Die Technologie der digitalen Zentralbankwährung für Privatkunden

BIZ-Quartalsbericht | März 2020 | 01. März 2020

von Raphael Auer und Rainer Boehme

PDF-Volltext (476kb) | 16 Seiten

Digitale Zentralbankwährungen (CBDCs) versprechen, bargeldähnliche Sicherheit und Komfort für Peer-to-Peer-Zahlungen zu bieten. Um dies zu erreichen, müssen sie belastbar und zugänglich sein. Außerdem sollten sie die Privatsphäre des Benutzers schützen und gleichzeitig eine effektive Strafverfolgung ermöglichen. Verschiedene technische Designs erfüllen diese Attribute in unterschiedlichem Maße, je nachdem, ob sie Intermediäre, eine konventionelle oder verteilte Infrastruktur, einen konto- oder tokenbasierten Zugang und eine grenzüberschreitende Verknüpfung mit dem Einzelhandel aufweisen. Wir erläutern die zugrundeliegenden Kompromisse und die damit verbundene Hierarchie der Designentscheidungen.1

JEL-Klassifikation: E42, E44, E51, E58, G21, G28.

Die Frage, ob Zentralbanken digitale Währungen an die Allgemeinheit ausgeben sollten, hat zunehmend an Aufmerksamkeit gewonnen. Dieser Sonderbeitrag skizziert einige wichtige technologische Designüberlegungen für eine Retail-CBDC, für den Fall, dass eine Zentralbank beschließt, eine solche auszugeben. Wir untersuchen nicht die Argumente für oder gegen die Ausgabe, die systemischen Implikationen oder wie diese gehandhabt werden könnten.2

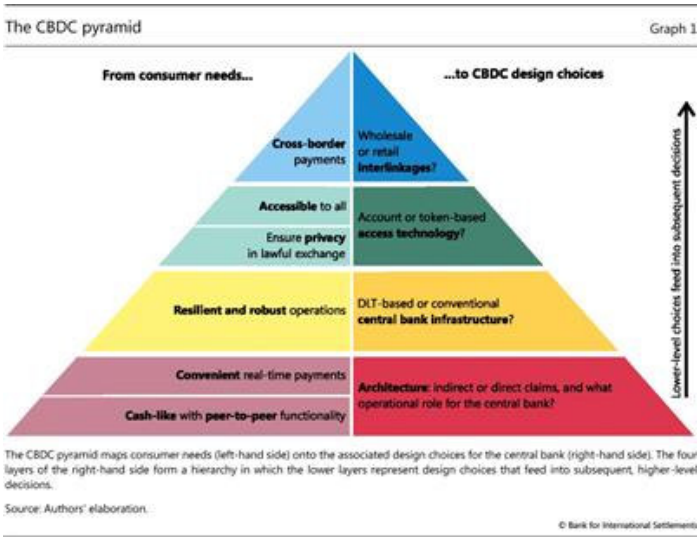
Unser Ansatz orientiert sich an den Bedürfnissen der Verbraucher und den damit verbundenen technischen Designentscheidungen. Derzeitiges elektronisches Geld für den Einzelhandel stellt eine Forderung an einen Intermediär dar, anstatt als digitales Äquivalent von Bargeld zu fungieren. CBDCs könnten potenziell eine bargeldähnliche Sicherheit für Peer-to-Peer-Zahlungen bieten. Gleichzeitig sollten sie im grenzüberschreitenden Zahlungsverkehr Bequemlichkeit, Ausfallsicherheit, Zugänglichkeit, Datenschutz und Benutzerfreundlichkeit bieten. Verschiedene technische Designs erfüllen diese Kriterien in unterschiedlichem Maße, mit den damit

verbundenen technischen Kompromissen. Wir untersuchen diese Themen. Das Ziel ist es nicht, einen bestimmten Ansatz zu fördern oder hervorzuheben, sondern eine Grundlage für systematischere Diskussionen zu schaffen.

Die wichtigsten Erkenntnisse
Ein vertrauenswürdiges und weithin nutzbares CBDC für den Einzelhandel muss sicher und zugänglich sein, bargeldähnlichen Komfort bieten und die Privatsphäre schützen.
Verschiedene technische Designs erfüllen diese Kriterien in unterschiedlichem Maße, und die damit verbundenen Kompromisse müssen identifiziert werden.
Das Design einer Retail-CBDC muss die Glaubwürdigkeit direkter Ansprüche an die Zentralbank mit den Vorteilen der Nutzung von Zahlungsintermediären abwägen.
Unser Ansatz wird grafisch in der "CBDC-Pyramide" dargestellt, die die Bedürfnisse der Verbraucher auf die damit verbundenen Designentscheidungen für die Zentralbank abbildet. Dieses Schema bildet eine Hierarchie, in der die unteren Ebenen Designentscheidungen darstellen, die in nachfolgende, übergeordnete Entscheidungen einfließen.

Wir beginnen mit der Einführung der vier wichtigsten Designentscheidungen, die in den vier Schichten der CBDC-Pyramide dargestellt werden. Wir bewerten die rechtliche Struktur von Forderungen und die operativen Rollen der Zentralbank und privater Institutionen in verschiedenen CBDC-Architekturen. Wir diskutieren die Wahl zwischen Distributed-Ledger-Technologie (DLT) und einer zentral gesteuerten Infrastruktur. Wir vergleichen tokenbasierte Systeme und kontobasierte Systeme. Bevor wir zum Schluss kommen, bewerten wir, wie die Entwicklung von CBDCs die aktuellen Bemühungen zur Überarbeitung des grenzüberschreitenden Zahlungsverkehrs verstärken könnte.

Von Verbraucherbedürfnissen zu Designentscheidungen: die CBDC-Pyramide



Der Fokus unseres Ansatzes liegt auf dem "Retail"-Aspekt von CBDC; wir fragen, welche Verbraucherbedürfnisse ein CBDC adressieren könnte.3 Wir skizzieren daher die Entwicklung eines CBDC durch einen Ansatz, der von den Verbraucherbedürfnissen zu den Designentscheidungen führt.4 Die linke Seite der CBDC-Pyramide (Grafik 1) stellt solche Verbraucherbedürfnisse und sechs damit verbundene Merkmale dar, die ein CBDC nützlich machen würden. Beginnend mit der bargeldähnlichen Peer-to-Peer-Nutzbarkeit, umfassen diese Merkmale auch bequeme Echtzeitzahlungen, Zahlungssicherheit, Datenschutz, breite Zugänglichkeit und einfache Nutzung bei grenzüberschreitenden Zahlungen. Auf der rechten Seite der Pyramide sind die damit verbundenen Design-Entscheidungen dargestellt.

Weitere Lektüre
Drohende Ankunft -
eine Fortsetzung der Umfrage zu digitalen Zentralbankwährungen
Zentralbank-Digitalwährungen
Die Zukunft des Geldes und des Zahlungsverkehrssystems: Welche Rolle für Zentralbanken?
Das Hauptbedürfnis des Verbrauchers ist, dass die CBDC einen bargeldähnlichen Anspruch gegenüber der Zentralbank verkörpert, der idealerweise in Peer-to-Peer-Umgebungen übertragbar ist. Heute sind selbst Verbraucher, die normalerweise lieber elektronisch bezahlen, zuversichtlich, dass sie im Falle einer drohenden Finanzkrise ihre E-Geld-Bestände in Bargeld umschichten könnten. Diese Flucht in Bargeld war in vielen Krisenzeiten zu beobachten,

auch in der jüngsten. Die größte Sorge besteht darin, dass eine schwere Finanzkrise, wenn Bargeld in Zukunft nicht mehr allgemein akzeptiert würde, zu weiteren Verwerfungen führen könnte, indem sie das Tagesgeschäft und die Transaktionen im Einzelhandel beeinträchtigt.5

Gleichzeitig ist es unwahrscheinlich, dass die Verbraucher ein CBDC annehmen, wenn es weniger bequem zu bedienen ist als die heutigen elektronischen Zahlungen. Banken und Zahlungsdienstleister betreiben eine hochentwickelte Infrastruktur, die Nachfragespitzen, wie z.B. am Singles Day in China oder am Black Friday in den USA, bewältigen kann. Und Intermediäre helfen, den Zahlungsfluss zu glätten, indem sie das Risiko übernehmen, zum Beispiel bei Verbindungsunterbrechungen oder Offline-Zahlungen.

Diese beiden Bedürfnisse - bargeldähnliche Sicherheit und Benutzerfreundlichkeit - führen zu der grundlegenden Designüberlegung für ein CBDC (siehe unterste Schicht der Pyramide in Grafik 1): die Wahl der operativen Architektur und wie sie die Nachfrage des Verbrauchers nach einem bargeldähnlichen Anspruch an die Zentralbank mit der Bequemlichkeit, die Intermediäre dem Zahlungssystem verleihen, in Einklang bringt. Die Wahl wird durch zwei Fragen bestimmt. Ist die CBDC ein direkter Anspruch an die Zentralbank oder ist der Anspruch indirekt, über Zahlungsintermediäre? Welche operative Rolle spielen die Zentralbank und die Intermediäre des privaten Sektors im täglichen Zahlungsverkehr?

Darüber hinaus bedeutet das Bedürfnis des Verbrauchers nach bargeldähnlicher Zahlungssicherheit, dass ein CBDC nicht nur vor der Insolvenz oder technischen Pannen von Intermediären, sondern auch vor Ausfällen der Zentralbank sicher sein muss. Die Wahl ist, ob diese Infrastruktur auf einer konventionellen, zentral gesteuerten Datenbank oder stattdessen auf DLT basiert - Technologien, die sich in ihrer Effizienz und dem Grad des Schutzes vor Single Points of Failure unterscheiden. Wichtig ist, dass diese Entscheidung erst getroffen werden kann, wenn die Architektur feststeht, da DLT nur für einige

Betriebskonfigurationen in Frage kommt. Deshalb liegt die Wahl der Infrastruktur in der zweiten Schicht der Pyramide.

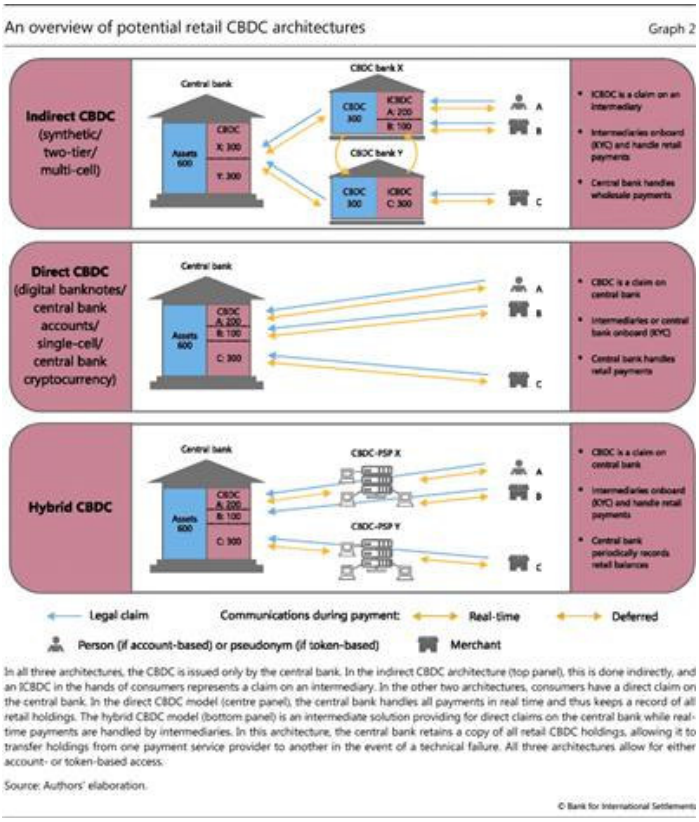
Die CBDC-Pyramide

Zwei weitere Verbraucherbedürfnisse sind der einfache, universelle Zugang und der Schutz der Privatsphäre.6 Aus technischer Sicht gibt es einen grundlegenden Kompromiss zwischen dem Schutz der Privatsphäre und dem einfachen Zugang auf der einen Seite und der einfachen Strafverfolgung auf der anderen. Die damit verbundene Design-Entscheidung - die dritte Ebene der Pyramide - besteht darin, ob der Zugang zum CBDC an ein Identitätssystem gebunden ist (d. h. eine kontobasierte Technologie) oder stattdessen über kryptografische Verfahren erfolgt, die keine Identifizierung erfordern (d. h. eine Zugangstechnologie, die auf sogenannten digitalen Token basiert).

Das letzte Kundenbedürfnis, das wir in Betracht ziehen, ist, dass CBDCs auch grenzüberschreitende Zahlungen ermöglichen sollten. Auf einer Design-Ebene könnte dies über technische Verbindungen auf der Großhandelsebene erfolgen, die auf den heutigen Systemen aufbauen. Alternativ könnten neuartige Anbindungen auf der Retail-Ebene vorgesehen werden, d.h. die Verbraucher könnten ausländische digitale Währungen direkt halten. Wichtig ist, dass die Art und Weise der Umsetzung der letztgenannten Option davon abhängt, ob das CBDC konten- oder tokenbasiert ist. Aus diesem Grund gehört diese Gestaltungsmöglichkeit in die oberste Schicht der Pyramide.

Architektur: indirekte oder direkte Forderungen und die operative Rolle der Zentralbank

Die unterste Schicht der CBDC-Pyramide ist die rechtliche Struktur der Forderungen und die jeweilige operative Rolle der Zentralbank und privater Institutionen im Zahlungsverkehr. Unsere Analyse beginnt mit einem Überblick über mögliche technische Architekturen für ZBDCs. In allen drei Architekturen, die in Grafik 2 dargestellt sind, ist die Zentralbank per Definition die einzige Partei, die CBDCs ausgibt und einlöst. Wir stellen fest, dass alle drei Architekturen entweder konto- oder tokenbasiert sein können und auf verschiedenen Infrastrukturen laufen können. Diese Wahlmöglichkeiten werden weiter unten diskutiert.



Die Hauptunterschiede liegen hier in der Struktur der Rechtsansprüche und der Aufzeichnung durch die Zentralbank. Im "indirekten CBDC"-Modell (Grafik 2, oberes Feld) hat der Verbraucher einen Anspruch gegenüber einem Intermediär, wobei die Zentralbank nur die Großkundenkonten aufzeichnet. Im "direkten CBDC"-Modell (mittleres Feld) stellt die CBDC eine direkte Forderung gegenüber der Zentralbank dar, die alle Guthaben aufzeichnet und bei jeder Transaktion aktualisiert. Das "hybride CBDC"-Modell (unteres Feld) ist eine Zwischenlösung, die direkte Forderungen an die Zentralbank vorsieht und gleichzeitig die Abwicklung von Zahlungen durch Intermediäre ermöglicht.

Betrachten wir zunächst das indirekte CBDC-Modell (oberes Feld). Dieser Begriff wird von Kumhof und Noone (2018) verwendet und entspricht der "synthetischen CBDC" in Adrian und Mancini-Griffoli (2019). Dieses Modell wird wegen seiner Ähnlichkeit mit dem bestehenden zweistufigen Finanzsystem auch als "zweistufiges CBDC" bezeichnet; eine Token-basierte Variante wird als "mehrzelliges CBDC" in Ali (2018) vorgeschlagen. Für Verbraucher stellt diese Art von CBDC keine direkte Forderung an die Zentralbank

dar. Stattdessen wird der Intermediär (in Grafik 2 wegen seiner großen Ähnlichkeit mit einer engen Zahlungsverkehrsbank als "CBDC-Bank" bezeichnet) beauftragt, jede ausstehende indirekte CBDC-ähnliche Verbindlichkeit gegenüber dem Verbraucher (in Grafik 2 als "ICBDC" bezeichnet) durch seinen Bestand an tatsächlichen CBDCs (oder anderem Zentralbankgeld), die bei der Zentralbank hinterlegt sind, vollständig zu besichern.7 Genau wie im heutigen System wickeln die Intermediäre die gesamte Kommunikation mit den Privatkunden ab, wickeln Nettozahlungen ab und senden Zahlungsnachrichten an andere Intermediäre und Großkunden-Zahlungsanweisungen an die Zentralbank. Letztere rechnet die Großkunden-CBDC-Konten endgültig ab.

Ein Überblick über mögliche Retail-CBDC-Architekturen
Das indirekte CBDC bietet nicht nur den Komfort heutiger Systeme, die auf Intermediären basieren, sondern entlastet die Zentralbank auch von der Verantwortung für die Beilegung von Streitigkeiten, Know-Your-Customer (KYC) und ähnlichen Dienstleistungen. Der Nachteil ist jedoch, dass die Zentralbank keine Aufzeichnungen über die einzelnen Forderungen führt (nur die Intermediäre tun dies, während die Zentralbank nur die Großkundenbestände aufzeichnet), noch gibt es einen bargeldähnlichen direkten Nachweis der Forderung. Daher kann die Zentralbank Forderungen von Verbrauchern ohne Informationen des Intermediärs nicht einlösen.8 Wenn der Intermediär unter Druck steht, könnte die Bestimmung des rechtmäßigen Eigentümers ein potenziell langwieriges und kostspieliges Gerichtsverfahren mit ungewissem Ausgang bedeuten. Die regulatorischen und aufsichtsrechtlichen Fragen dieses Modells sowie die Fragen der Einlagensicherung sind daher ähnlich wie beim heutigen System.

Betrachten wir als nächstes ein direkt von der Zentralbank betriebenes CBDC, die direkte CBDC-Architektur (mittleres Feld). Eine Version würde von der Zentralbank verwaltete Konten umfassen. Mehrere Unternehmen des privaten Sektors entwickeln Token-basierte Varianten oder "digitale Banknoten".9 In dieser Architektur könnten KYC und die Sorgfaltspflicht gegenüber dem Kunden vom privaten Sektor oder der Zentralbank oder einer anderen Institution des

öffentlichen Sektors übernommen werden. Die Zentralbank wäre jedoch die einzige Institution, die Zahlungsdienstleistungen abwickelt.

Das direkte CBDC ist aufgrund seiner Einfachheit attraktiv, da es die Abhängigkeit von Intermediären eliminiert, indem es auf diese verzichtet. Dies bringt jedoch Kompromisse in Bezug auf die Zuverlässigkeit, Schnelligkeit und Effizienz des Zahlungssystems mit sich. Ein Aspekt ist, dass der Aufbau und Betrieb technischer Kapazitäten in dieser Größenordnung oft als besser vom privaten Sektor übernommen wird, wie man an den heutigen Kreditkartennetzwerken sieht. Zweitens: Selbst wenn eine Zentralbank die notwendigen technischen Kapazitäten aufbauen würde, könnte die resultierende CBDC für die Verbraucher weniger attraktiv sein als die heutigen Massenzahlungssysteme. Elektronische Zahlungen müssen mit Verbindungsausfällen oder Offline-Zahlungen zurechtkommen, was eine Risikoübernahme durch Intermediäre mit sich bringt. Wichtig ist, dass es die Kundenbeziehung - basierend auf KYC - ist, die es dem Intermediär erlaubt, solche Risiken zu akzeptieren. Solange eine Zentralbank nicht die Verantwortung für KYC und Customer Due Diligence übernimmt - was eine massive Ausweitung des Geschäftsbetriebs, weit über die bestehenden Mandate hinaus, erfordern würde -, wäre es schwierig, diesen Service anzubieten.10

Neben diesen beiden reinen Optionen kann man sich auch neuartige zukünftige Lösungen vorstellen, die Elemente sowohl der indirekten als auch der direkten CBDC vereinen.11 Wir bezeichnen diese dritte Art von Architektur als hybride CBDC (unteres Feld). In diesem Modell wird eine direkte Forderung an die Zentralbank mit einer Nachrichtenschicht des privaten Sektors kombiniert. Auch hier sind sowohl token- als auch kontobasierte Varianten denkbar.

Ein Schlüsselelement der hybriden CBDC-Architektur ist der rechtliche Rahmen, der die Forderungen untermauert, sie von den Bilanzen der Zahlungsdienstleister (PSPs) trennt und die Übertragbarkeit ermöglicht. Wenn ein PSP ausfällt, werden die

Bestände des CBDC nicht als Teil des Vermögens des PSP betrachtet, das den Gläubigern zur Verfügung steht. Der rechtliche Rahmen sollte auch die Portabilität in großen Mengen ermöglichen, d. h. der Zentralbank die Befugnis geben, Privatkundenbeziehungen von einem ausfallenden PSP auf einen voll funktionsfähigen zu übertragen.12
Das zweite Schlüsselelement ist die technische Fähigkeit, die Portabilität von Beständen zu ermöglichen. Da die Anforderung darin besteht, Zahlungen aufrechtzuerhalten, wenn ein Intermediär unter technischem Stress steht, muss die Zentralbank über die technische Fähigkeit verfügen, die Guthaben von Privatkunden wiederherzustellen. Sie behält daher eine Kopie aller Retail-GBDC-Bestände, so dass sie im Falle eines technischen Ausfalls die Retail-GBDC-Bestände von einem PSP auf einen anderen übertragen kann. 13

Das hybride CBDC hätte sowohl Vor- als auch Nachteile gegenüber der indirekten oder direkten CBDC-Architektur. Als Zwischenlösung könnte es eine bessere Ausfallsicherheit bieten als das indirekte CBDC, allerdings um den Preis einer komplexer zu betreibenden Infrastruktur für die Zentralbank. Andererseits ist das hybride CBDC immer noch einfacher zu betreiben als ein direktes CBDC. Da die Zentralbank nicht direkt mit den Privatkunden interagiert, kann sie sich auf eine begrenzte Anzahl von Kernprozessen konzentrieren, während Intermediäre andere Dienste wie die sofortige Zahlungsbestätigung übernehmen.

Konventionelle oder DLT-basierte Zentralbankinfrastruktur?
Welche Infrastruktur könnten die verschiedenen CBDC-Architekturen für die Zentralbank erfordern, und wie könnten sie auf die belastbarste Weise implementiert werden? Diese Entscheidung, die als zweite Stufe der CBDC-Pyramide dargestellt wird, folgt unmittelbar auf die Entscheidung über die Architektur, da sich die Infrastrukturanforderungen für die Zentralbank bei den drei in Grafik 2 dargestellten Architekturen erheblich unterscheiden.

Für die Zentralbank bedeutet das indirekte CBDC eine ähnliche Belastung wie das heutige System. Im Gegensatz dazu würde das direkte CBDC massive technologische Fähigkeiten erfordern, da die

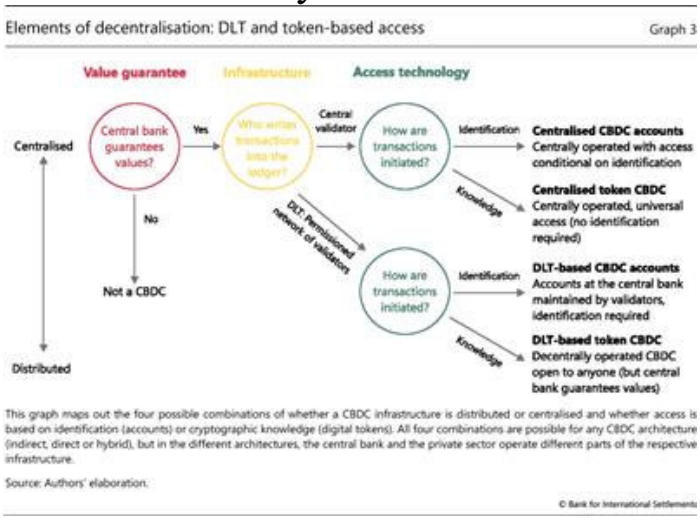
Zentralbank alle Transaktionen selbst abwickelt und dabei ein Volumen an Zahlungsverkehr bewältigt, das mit dem der heutigen Kredit- oder Debitkartenbetreiber vergleichbar ist. Die hybride CBDC-Architektur ist im Betrieb komplexer als das indirekte Modell, da die Zentralbank die Guthaben der Kunden führt. Dennoch könnte sie mit der heutigen Technologie und einer relativ bescheidenen Infrastruktur selbst in den größten Währungsräumen der Welt in großem Umfang umgesetzt werden.14

Die Infrastruktur könnte auf einer konventionellen, zentral gesteuerten Datenbank oder auf einem neuartigen verteilten Ledger basieren. Grafik 3 zeigt, wie Elemente der DLT eine Rolle bei CBDC spielen könnten. Die erste DLT-bezogene Design-Entscheidung hängt davon ab, ob die Autorität zur Aktualisierung der Datenbank zentralisiert oder an ein Netzwerk von identifizierten und überprüften Validatoren delegiert wird.15

Konventionelle und DLT-basierte Infrastrukturen speichern Daten oft mehrfach und an physisch getrennten Orten. Der Hauptunterschied zwischen ihnen liegt darin, wie die Daten aktualisiert werden. In konventionellen Datenbanken wird die Ausfallsicherheit typischerweise durch die Speicherung von Daten über mehrere physische Knoten erreicht, die von einer autoritativen Instanz - dem obersten Knoten einer Hierarchie - kontrolliert werden. Im Gegensatz dazu wird in vielen DLT-basierten Systemen der Ledger von verschiedenen Entitäten gemeinsam dezentral und ohne einen solchen Top-Knoten verwaltet. Folglich muss jede Aktualisierung des Ledgers zwischen den Knoten aller Entitäten abgestimmt werden (oft unter Verwendung von Algorithmen, die als "Konsensmechanismen" bekannt sind). Dies beinhaltet typischerweise das Versenden und Abwarten von Antworten auf mehrere Nachrichten, bevor eine Transaktion endgültig zum Ledger hinzugefügt werden kann.

Der Overhead, der für den Betrieb eines Konsensmechanismus erforderlich ist, ist der Hauptgrund, warum DLTs einen geringeren Transaktionsdurchsatz haben als herkömmliche Architekturen. Konkret bedeuten diese Grenzen, dass aktuelle DLT angesichts des wahrscheinlichen Datendurchsatzes nicht für die direkte ZBK

verwendet werden könnten, außer in sehr kleinen Gerichtsbarkeiten. Allerdings könnte DLT für die indirekte CBDC-Architektur verwendet werden, da die Anzahl der Transaktionen in vielen Großkunden-Zahlungssystemen vergleichbar ist mit der, die von bestehenden Blockchain-Plattformen verarbeitet wird, wie auch in mehreren von Zentralbanken durchgeführten Großkunden-CBDC-Experimenten gezeigt wurde (Bech, Hancock, Rice und Wadsworth (2020, in dieser Ausgabe)). Auch Enterprise-Versionen von DLT könnten für die hybride CBDC-Architektur denkbar sein.



Elemente der Dezentralisierung: DLT und tokenbasierter Zugang

Wenn es darum geht, Ausfallsicherheit zu erreichen, hat weder ein DLT-basiertes noch ein konventionelles System einen eindeutigen Vorteil. Die Schwachstellen sind einfach unterschiedlich. Die Hauptschwachstelle einer konventionellen Architektur ist der Ausfall des obersten Knotens, zum Beispiel durch einen gezielten Hackerangriff. Die Hauptschwachstelle der DLT ist der Konsensmechanismus, der z. B. durch einen Denial-of-Service-Angriff unter Druck gesetzt werden kann.

Insgesamt muss man Kosten und Nutzen des Einsatzes von DLT sorgfältig abwägen. Diese Technologie lagert im Wesentlichen die Befugnis, Forderungen in der Bilanz der Zentralbank zu berichtigen, an externe Validierer aus,16 was nur dann von Vorteil ist, wenn man darauf vertraut, dass dieses Netzwerk zuverlässiger arbeitet als die Zentralbank. Laufende Beurteilungen von DLT-basierten Proofs-of-

Concept sind tendenziell negativ (siehe Kasten für einen kurzen Überblick). Bei den noch laufenden DLT-basierten Projekten bleibt abzuwarten, ob tatsächlich skalierbare Implementierungen auf die Technologie setzen werden.17

Doch selbst wenn man sich gegen die Verwendung von DLT als Backbone-Infrastruktur eines CBDC entscheidet, könnte eine eng verwandte Technologie dennoch nützlich sein. Unabhängig davon, ob die Infrastruktur auf DLT basiert oder nicht, kann der Zugang immer noch auf Kryptographie statt auf Identifikation basieren - Grafik 3 skizziert die möglichen Kombinationen, und der Kasten zeigt, welche Kombinationen von den Zentralbanken untersucht werden.

Token- oder kontobasierter Zugang, und wie wird die Privatsphäre geschützt?
Wenn die Architektur und die Infrastruktur des CBDC gewählt sind, stellt sich die Frage, wie und wem man Zugang gewähren soll. Dies ist die dritte Ebene der CBDC-Pyramide.

Eine erste Möglichkeit ist, dem konventionellen Kontomodell zu folgen und das Eigentum an eine Identität zu binden (Grafik 4, linke Seite). Ansprüche werden in einer Datenbank dargestellt, die den Wert zusammen mit einem Verweis auf die Identität aufzeichnet, genau wie bei einem Bankkonto. Dies hat im Fall von CBDCs Nachteile. Insbesondere hängt es von "starken" Identitäten für alle Kontoinhaber ab - Schemata, die jede Person auf einen und nur einen Identifikator über das gesamte Zahlungssystem abbilden. Solche Schemata können in einigen Rechtsordnungen eine Herausforderung darstellen und damit den universellen Zugang beeinträchtigen.18

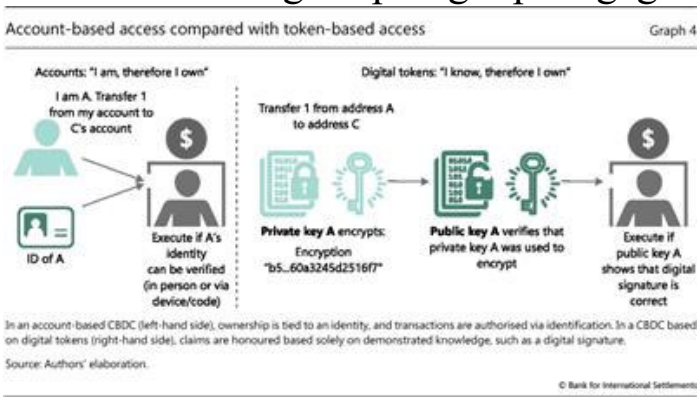
Die zweite Möglichkeit besteht darin, dass die Zentralbank Forderungen nur dann einlöst, wenn der CBDC-Benutzer die Kenntnis eines verschlüsselten Wertes nachweist - eine Option, die manchmal als digitale Token bezeichnet wird (Grafik 4, rechte Seite). Ein Beispiel dafür ist die Verwendung des geheimen Teils eines öffentlich-privaten Schlüsselpaars zum Signieren einer Nachricht, eine Technologie, die von Auer, Böhme und Wadsworth (2020, in dieser Ausgabe) beschrieben wird.

Ein Token-basiertes System würde den universellen Zugang sicherstellen - da jeder eine digitale Signatur erhalten kann - und es würde standardmäßig eine gute Privatsphäre bieten. Es würde dem CBDC auch erlauben, sich mit Kommunikationsprotokollen zu verbinden, d. h. es wäre die Basis für Mikrozahlungen im Internet der Dinge. Aber die Nachteile sind gravierend. Einer davon ist das hohe Risiko, Gelder zu verlieren, wenn die Endnutzer ihren privaten Schlüssel nicht geheim halten. Außerdem würden sich Herausforderungen bei der Gestaltung eines effektiven AML/CFT-Rahmens für ein solches System ergeben. Die Strafverfolgungsbehörden würden auf Schwierigkeiten stoßen, wenn sie versuchen, Anspruchsinhaber zu identifizieren oder Geldströme zu verfolgen, genau wie bei Bargeld oder Inhaberpapieren. Retail-Zentralverwahrer bräuchten daher zusätzliche Schutzmaßnahmen, wenn sie diesen Weg beschreiten würden.19

Wir betonen, dass die Dimension des Datenschutzes weit über die Frage hinausgeht, ob das System auf Konten oder digitalen Token basiert. Finanzdaten auf Transaktionsebene offenbaren sensible persönliche Daten. Daher sind zwei Aspekte des Datenschutzes von entscheidender Bedeutung für das Design eines CBDC. Der erste ist die Menge an persönlichen Informationen, die Transaktionspartner übereinander erfahren, wenn das System normal funktioniert.20 Der zweite ist das Risiko großflächiger Verletzungen der Daten, die sich im Besitz des Systembetreibers oder von Vermittlern befinden.

Entscheidend ist, dass ein CBDC, das es Händlern ermöglicht, Zahlungsdaten zu sammeln und mit Kundenprofilen zu verknüpfen, die eigentliche Natur des Zahlungsverkehrs verändert - von einem einfachen Austausch von Werten zu einem Austausch von Werten gegen ein Bündel von Daten. Daher sollte ein CBDC die Privatsphäre seiner Benutzer gegenüber ihren Transaktionspartnern wahren, d.h. die Transaktionspartner würden standardmäßig über "unsympathische Pseudonyme" interagieren, wie es in Chaums (1985) Pionierarbeit über elektronisches Geld vorgesehen ist. In einem solchen System erhält ein Händler einen Nachweis, dass die Zahlung für eine

bestimmte Rechnung erfolgt ist, aber es werden keine Informationen über den Zahlungsempfänger preisgegeben.



Kontobasierter Zugang im Vergleich zu tokenbasiertem Zugang

Abhängig von der Beteiligung von Intermediären und den Informationen, die sie erhalten, müssen die technischen Schutzmaßnahmen für den Datenschutz durch einen rechtlichen Rahmen ergänzt werden, der die Datenerfassung durch Front-End-Anwendungen, z. B. die Smartphone-Bezahl-App, einschränkt. Datenverlust ist eine weitere Bedrohung, da Zahlungssysteme ein Hauptziel für Cyberangriffe sind. In diesem Zusammenhang ist zu beachten, dass nicht alle Technologien zur Verbesserung der Privatsphäre ausgereift sind. So haben sich beispielsweise einige sogenannte Zero-Knowledge-Proofs bereits als angreifbar erwiesen (Ruffing et al. (2018)). Der einzige todsichere Weg, um nicht viele Daten zu verlieren, ist, sie nicht zu speichern oder alte Transaktionen so schnell wie möglich unwiderruflich zu löschen. Dieses Prinzip der Datenminimierung ist in vielen Datenschutzgesetzen verankert. Wo dies nicht möglich ist, muss auf Aggregation und Anonymisierung zurückgegriffen werden. Ein letzter Ausweg ist die Speicherung an räumlich getrennten (und offline) Orten, die durch gesetzliche Zugriffsverfahren geschützt sind.

Grenzüberschreitende Zahlungen: Wholesale- oder Retail-Verbindungen?
Sobald klar ist, wie ein CBDC konfiguriert ist und wie ansässige Verbraucher darauf zugreifen können, stellt sich die Frage, ob es nur im Inland oder auch anderswo genutzt werden kann. Dies ist die oberste Schicht der CBDC-Pyramide.

Die Nachfrage nach nahtlosen und kostengünstigen grenzüberschreitenden Zahlungen ist parallel zum Wachstum des internationalen E-Commerce, der Überweisungen und des Tourismus gewachsen. Ein CBDC könnte mit den gleichen Optionen für Großkundenverflechtungen ausgestattet sein, die im derzeitigen System erforscht werden (Bech, Faruqui und Shirakami (2020, in dieser Ausgabe)).

Hier ist ein bemerkenswerter Aspekt, dass ein koordiniertes CBDC-Design eine "Clean-Slate"-Perspektive einnehmen und diese Vernetzungsoptionen von Anfang an einbeziehen könnte. Dies wäre eine einzigartige Gelegenheit, grenzüberschreitende Zahlungen zu vereinfachen (z. B. Carney (2019) und Cœuré (2019)) und Ineffizienzen und Mieten durch Verkürzung der Zahlungswertschöpfungskette zu reduzieren.

CBDCs würden auch neuartige Verflechtungen im Einzelhandel ermöglichen, wenn sie es den Verbrauchern erlauben, mehrere Währungen zu halten. Im heutigen kontobasierten System ist eine grenzüberschreitende Transaktion untrennbar mit einer Devisentransaktion verbunden. Der Intermediär, der die Transaktion abwickelt, kann zusätzliche Gebühren und ungünstige Wechselkurse anwenden. Wenn Verbraucher dagegen die Möglichkeit hätten, Devisen im Voraus zu kaufen, bevor sie sie im Ausland ausgeben, so wie sie es mit Bargeld tun können, würde dies die Zahlung von der Devisentransaktion trennen. Dies wiederum würde die Möglichkeit eröffnen, Retail-Wallets direkt mit wettbewerbsfähigen Devisenmärkten zu verbinden.

Wichtig ist, dass der Spielraum für solche Einzelhandelsverknüpfungen und ihre Ausgestaltung von den nationalen Zugangsbedingungen abhängen würde. Wenn ein nationales System auf digitalen Token basiert, wird es standardmäßig für ausländische Einwohner zugänglich sein. Wenn es kontobasiert ist, wäre die Interoperabilität eine Designentscheidung, die auch international koordiniert werden könnte.

Fazit

Da die Zentralbanken eine Schlüsselrolle bei den Zahlungssystemen spielen, könnten sowohl die rückläufige Verwendung von Bargeld als auch die damit verbundenen Entwicklungen im privaten Sektor sie dazu veranlassen, "aufzusteigen" und eine aktivere Rolle zu übernehmen (Carstens (2019 und 2020, in dieser Ausgabe)). Sollten sie dies tun wollen, stehen ihnen viele Wege offen.

In diesem Beitrag haben wir einen hypothetischen Weg beschritten, indem wir die Entscheidungen untersucht haben, die während der Entwurfsphase eines CBDC getroffen werden könnten, und wie der damit verbundene Entscheidungsprozess strukturiert sein könnte. Auf dem Weg dorthin haben wir aufgezeigt, wie sich die Bedürfnisse der Verbraucher in technischen Kompromissen niederschlagen könnten. Aus unserer Analyse ergeben sich einige designbezogene Überlegungen, z. B. hinsichtlich der Machbarkeit von DLT-basierten im Vergleich zu konventionelleren technischen Infrastrukturen, aber andere Entscheidungen bleiben weniger eindeutig.

Mit einem Rahmen für die Entscheidungsfindung im Hinterkopf, könnten mehr praktische Erfahrungen mit spezifischen Design-Entscheidungen hilfreich sein. Der Kasten gibt einen Überblick über die laufenden technischen Gestaltungsbemühungen der Zentralbanken entlang der in diesem Beitrag genannten technischen Dimensionen. Da sich die meisten Projekte noch in einem frühen Stadium befinden, ist die wichtigste Erkenntnis, dass Zentralbanken auf der ganzen Welt eine Vielzahl von Prototypen erforschen, die fast das gesamte Spektrum der in der CBDC-Pyramide dargestellten möglichen Designs abdecken. Wenn die Ergebnisse dieser Experimente international ausgetauscht werden, wird sich ein klareres Bild davon ergeben, welche technologischen Möglichkeiten für CBDCs generell geeignet sind und wie das optimale Design von den spezifischen Umständen der einzelnen Länder abhängen könnte. Dies wiederum könnte dazu beitragen, die Debatte darüber zu führen, ob und wie CBDCs tatsächlich ausgegeben werden sollten.

Eine Bestandsaufnahme: laufende CBDC-Projekte im Einzelhandel

Raphael Auer, Giulio Cornelli und Jon Frost

Von den vielen Zentralbanken, die die Möglichkeit eines Retail-CBDCs untersuchen (Boar et al. (2020)), haben mehrere Forschungsarbeiten oder Stellungnahmen zu den damit verbundenen Beweggründen, Architekturen, Risiken und Vorteilen veröffentlicht. Die folgende Tabelle zeigt 17 ausgewählte Projekte oder Berichte, die vor dem 19. Februar 2020 veröffentlicht wurden. #
Sie deckt weder Großkunden-Zentralverwahrer noch grenzüberschreitende Zahlungsverkehrsprojekte ab, an denen kein Zentralverwahrer beteiligt ist. Wenn es um die vier wichtigsten Gestaltungsmöglichkeiten geht (Grafik 1 im Haupttext), ziehen viele Zentralbanken immer noch mehrere Optionen in Betracht, und es ist nicht immer möglich, sie zu klassifizieren. Hinsichtlich der Architektur (Grafik 2 im Haupttext) konzentrieren sich fünf Projekte auf ein direktes CBDC, zwei auf ein indirektes CBDC, und zehn Projekte untersuchen mehrere Designs oder spezifizieren die Architektur nicht.

Was die Infrastruktur betrifft (Grafik 3 im Haupttext), so konzentriert sich nur ein Projekt auf eine konventionelle Technologie, während fünf auf DLT setzen. Allerdings sind die Erfahrungen mit der letztgenannten Technologie nicht immer ermutigend. Die Sveriges Riksbank (2018) stellt fest, dass die DLT noch immer unter unzureichender Leistung und Skalierbarkeit leidet. Die Nationalbank der Ukraine (2019) kommt zu dem Schluss, dass DLT in einem zentralisierten Ausgabesystem möglicherweise keine grundlegenden Vorteile bietet. Allgemeiner stellt die ECCB (2020) fest, dass DLT keine bargeldähnliche Widerstandsfähigkeit bei längeren Stromausfällen gewährleisten könnte.

Hinsichtlich der Zugangstechnologie (Grafik 4 im Haupttext) sehen drei Projekte einen Zugang auf Basis digitaler Token vor, während drei Projekte den Schwerpunkt auf einen kontobasierten Zugang legen.

Was den Fokus auf grenzüberschreitende Verflechtungen angeht, so hat kein CBDC-Projekt einen expliziten Fokus auf Zahlungen außerhalb des Zuständigkeitsbereichs der Zentralbank.

Bemerkenswert ist, dass mehrere Zentralbanken parallel zu ihren CBDC-Bemühungen an grenzüberschreitenden Zahlungsverkehrsversuchen mit einem Verbraucherfokus arbeiten. Darüber hinaus könnten Großkundeninitiativen wie das Projekt Jasper (Bank of Canada), das Projekt Ubin (Monetary Authority of Singapore), das Projekt Stella (EZB und Bank of Japan) und das Projekt Lion Rock-Inthanon (Hong Kong Monetary Authority und Bank of Thailand) potenziell dazu beitragen, effizientere Massentransaktionen über das Bankensystem zu unterstützen.

Nur sehr wenige Projekte wurden bereits abgeschlossen, wobei die Ergebnisse sehr unterschiedlich ausfallen. Einige wenige Jurisdiktionen, darunter Dänemark und die Schweiz, haben festgestellt, dass derzeit die Kosten eines Retail-CBDC die Vorteile überwiegen würden. Eine größere Anzahl entwickelt weiterhin aktiv Retail-CBDCs; Boar et al. (2020) stellen fest, dass mehr als ein Drittel aller befragten Zentralbanken die Ausgabe einer Retail-CBDC als mittelfristige Möglichkeit ansieht. Mit Blick auf die Zukunft lautet die allgemeine Schlussfolgerung aus technologischer Sicht, dass derzeit eine Vielzahl von technischen Designs in Betracht gezogen wird. Dies unterstreicht die Notwendigkeit einer internationalen Koordination zum Erfahrungsaustausch.

Ausgewählte CBDC-Projekte im Einzelhandel
Ausgewählte Retail-CBDC-Projekte

Selected retail CBDC projects

Table A

Design choices				Project/country	Notes on status, motivation and conclusion
Architecture[1]	Infrastructure[2]	Access[3]	International[4]		
D	U	A	N	Rafkróna Iceland	Research; aims to address "steadily diminishing use of banknotes and coin"; "many issues have yet to be clarified, and they must be dealt with appropriately before a position can be taken".
D	U	A	N	Sand Dollar The Bahamas	Pilot; improve "financial inclusion ..., [reduce] the size of legitimate but unrecorded economic activities, [strengthen] national defences against money laundering and other illicit ends [and]... deliver government services through digital channels, thereby improving tax administration and increasing the efficiency of spending".
D	U	U	N	"E-krona"* Denmark	Research; "the potential benefits of introducing CBDC [are not assessed to] match the considerable challenges that the introduction would present".
D	U	U	N	"E-krona"* Norway	Working group; focus on "independent back-up solution, credit risk-free alternative to bank deposits, competition, legal tender"; "more information is required before a conclusion can be reached".
D	U	U	N	E-krona Sweden	Ongoing work; "within a few years, if the current trend continues, we will find ourselves in a situation where cash is no longer generally accepted as a means of payment"; "an account-based e-krona could rationalise payments from agencies and make them less dependent on commercial agents".
I	D	T	N	Digital Fiat Currency Brazil	Research; "Improve the efficiency of the monetary function, ... payment processes and systems, ... financial inclusion and ... user experience".
I	D	U	I	"E-euro"* ECB	Research; "CBDC with the status of legal tender could guarantee that all users have, in principle, access to a cheap and easy means of payment"; "proof of concept also highlights a number of areas where there is room for improvement".
U	C	A	N	Dinero Electrónico Ecuador	Pilot; "means of payment available to absolutely all Ecuadorians". Operated 2014–16; discontinued.
U	D	T	I	DXCD Eastern Caribbean	Pilot; aims to address the "high cost of current payment instruments and banking services", needs of customers and inefficient cheque settlement.
U	D	U	N	Bakong Cambodia	Pilot; aims to "increase access to quality formal financial services"; "decrease demand for... cash".
U	D	U	N	E-hryvnia Ukraine	Pilot; test DLT "as a technological framework for e-hryvnia issuance and circulation"; no fundamental advantage in using DLT in a centralised model.
U	U	T	N	Electronic legal tender South Africa	Expression of interest; "The scope of this project is specific to the use of a CBDC as electronic legal tender (ELT), similar to the characteristics of, and complementary to, cash."
U	U	U	N	Billete Digital Uruguay	Pilot; "Digital bills that aim to have same functions and uses as physical bills"; ongoing evaluation.
U	U	U	N	DC/EP (Digital Currency/Electronic Payments) China	Ongoing work; aims to create digital alternative to cash and coins for retail use.
U	U	U	N	E-shekel Israel	Research; "help in the struggle against ... unreported transactions"; "contribute to the high-tech sector (fintech)"; Conclusion that "the team does not recommend that the Bank of Israel issue digital currency (e-shekel) in the near future".
U	U	U	U	"E-euro"* France	Research; "account based model would offer better results for a retail CBDC. However, it might also lead to a greater loss of resources for banks".
U	U	U	U	E-franc Switzerland	Research; "Examine the opportunities and risks of introducing a cryptofranc (e-franc)"; "additional benefits currently low and outweighed by risks".

[1] D = direct; I = indirect; U = unspecified or multiple options under consideration. [2] C = conventional; D = DLT; U = unspecified or multiple options under consideration. [3] A = account-based; T = token-based; U = unspecified or multiple options under consideration. [4] I = international; N = National; U = unspecified or multiple options under consideration. * Not an official designation.

Sources: Central bank websites; www.unescap.org; www.efd.admin.ch; www.cf40.org.cn.