem AML-Rahmen der Union zugrunde liegt, und durch den Ausschluss der vollständigen Anonymität steht die Initiative im Einklang mit den Zielen des AML-Pakets, das von der Kommission im Juli 2021 angenommen wurde. Zugleich bietet die Initiative ein hohes Maß an Datenschutz für digitale Offline-Euro-Zahlungen, die bargeldähnliche Zahlungen sind. Digitale Online-Euro-Zahlungen unterliegen den gleichen Regeln für Datenschutz, Privatsphäre und Geldwäschebekämpfung wie sie für private digitale Zahlungsmittel gelten. Das befindet sich im Einklang mit dem EU-Rahmen für Geldwäsche und Terrorismusbekämpfung, PSD2, der Datenschutz-Grundverordnung und der Strategie der Kommission für offene Daten.

Vorgesehen ist, dass bei der Offline-Nutzung des digitalen Euro die eigene Bank nur "den gleichen Datenumfang sehen wie bei der Verwendung von Bargeld". „Sie wüsste also, wenn jemand digitale Euros auf ein zugehöriges Konto einzahlt oder abhebt beziehungsweise sie in ein lokales Speichergerät nebst Wallet lädt oder etwas davon abzweigt. Dieses "hohe Maß an Privatsphäre ist dasselbe wie beim Abheben von Banknoten an Geldautomaten", erklärt die Kommission. Was Nutzer konkret kaufen, wohin Zahlungen gehen sowie andere Details zu Transaktionen bleiben der Bank verborgen“¹⁶.

SICHERHEIT DES DIGITALEN EURO

Was die IT-Sicherheit betrifft, fällt der Digitale Euro unter die Bestimmungen des Cyber Resilience Frameworks der EU¹⁷. Dieses Framework umfasst verschiedene Sicherheitsmaßnahmen, um die Widerstandsfähigkeit gegen Cyberangriffe sicherzustellen und die Auswirkungen von Sicherheitsverletzungen zu minimieren.

Die Sicherheit des Digitalen Euros wird nicht durch eine Blockchain gewährleistet, sondern durch die Kontrolle der EZB¹⁸. Der Blockchain Bundesverband ist dagegen der Ansicht, dass ohne die Nutzung der Blockchain-Technologie die Risiken die Chancen

¹⁶ ["Kein Big-Brother-Projekt": EU-Kommission steckt Rahmen für digitalen Euro ab](#)

¹⁷ [VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung \(EU\) 2019/1020](#)

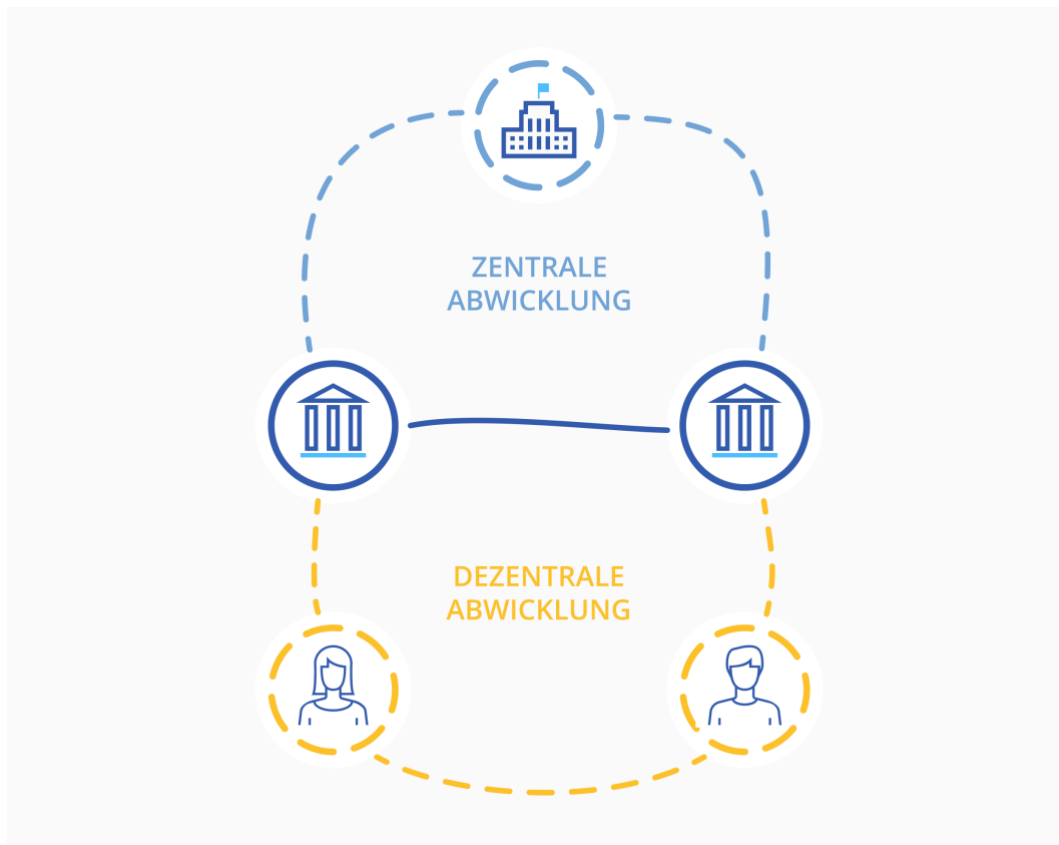
¹⁸ [Der digitale Euro](#)

DIGITALER EURO

des digitalen Euros überwiegen. „Sollte der digitale Euro nicht auf einer dezentralen Infrastruktur wie der Blockchain- oder Distributed Ledger-Technologie aufgebaut werden, so ist dieser abzulehnen“¹⁹.

Laut EZB sollten Endnutzer-Lösungen und alle privaten Systeme, die an der Bereitstellung von Dienstleistungen für einen digitalen Euro beteiligt sind, sicher mit der Backend-Infrastruktur der Zentralbank verbunden sein. Dabei muss ein maximaler Schutz gegen die Gefahr einer unbefugten – d. h. von der Zentralbank nicht autorisierten – Schaffung von digitalen Euro gewährleistet sein²⁰.

Für die Backend-Infrastruktur stehen eine zentrale Abwicklung oder eine dezentrale Abwicklung zur Diskussion.



Der Hauptunterschied zwischen einem direkten Modell und einem indirekten Modell besteht in der Rolle des privaten Sektors. Bei einem direkten Modell sind beaufsichtigte Intermediäre lediglich Gatekeeper, während ihnen in einem indirekten Modell eine bedeutendere Funktion, etwa als Abwicklungsstelle,

¹⁹ [Positionspapier zum digitalen Euro](#)

²⁰ [Bericht über einen digitalen Euro](#)

DIGITALER EURO

zukäme. In beiden Fällen könnte der private Sektor neue Geschäftsaktivitäten entwickeln, die auf Dienstleistungen für den digitalen Euro beruhen (EZB)²¹.

Nach Ansicht des Atlantic Councils würde eine CBDC wie der digitale Euro zwar vielen der gleichen Cybersicherheitsrisiken ausgesetzt sein wie die bestehenden Finanzsysteme, doch würde die Einrichtung eines CBDC auch neue Risiken schaffen.

Je nach der Wahl des CBDC-Designs wären das²²:

- Verstärkte Zentralisierung der Zahlungsverarbeitung und sensibler Nutzerdaten. Es ist möglich, dass eine Zentralbank Benutzeraktivitäten und Transaktionen speichert.
- Geringere aufsichtsrechtliche Kontrolle der Finanzsysteme
- Erhöhte Schwierigkeiten bei der Rückabwicklung betrügerischer oder fehlerhafter Transaktionen
- Herausforderungen bei der Verwaltung von Zahlungsverkehrsdaten und Schlüsselverwahrung
- Anfälligkeit für fehlerhafte oder böswillige Transaktionen, die durch komplexe, automatisierte Finanzanwendungen ermöglicht werden
- Zunehmende Abhängigkeit von Dritten (z. B. Nicht-Banken)

Da jede Währungsvariante unterschiedliche Kompromisse in Bezug auf Leistung, Sicherheit und Datenschutz bietet, sei die Entscheidung, welche Variante der digitalen Währung als CBDC eingesetzt werden soll, eine politische Entscheidung für Finanzministerien, Zentralbanken und Gesetzgeber. Sie sollte auf der Grundlage einer gründlichen Analyse der relativen technischen Kompromisse getroffen werden.

Die Transaktionen sollten für Unbefugte (z. B. Telekommunikationsanbieter) nicht sichtbar sein. Die Vertraulichkeit wird in der Regel durch die Verschlüsselung von Daten erreicht beim Transport über nicht vertrauenswürdige Kanäle. Solche Techniken sind im Bankensektor weit verbreitet. Beim Atlantic Council geht man nicht davon aus, dass sie sich in den verschiedenen CBDC-Varianten wesentlich unterscheiden werden

²¹ [Report on a digital euro](#)

²² [MISSING KEY: The Challenge of Cybersecurity and Central Bank Digital Currency](#)

SCHLUSSBETRACHTUNG

Ob der digitale Euro, wie der Bankenverband schreibt, der nächste evolutionäre Schritt des Geldes ist oder sein wird, lässt sich zum jetzigen Zeitpunkt nicht mit Gewissheit sagen. Ein Blick auf die Geschichte des Geldes der letzten Jahrzehnte zeigt jedoch, dass das Medium Geld immer unstofflicher wird. Bereits Anfang der 1970er Jahre schrieb der Bankhistoriker Volkmar Muthesius:

Demnächst werden wir es vielleicht erleben, dass das Buchgeld in seiner heutigen Form seinerseits gewissermaßen abstirbt und ersetzt wird durch Datenspeicher, durch elektronische Vorgänge in Speichergeräten, womit ein weiteres Stadium der Entstofflichung, also einer speziellen Art von Abstraktion sich vollziehen wird – wer vermöchte zu sagen, ob es das letzte sein wird?²³

Gut möglich, dass der digitale Euro ein weiteres Stadium der Entstofflichung markiert. Die sich zunehmend vernetzende Wirtschaft wird im Idealfall stark profitieren. Sofern es gelingt, die Transaktionskosten, wie beabsichtigt, zu senken, haben auch die Verbraucherinnen und Verbraucher einige Vorteile.

Nicht zu unterschätzen sind dabei die Cybersicherheitsrisiken, die ebenfalls ein neues Stadium kennzeichnen. Die Manipulation eines gesetzlichen Zahlungsmittels im großen Stil ist damit – prinzipiell – möglich – mit unabsehbaren Folgen für die Wirtschaft und Gesellschaft. Im Hintergrund lauert das Schreckensszenario des gläsernen Bürgers, dessen Handlungen an zentraler, staatlicher Stelle lückenlos dokumentiert werden.

Insofern ist es zu begrüßen, dass an dem guten alten Bargeld – erst einmal - nicht gerüttelt wird.

²³ [Bankhistorische Fundstücke – Volkmar Muthesius](#)

Impressum

Kontakt

Ralf Keuper

Kolpingstr. 3

33428 Harsewinkel

E-Mail: ralf.keuper@bankstil.de

Autor: Ralf Keuper

V.i.S.d.P.