

Zur Abwägung zwischen der informationellen Selbstbestimmung und finanziellen Integrität im Bereich eines retail CBDC

ROBERT RAOUL KAHNAU

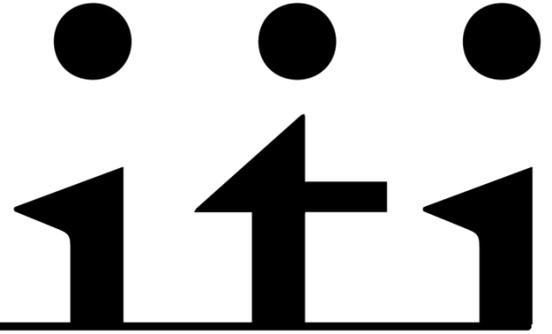
Zitiervorschlag

KAHNAU, Zur Abwägung zwischen der informationellen Selbstbestimmung und finanziellen Integrität im Bereich eines retail CBDC
in: cognitio 2023/2.

URL: cognitio-zeitschrift.ch/2023-2/Kahnau

DOI: [10.5281/zenodo.10083664](https://doi.org/10.5281/zenodo.10083664)

ISSN: 2624-8417



Zur Abwägung zwischen der informationellen Selbstbestimmung und finanziellen Integrität im Bereich eines retail CBDC

ROBERT RAOUL KAHNAU*

Dieser Beitrag befasst sich mit der aktuellen Thematik der Ausgestaltung digitalen Zentralbankgeldes für das Publikum, welches auch als retail Central Bank Digital Currency (rCBDC) bezeichnet wird. Hinsichtlich dieses Beitrags geht es dabei primär um die damit verbundene Abwägung zwischen der verfassungsrechtlich geschützten informationellen Selbstbestimmung und der finanziellen Integrität. Somit wird eine Rechtsfrage erörtert, welche sich an einer Schnittstelle zwischen dem Finanzmarkt- und Währungsrecht und dem genannten Grundrecht, respektive Datenschutzrecht, befindet.

* BLaw, Student Rechtswissenschaften Universität Basel. Der vorliegende Beitrag ist eine gekürzte Fassung der im FS 22 eingereichten Seminararbeit des Autors (kahnaurobert@gmail.com).

Inhaltsübersicht

I. Einleitung	2
II. Taxonomie des Geldes	3
III. Aktuelle Situation im weltweiten Zahlungsverkehr	4
A. Abnahme der Nutzung des Bargeldes als Zahlungsmittel	4
B. Kryptobasierte Zahlungsmittel	5
C. Reaktion der Zentralbanken	5
IV. Rechtliche Grundlagen zur Privatsphäre und zum Datenschutz	6
A. Allgemeines zur informationellen Selbstbestimmung	6
B. Datenschutz im Bereich des digitalen Geldes	7
C. Einschränkungen zur Bekämpfung von Delikten	9
1. Beispiele zur Beschränkung des Bargeldverkehrs	10
2. Beispiele zur Beschränkung des unbaren Zahlungsverkehrs	10
V. Ausgestaltungsmöglichkeiten der Infrastruktur eines rCBDC	11
A. Zentralisierte und dezentralisierte Register	11
B. Token-basierte und Saldo-basierte rCBDC	12

C. Ausgewählte Ansätze	12
1. Modell des SNB Working Paper	12
2. Modell der EZB	13
VI. Interessenabwägung	14
A. Übersicht der vertretenen Ansätze	14
B. Stellungnahme	15
VII. Schlusswort	17

I. Einleitung

Das Geldwesen ist nicht statisch, sondern einem stetigen Wandel unterworfen.¹ Insbesondere wird zur heutigen Zeit davon gesprochen, dass es erneut einen Innovationschub erfahre.² Die Digitalisierung spielt in diesem Zusammenhang eine entscheidende Rolle.³ So treten neue Formen des Geldes in Konkurrenz zu den bisherigen staatlich emittierten, gesetzlichen Zahlungsmitteln.⁴

Mit steigender Nachfrage nach virtuellen Währungen und dem parallel dazu laufenden Trend der Abnahme der Bargeldnutzung, sehen sich zahlreiche Zentralbanken vor der Aufgabe, das von ihnen emittierte Bargeld dem digitalen Zeitgeist anzupassen.⁵ Dabei birgt die Erforschung eines von den Zentralbanken zu emittierenden digitalen Bargeldäquivalent für das Publikum, auch als

retail Central Bank Digital Currency bezeichnet (rCBDC), einige Rechtsfragen.⁶

Der vorliegende Beitrag befasst sich dabei spezifisch mit der Abwägungsfrage zwischen der Gewährleistung der Privatsphäre, i.S. der grundrechtlich geschützten informationellen Selbstbestimmung, und der finanziellen Integrität, i.S. der damit verbundenen Deliktsbekämpfung, hinsichtlich der Emission und Nutzung eines rCBDC.

Zum Verständnis der zu untersuchenden Thematik wird in einem ersten Abschnitt dieses Beitrags eine Taxonomie des Geldes *de lege lata* erstellt, um einen Überblick der derzeitig anerkannten Zahlungsmittel zu erlangen. Darauf folgend wird aufgezeigt, wie die aktuelle Situation im weltweiten Zahlungsverkehr aussieht, sodass nachvollzogen werden kann, weshalb ein digitales Zentralbankgeld für das Publikum (rCBDC) in das Programm der Zentralbanken aufgenommen wurde.⁷ Das Herzstück dieser Arbeit bildet die bereits erwähnte Abwägungsfrage hinsichtlich der Gewährleistung der informationellen Selbstbestimmung und der finanziellen Integrität bei der technischen Ausgestaltung eines rCBDC. Um letztlich anhand zweier vertretenen Ansätze Stellung dazu nehmen zu können, soll der Leser vorweg mit den rechtlichen Grundlagen der informationellen Selbstbestimmung und der technischen Ausgestaltungsmöglichkeiten eines rCBDC vertraut gemacht werden. Dies ist für die Abwägung von Bedeutung, denn je nach Ausgestaltung zeitigen sich unterschiedliche Auswirkungen auf die informationelle Selbstbestimmung und auf die finanzielle Integrität.⁸

¹ KAUFMANN CHRISTINE/UTZ FLORIAN, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), BSK, Bundesverfassung, Basel 2015, N 1-6 zu Art. 99; TRONNIER FRÉDÉRIC, Privacy in Payment in the Age of Central Bank Digital Currency, in: Friedewald Michael/Schiffner Stefan/Krenn Stephan (Hrsg.), *Privacy and Identity Management, IFIP AICT 619*, S. 96 ff., S. 96 1.

² CARSTENS AUGUSTÍN, *Ideen zur Zukunft des Geldes*, in: Frankfurter Allgemeine Zeitung vom 14. Juni 2019, passim.

³ GRÜNEWALD SERAINA N./ZELLWEGE-GUTKNECHT CORINNE/GEVA BENJAMIN, *Digital Euro and ECB Powers*, in: Common Market Law Review 2021/58(4), S. 1029 ff., S. 2.

⁴ Vgl. unten in Kapitel III.B.

⁵ Vgl. unten in Kapitel III passim.

⁶ Vgl. unten in Kapitel IV.

⁷ ZELLWEGE-GUTKNECHT CORINNE/WEBER ROLF H., *Digital Money – Taxonomy and Regulatory Approaches*, in: Zeitschrift für Europarecht 2022/06, S. G1 ff., S. G8.

⁸ AUER RAPHAEL/BÖHME RAINER, *The technology of retail central bank digital currency*, BIS Quarterly Review, 2020, S. 85.

Da der Beitrag aus Schweizer Sicht verfasst wurde, ist vorweg festzuhalten, dass sowohl die Schweizerische Nationalbank (SNB) als auch der Bundesrat, zumindest momentan, keinen Bedarf zur Einführung eines rCBDC sehen.⁹ Trotz dessen untersteht der vorliegende Beitrag der Annahme, dass es in Zukunft zu einer Einführung eines Schweizer rCBDC kommen wird. Indiz dafür bildet die Annahme des Bundesrates, dass sich digitale Bargeldalternativen in den kommenden Jahren vermehren werden, weshalb er in engem Austausch mit den relevanten Akteuren steht.¹⁰

II. Taxonomie des Geldes

Das Bundesgericht (BGer) spricht dann von einem Zahlungsmittel, wenn es von einem völkerrechtlichen Staat als solches herausgegeben wird.¹¹ Aus der Unbestimmtheit dieser vagen Umschreibung lässt sich ableiten, dass sich weder in der Schweizerischen Bundesverfassung noch auf der gesetzlichen Ebene eine Definition des Geldbegriffs vorfinden lässt.¹² Vielmehr kann von einem Medium als Geld gesprochen werden, wenn es drei Funktionen kumulativ erfüllt. Danach fungiert es als eine Recheneinheit, als ein

Tauschmittel und als ein Wertaufbewahrungsmittel.¹³

Jedoch gilt nicht jedes Medium, welches die drei genannten Funktionen erfüllt, als gesetzlich vorgesehene Zahlungsmittel.¹⁴ So sind nach Art. 2 WZG und i.S.v. Art. 84 OR lediglich die vom Bund ausgegebenen Münzen, die von der SNB ausgegebenen Banknoten und die auf Franken lautenden Sichtguthaben bei der SNB darunter zu subsumieren.¹⁵ Die Münzen und Zentralbanknoten werden unter dem Oberbegriff des Bargeldes zusammengefasst und staatlich emittiert.¹⁶ Für dessen Verwendung muss kein Intermediär hinzugezogen werden.¹⁷ Die von den Geschäftsbanken bei der SNB gehaltenen Sichtguthaben stellen eine Form staatlichen Buchgeldes dar. Im Gegensatz zum Bargeld haben sie keine physische äussere Form, sondern existieren auf digitaler Ebene.¹⁸ Von den gesetzlichen Zahlungsmitteln zu trennen, ist das Geschäftsbankenbuchgeld, welches rund 90% der Geldmenge in der Schweiz ausmacht.¹⁹ Diese Buchgelder sind die von Bankkunden bei Geschäftsbanken elektronisch gehaltenen Einlagen, welche ebenfalls auf der Grundlage der staatlichen Währung beruhen, jedoch von privater Hand emittiert werden.²⁰ Sie verkörpern

⁹ Bericht des Bundesrates, [Digitales Zentralbankgeld, Bericht in Erfüllung des Postulats 18.3159](#), Wermuth vom 14.03.2018, S. 40.

¹⁰ Bericht des Bundesrates, [Die Akzeptanz von Bargeld in der Schweiz, Bericht in Erfüllung des Postulats 18.4399](#), Birrer-Heimo vom 14.12.2018, S. 32.

¹¹ BGE 82 IV 198, E. 1; GLESS SABINE/KUGLER PETER/STAGNO DARIO, Was ist Geld? Und warum schützt man es?, in: recht 2015, S. 82 ff., S. 82.

¹² HETTICH PETER, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), SGK zur Schweizerischen Bundesverfassung, Art. 81-197, 3. Aufl., Zürich/St. Gallen/Basel/Genf 2014, N 6 zu Art. 99 BV; ZELLWEGE-GUTKNECHT CORINNE, in: Plenio Martin/Senn Myriam (Hrsg.), Kommentar zum Nationalbankengesetz und Bundesgesetz über die Währung und die Zahlungsmittel, Zürich/St. Gallen 2020, N 3 zu Art. 1 WZG.

¹³ Bericht Digitales Zentralbankgeld (Fn. 9), S. 15.

¹⁴ JORDAN THOMAS J., [Wie Geld durch die Zentralbank und das Bankensystem geschaffen wird](#), Referat vom 16. Januar 2018, S. 4.

¹⁵ ZELLWEGE-GUTKNECHT CORINNE/WEBER ROLF H., [Private Zahlungsmittel und Zahlungssysteme](#), in: Jusletter vom 11. Januar 2021, S. 4.

¹⁶ ZELLWEGE-GUTKNECHT/WEBER (Fn. 7), S. G8.

¹⁷ KLEIN MANUEL/GROSS JONAS/SANDNER PHILIPP, ifo Schnelldienst, Ifo Institute – Leibniz Institute for Economic Research, [Der digitale Blockchain-Euro: Sind Central Bank Digital Currencies die Zukunft?](#), Universität München 2020, S. 40.

¹⁸ Bericht Digitales Zentralbankgeld (Fn. 9), S. 19.

¹⁹ JORDAN (Fn. 14), S. 3; NOBEL PETER, Schweizerisches Finanzmarktrecht, 4. Aufl., Bern 2019, § 4 N 7.

²⁰ JORDAN THOMAS J., [Währungen, Geld und digitale Token](#), Referat vom 5. September 2019, S. 3; Bericht Digitales Zentralbankgeld (Fn. 9), S. 15.

einen Anspruch des Kunden seine Einlagen bei Bedarf in Banknoten und Münzen, also in gesetzliche Zahlungsmittel, umzutauschen.²¹

Die jüngste Form des Geldes bilden die virtuellen Währungen, worunter die Kryptowährungen zu subsumieren sind.²² Sie lauten auf einer eigenen Währungseinheit und werden von Privaten emittiert, ohne der Zuschaltung eines Intermediär.²³ Wie das Geschäftsbankenbuchgeld gehören sie ebenfalls nicht zu den gesetzlichen Zahlungsmitteln.²⁴ Eine bedeutsame Ausprägung der Kryptowährungen bilden die sog. *stable coins*, welche weniger volatil sind. Dies soll dadurch ermöglicht werden, indem sie sich z.B. an Eigenschaften stabileren Geldes binden.²⁵

Geld ist jedoch nicht statisch, sondern einem stetigen Wandel unterworfen.²⁶ Weltweite Digitalisierung spielt dabei eine entscheidende Rolle.²⁷ So spricht AUGUSTÍN CARSTENS, ehemaliger Generaldirektor der Bank für Internationalen Zahlungsausgleich (BIZ), davon, dass das Geldwesen erneut einen Innovationsschub erfahre.²⁸ Was darunter zu verstehen ist, soll anhand des folgenden Kapitels erläutert werden.

III. Aktuelle Situation im weltweiten Zahlungsverkehr

In den folgenden Abschnitten werden zentrale Aspekte des sich ändernden Zahlungsverkehrs aufgezeigt, die den Zusammenhang zur Einführung eines rCBDC darstellen. Zuerst wird aufgezeigt, welchen Stellenwert die Bargeldnutzung aktuell in der Bevölkerung einnimmt. Anschliessend wird die dargestellte Situation mit dem Aufkommen von Kryptowährungen in Verbindung gesetzt, um schliesslich die Reaktion der Zentralbanken als Produkt der geschilderten Situation nachvollziehen zu können.

A. Abnahme der Nutzung des Bargeldes als Zahlungsmittel

Dass das Bargeld als Zahlungsmittel weniger eingesetzt wird, darf nicht als allgemein geltendes Phänomen aufgefasst werden. Gemäss der *Bank of England* sei dies lediglich als Trend aufzufassen.²⁹ So sind bspw. Schweden und Norwegen stärkere Vertreter des unbaren Zahlungsverkehrs, währenddessen in der Schweiz, zumindest momentan, der Barzahlungsverkehr weiterhin bevorzugt wird. Trotzdem lässt sich in der Schweiz der Beginn einer Abnahme der Bargeldnutzung erkennen.³⁰ Ein Indikator dieser unterschiedlichen Bargeldaffinität lässt sich anhand sozio-demographischer Beobachtungen aufzeigen, welche festhalten, dass ältere Bevölkerungsschichten und Haushalte niedrigeren Einkommens die Bargeldnutzung bevorzugen.³¹ Hierbei handelt es sich um den Ein-

²¹ JORDAN (Fn. 14), S. 4.

²² MÜLLER LUKAS/ONG MALIK, Aktuelles zum Recht der Kryptowährungen, in: AJP 2020, S. 198 ff., S. 199 II A; PwC, [Central Bank Digital Currencies and the future of Money](#), 2021, S. 3.

²³ JORDAN (Fn. 20), S. 3; ZELLWEGE-GUTKNECHT/WEBER (Fn. 7), S. G9.

²⁴ MÜLLER/ONG (Fn. 22), S. 206 III B.

²⁵ GRECO SERGIO/KRAMER STEFAN, in: Arpagaus Reto/Stadler Ralph/Werlen Thomas (Hrsg.), *Das Schweizerische Bankgeschäft*, 8. Aufl., Zürich/Basel/Genf 2021, N 2694.

²⁶ KAUFMANN/UTZ (Fn. 1), N 1-6 zu Art. 99; TRONNIER (Fn. 1), S. 96 1.

²⁷ GRÜNEWALD/ZELLWEGE-GUTKNECHT/GEVA (Fn. 3), S. 2.

²⁸ CARSTENS, (Fn. 2), passim.

²⁹ Bank of England, [Central Bank Digital Currency: Opportunities, challenges and design](#), 2020, S. 14.

³⁰ Bericht Die Akzeptanz von Bargeld in der Schweiz (Fn. 10), S. 16 f.; Sveriges Riksbank, [The Riksbank's e-krona project, Report 2](#), 2018, S. 5.

³¹ BORDO MICHAEL D./LEVIN ANDREW T., NBER Working Paper No. 23711, [Central Bank Digital Currency and the Future of Monetary Policy](#), 2017, S. 9; SERFLING OLIVER, [Was denken die Deutschen über die Abschaffung des Bargelds?](#), in: Lempp Jakob/Pitz Thomas/Sickmann Jörn (Hrsg.), *Die Zukunft*

satz des Bargeldes als Zahlungsmittel und nicht um dessen allgemeinen Umlauf in der Bevölkerung.³²

Nebst der umfassenden Abnahme der Bargeldnutzung in Schweden wird zusätzlich erwartet, dass bis zum Jahre 2025 die Hälfte der schwedischen Einzelhändler Bargeld nicht mehr als Zahlungsmittel akzeptieren werden.³³ In England liess sich in der Zeitspanne von 2008 bis 2018 eine Abnahme der Bargeldnutzung von 32% beobachten, wobei in Zukunft eine weitere Abnahme zu erwarten sei.³⁴ Trotz gegenüberstehender Haltung anerkennt die SNB ebenfalls die Möglichkeit einer solchen zukünftigen Erscheinung in der Schweizer Bevölkerung.³⁵ Motive dafür gibt es mehrere, wobei eines unter dem Kapitel IV.C dieses Beitrags aufgezeigt wird.³⁶

B. Kryptobasierte Zahlungsmittel

Mit dem Aufkommen von *Bitcoin* im Jahre 2008 kam es zur Einführung kryptobasierter Zahlungsmittel.³⁷ Dies wurde insbesondere dadurch begünstigt, dass es infolge der parallel dazu zu laufen beginnenden Finanzkrise, zu einem Vertrauensverlust in die staatlich geführte Geldpolitik kam.³⁸ Die Nachfrage nach virtuellen Währungen ist seither gestiegen.³⁹ Verbunden mit dem bereits aufgezeig-

ten Trend der Abnahme der Bargeldnutzung, werden Kryptowährungen als Konkurrenz dazu angesehen.⁴⁰ Diese Thematik wurde trotzdem von den Zentralbanken anfänglich ignoriert. Seit dem Jahre 2019, als *Facebook* die Einführung eines *stable coins* unter der Bezeichnung *Libra* ankündigte, weckte dies in den Zentralbanken jedoch einen Handlungsbedarf.⁴¹

C. Reaktion der Zentralbanken

Der angesprochene Handlungsbedarf betrifft die Einführung eines rCBDC. Darunter ist eine neue Form eines gesetzlichen Zahlungsmittels zu verstehen, welches in digitaler Form neben das bisherige Bargeld treten soll und für die breite Bevölkerung zugänglich ist.⁴² Es kann als solches direkt verwendet werden und stellt nicht lediglich einen Anspruch auf den Erhalt bestehender gesetzlicher Zahlungsmittel dar.⁴³ Jedoch sehen nicht sämtliche Zentralbanken denselben Handlungsbedarf in diesem Bereich. Einige haben einen rCBDC bereits eingeführt, andere befinden sich noch in einem Untersuchungsstadium oder sehen dafür keinen Nutzen.⁴⁴ Eine Studie aus dem Jahre 2020 der BIZ, welche in Kapitel VI.A aufgeführt wird, ermöglicht einen genaueren Einblick in das Verhalten der jeweiligen Zentralbanken.⁴⁵

des Bargeldes – Perspektiven aus Praxis und Wissenschaft, S. 1 ff., S. 6.

³² ZELLWEGE-GUTKNECHT CORINNE/GEVA BENJAMIN/GRÜNEWALD SERAINA N., Osgoode Legal Studies Research Paper, *The ECB and € E-Banknotes*, Kanada 2020, S. 13.

³³ ARVIDSSON NIKLAS/HEDEMAN JONAS/SEGENDORF BJÖRN, Handelsrådet, *Närslutar svenska handlare acceptera kontanter?*, 2018, S. 5, 16.

³⁴ UK Finance, *UK Payment Markets Summary 2019*, Report 2019, S. 3; Bank of England (Fn. 29), S. 14.

³⁵ Bericht Digitales Zentralbankgeld (Fn. 9), S. 25.

³⁶ Vgl. ZELLWEGE-GUTKNECHT/GEVA/GRÜNEWALD (Fn. 32), S. 9-17.

³⁷ PwC (Fn. 22), S. 3.

³⁸ Bericht Digitales Zentralbankgeld (Fn. 9), S. 10.

³⁹ ATAKO NERANDA N., *Privacy Beyond Possession: Solving the Access Conundrum in Digi-*

tal Dollars, in: *Vanderbilt Journal of Entertainment & Technology Law*, 23 (4) Article 3, S. 821ff., S. 822.

⁴⁰ MÜLLER/ONG (Fn. 22), S. 201 II C.

⁴¹ MÜLLER/ONG (Fn. 22), S. 198 I.

⁴² ATAKO (Fn. 39), S. 829; KLEIN/GROSS/SANDNER (Fn. 17), S. 43.

⁴³ KLEIN/GROSS/SANDNER (Fn. 17), S. 43.

⁴⁴ BOAR CORDUTA/WEHRLI ANDREAS, *Ready, steady, go? – Results on the third BIS survey on central bank digital currency*, BIS Papers 2021/114, S. 6.

⁴⁵ BOAR/WEHRLI (Fn. 44), S. 6.

IV. Rechtliche Grundlagen zur Privatsphäre und zum Datenschutz

Die zunehmende Verlagerung des Geldwesens in den digitalen Bereich wirft verfassungsrechtlich gesehen gewisse Fragen auf.⁴⁶ Dies insbesondere in Bezug auf die Ausgestaltung des von den Zentralbanken diskutierten rCBDC. Im Lichte des vorliegenden Beitrags wird von der Prämisse ausgegangen, dass mit einhergehender Abnahme der Bargeldnutzung, rCBDC als digitales Äquivalent dazu fungieren soll. In Diskussion steht u.a. die Einwirkung auf das Grundrecht der informationellen Selbstbestimmung.⁴⁷

A. Allgemeines zur informationellen Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist in [Art. 13 Abs. 2 BV](#) verankert und bildet einen Bestandteil des verfassungsrechtlichen Schutzes der Privatsphäre.⁴⁸ Daraus wird das Recht abgeleitet, dass personenbezogene Daten einen Schutz vor dessen Missbrauch finden sollen. So wird die informationelle Selbstbestimmung auch als Datenschutzgrundrecht bezeichnet.⁴⁹

Entsprechend dem Wortlaut der Bundesverfassung, besteht lediglich ein «Schutz vor Missbrauch [...] persönliche[r] Daten».⁵⁰ In Übereinstimmung von BGer und Lehre erstreckt sich der sachliche Schutzbereich die-

ses Grundrechts jedoch noch weiter.⁵¹ Nebst dem Missbrauch fällt u.a. das Aufbewahren, Erheben, Sammeln, Verarbeiten, Speichern und Weitergeben darunter.⁵² Dadurch soll es dem Einzelnen selbst überlassen werden darüber zu entscheiden, wem der Zugang zu seinen persönlichen Daten gewährt werden soll, um eine freie Persönlichkeitsentfaltung in der Gesellschaft vornehmen zu können.⁵³

Zu den personenbezogenen Daten i.S.v. [Art. 13 Abs. 2 BV](#) und [Art. 5 lit. a DSGVO](#) gehören solche Daten, anhand jener eine lebende Person identifiziert werden kann oder sich auf eine identifizierbare lebende Person beziehen.⁵⁴ Staatliche Eingriffe in den Schutzbereich dieses Grundrechts lassen sich jedoch in der heutigen Welt schlecht vermeiden.⁵⁵ Um diese zu rechtfertigen, müssen sie sich innerhalb der Schranken des [Art. 36 BV](#) befinden.⁵⁶ Danach bedarf es einer gesetzlichen Grundlage, eines öffentlichen Interesses am Eingriff, einer Wahrung der Verhältnismässigkeit des Eingriffs als auch eine Respektierung des Kerngehalts des betroffenen Grundrechts.⁵⁷ Die derzeitigen technischen Entwicklungen stellen jedoch die Gewährleistung der informationellen

⁴⁶ BARTONE ROBERTO, Abschaffung des Bargeldes? Eine Problemskizze, in: Jachmann-Michel Monika/Radke Holger/Voelzke Thomas/Weth Stephan/Winterhoff Christian (Hrsg.), jM 7 2016, S. 285 ff., S. 287 E.

⁴⁷ TRONNIER (Fn. 1), S. 96.

⁴⁸ DIGGELMANN (Fn. 1), N 32 zu Art. 13; MÜLLER JÖRG PAUL/SCHEFER MARKUS, Grundrechte in der Schweiz, Im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakete, 4. Aufl., Bern 2008, S. 164.

⁴⁹ BIAGGINI GIOVANNI, Bundesverfassung der Schweizerischen Eidgenossenschaft, BV Kommentar, 2. Aufl., Zürich 2017, N 11 zu Art. 13 BV.

⁵⁰ [Art. 13 Abs. 2 BV](#).

⁵¹ [BGE 128 II 259](#) E. 3.2; KIENER REGINA/KÄLIN WALTER/WYTTENBACH JUDITH, Grundrechte, 3. Aufl., Bern 2018, § 14 N 57; SCHWEIZER (Fn. 12), N 72 zu Art. 13 BV.

⁵² DIGGELMANN (Fn. 1), N 33 zu Art. 13; KIENER/KÄLIN/WYTTENBACH (Fn. 51), § 14 N 57; MÜLLER/SCHEFER (Fn. 48), S. 167; SCHWEIZER (Fn. 12), N 74 zu Art. 13 BV.

⁵³ DIGGELMANN (Fn. 1) N 32 zu, Art. 13; MÜLLER/SCHEFER (Fn. 48), S. 167; VERNY ARSÈNE, [Indikatives Kurzgutachten zu der verfassungsrechtlichen Problematik einer Einführung von Höchstgrenzen für Bargeldzahlungen in der Bundesrepublik Deutschland](#), Berlin 2016, S. 1.

⁵⁴ BIAGGINI (Fn. 49), N 12 zu Art. 13 BV; SCHWEIZER (Fn. 12), N 75 zu Art. 13 BV.

⁵⁵ KIENER/KÄLIN/WYTTENBACH (Fn. 51), § 14 N 55.

⁵⁶ BIAGGINI (Fn. 49), N 15 zu Art. 13 BV.

⁵⁷ HÄFELIN ULRICH/HALLER WALTER/KELLER HELEN/THURNHERR DANIELA, Schweizerisches Bundesstaatsrecht, 10. Aufl., Zürich/Basel/Genf 2020, § 9 N 302.

Selbstbestimmung vor neue Herausforderungen.⁵⁸

B. Datenschutz im Bereich des digitalen Geldes

Mit der Abnahme des Bargeldverkehrs nimmt parallel die Gewährleistung der Anonymität bei Zahlungsvorgängen ab.⁵⁹ Dies rührt daher, dass es bei Transaktionen digitalen Geldes zur Aufnahme von Daten in elektronischen Registern kommt, sodass es weder kopiert noch wiederverwendet werden kann.⁶⁰ Auf diese Weise entstehen elektronische Spuren, anhand jener Rückschlüsse auf Aktivitäten einer bestimmten Person gezogen werden können.⁶¹ Finanzielle Transaktionsdaten natürlicher Personen beinhalten dabei das Potenzial tiefgründige Einblicke in den Alltag Privater zu erlangen.⁶² So spricht ARSÈNE VERNY bereits davon, dass eine Person sich heutzutage durch ihren Konsum von Waren definieren lasse.⁶³ Daraus lässt sich ableiten, dass anhand einer umfassenden Sammlung von Finanztransaktionsdaten die Möglichkeit besteht detaillierte Persönlichkeitsprofile zu erstellen i.S.v. [Art. 5 lit. f DSGVO](#).⁶⁴ Momentan

ist es einer Person jedoch selbst überlassen, ob sie persönliche Daten innerhalb eines Zahlungsvorgangs preisgeben möchte. Es steht ihr oftmals offen, entweder eine Barzahlung vorzunehmen und damit ihre Privatsphäre zu wahren, oder auf elektronische Bezahlsysteme zurückzugreifen.⁶⁵ Dies ist auch trotz abnehmender Bargeldnutzung möglich, solange es vom Zahlungsempfänger akzeptiert wird. Insbesondere bietet sich dies in der Schweiz an, wo eine sich kaum verändernde Bargeldakzeptanz besteht.⁶⁶

Unter der Annahme, dass digitales Zentralbankgeld für das Publikum jedoch in Zukunft einen digitalen Ersatz des schwindenden Bargeldes darstellen sollte, öffnet sich Raum zur Diskussion. Ein Wechsel des Geldwesens von Bargeld zu rCBDC liesse die Möglichkeit der freien Wahl, rein anonyme Transaktionen zu tätigen, entfallen.⁶⁷ Die Bevölkerung hätte keine andere Option als mittels elektronischer Abwicklung der Zahlungsvorgänge dem Staat Zugang zu ihren persönlichen Daten zu gewähren.⁶⁸

Unter der Auffassung von THILO WEICHERT, dass die Aussage des deutschen Bundesverfassungsgerichts (BVerfG) über Telekommunikationsdaten analog auf jene der Finanztransaktion angewendet werden könne, hielt dieses fest, dass ein Verzicht auf solche Daten im Alltag nicht möglich sei.⁶⁹ Da es somit zu einer massenhaften Speicherung personenbezogener Daten käme, wür-

⁵⁸ DIGGELMANN (Fn. 1), N 32 zu Art. 13; MÜLLER/SCHEFER (Fn. 48), S. 165.

⁵⁹ GARRATT RODNEY J./VAN OORDT MAARTEN R. C., [Privacy as a Public Good: A Case for Electronic Cash](#), in: *Journal of Political Economy* 2021/129(7), S. 2157 ff., S. 2158.

⁶⁰ Deutsche Bundesbank, [Digitales Geld: Optionen für den Zahlungsverkehr](#), 2021, S. 76.

⁶¹ DREHMANN MATHIAS/GOODHART CHARLES/KRUEGER MALTE, [The challenges facing currency usage: will the traditional transaction medium be able to resist competition from new technologies?](#), in: *Economy Policy* 2002/17,(34), S. 193 ff., S. 198; VERNY (Fn. 53), S. 4.

⁶² WEICHERT THILO, [Das Recht auf Anonymität finanzieller Transaktionen, Gutachten, Stellungnahme zu den Vorschlägen der EU – Kommission und des Rats der EU für eine 5. Geldwäsche-Richtlinie](#), 2016, S. 13.

⁶³ VERNY (Fn. 53), S. 4.

⁶⁴ HIRDINA RALPH, [Die gesetzliche Einschränkung von Bargeldzahlungen und die Abschaffung von Bargeld auf dem rechtlichen Prüfstand](#), Working Paper, Weidener Diskussionspapiere 2016/57, S. 13.

⁶⁵ KRUEGER MALTE, [Pros and cons of cash: the state of debate](#), in: Beer Christian/Gnan Ernest/Birchler Urs W. (Hrsg.), *Cash on Trial*, SURF Conference Proceedings 2016/1, S. 45 ff., S. 52.

⁶⁶ Bericht Die Akzeptanz von Bargeld in der Schweiz (Fn. 10), S. 18.

⁶⁷ KAHN CHARLES M./MCANDREWS JAMES/ROBERDS WILLIAM, [Money is Privacy](#), in: *International Economic Review* 2005/46(2), S. 377 ff., S. 377; KRUEGER (Fn. 65), S. 52.

⁶⁸ PAPIER HANS-JÜRGEN, [Gesetzliche Begrenzungen von Bargeldzahlungen – verfassungsrechtlich zulässig?](#), in: 3. Bargeldsymposium der Deutschen Bundesbank 2016, Frankfurt 2016, S. 31 ff., S. 36.

⁶⁹ [BVerfG, Urteil des Ersten Senats vom 02. März 2010](#), N 210; WEICHERT (Fn. 62), S. 13.

de dies den Schutzbereich der informationellen Selbstbestimmung tangieren. Es bedürfte folglich einer Rechtfertigung des staatlichen Eingriffs i.S.v. [Art. 36 BV](#), damit eine Emission eines rCBDC legitim wäre.⁷⁰

Ähnlichen Anlass zur Diskussion ergaben die von zahlreichen Industriestaaten begehrten Beschränkungen des Bargeldes.⁷¹ Denn dadurch sähe sich die jeweilige Bevölkerung zwangsweise dazu verpflichtet, in gewissen Situationen auf elektronische Zahlungsmittel zurückzugreifen, was ebenfalls eine massenhafte Ansammlung personenbezogener Daten darstellen könnte.⁷² Insbesondere der ehemalige Präsident des BVerfG, HANS-JÜRGEN PAPIER, gab seine verfassungsrechtlichen Bedenken in dieser Hinsicht zum Ausdruck.⁷³

Entsprechend vertritt das BVerfG die Meinung, dass eine anlasslose Vorratsdatenspeicherung nicht zulässig sei.⁷⁴ Aus Schweizer Sichtweise wird dieser Auffassung jedoch nicht gefolgt. Das BGer qualifiziert eine Vorratsdatenspeicherung von Randdaten der Telekommunikation als mit der Schweizerischen Bundesverfassung vereinbar. Dabei wird explizit darauf verwiesen, dass es eine zulässige Einschränkung der informationellen Selbstbestimmung darstelle.⁷⁵ Der Schutz der öffentlichen Sicherheit und Gesundheit, als auch die *in casu* relativ zu betrachtende Eingriffsintensität, trügen der Rechtfertigung dieses Eingriffs Genüge.⁷⁶ Anhand der gesammelten Daten liessen sich zwar Persönlichkeitsprofile erstellen, dies aber erst durch deren Verknüpfung, welche die Strafverfolgungsbehörden vornehmen würden. Diese hätten keinen unmittelbaren und uneingeschränkten Zugriff darauf.⁷⁷

Sollte auch hier wieder der bereits erläuterten Auffassung von WEICHERT gefolgt werden, so würde aus Schweizer Sicht ein Wechsel von Bargeld zu einem rCBDC mit dem Grundrecht der informationellen Selbstbestimmung vereinbar sein, trotz dass, wie das BGer einräumt, die Möglichkeit bestünde, Persönlichkeitsprofile zu erstellen.⁷⁸

Hinter dieser Annahme bietet sich Raum zur Diskussion, denn die ergangene Rechtsprechung des BGer ist im Gegensatz zu jener aus dem europäischen Raum eine Seltenheit. So äusserte sich nicht nur das BVerfG, sondern auch der EuGH abweichend der Ansicht des BGer.⁷⁹

Weiter scheint, nach der Auffassung von MICHAEL REINLE und LUKAS BÜHLMANN, eine zentrale Argumentation des BGer fragwürdig. Zur Rechtfertigung eines Grundrechtseingriffs bedarf es, wie bereits festgehalten, eines öffentlichen Interesses. Dieses bestand *in casu* am Schutz der öffentlichen Sicherheit und Gesundheit i.S. der Strafverfolgung. Eine solche sei hingegen nur möglich, wenn die Strafverfolgungsbehörden Zugang zu den umstrittenen Daten hätten. Das BGer betont jedoch explizit, dass eine Trennung vorzunehmen sei zwischen der reinen Speicherung der Daten und deren Verwendung bei den Strafbehörden.⁸⁰ Da es *in casu* lediglich um die Speicherung ging, scheine daher nicht ersichtlich, wie dies mit dem erwähnten öffentlichen Interesse in Verbindung zu setzen sei. Eine Trennung zwischen Speicherung und Verwendung der Daten zu ziehen, sei mit der erfolgten Argumentation des BGer daher nicht verein-

⁷⁰ PAPIER (Fn. 68), S. 37; VERNY (Fn. 53), S. 3.

⁷¹ HIRDINA (Fn. 64), S. 1.

⁷² HIRDINA (Fn. 64), S. 1; VERNY (Fn. 53), S. 4.

⁷³ PAPIER (Fn. 68), S. 40.

⁷⁴ [BVerfG, Urteil des Ersten Senats vom 02. März 2010](#), N 218.

⁷⁵ [BGE 1C_598/2016](#), 2. 3. 2018, E. 8.4.

⁷⁶ [BGE 1C_598/2016](#), 2. 3. 2018, E. 8.4.

⁷⁷ [BGE 1C_598/2016](#), 2. 3. 2018, E. 8.4.

⁷⁸ [BGE 1C_598/2016](#), 2. 3. 2018, E. 5.4.

⁷⁹ [EuGH, Privacy International/Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service](#), Rs. C-623/17, EU:C:2020:790, N 73, 81; SPRECHER FRANZISKA/LIENHARD ANDREAS/TSCHANNEN PIERRE/TSCHENTSCHER AXEL/ZELLER FRANZ, Die staatliche Rechtsprechung des Bundesgerichts in den Jahren 2017 und 2018 (1/2), in: ZBJV 2018/154, S. 641 ff., S. 665 f.

⁸⁰ [BGE 1C_598/2016](#), 2. 3. 2018, E. 5.4.

bar.⁸¹ Dazu wird das Urteil an den EGMR weitergezogen, weshalb die Sache noch nicht endgültig entschieden ist.⁸²

Weiter handelt es sich im erläuterten Entscheidung um Randdaten der Telekommunikation, welche im Gegensatz zu den in dieser Arbeit angesprochenen Finanztransaktionsdaten einen weniger gravierenden Einblick in die Privatsphäre der Nutzer gewähren, da sie lediglich äussere Umstände der Telekommunikation darstellen und den genauen Inhalt des Gesprächs nicht aufzeigen.⁸³ Sollte es sich daher in Zukunft nicht um blosser Randdaten handeln, würde die Rechtsprechung des BGer hinsichtlich der Vorratsdatenspeicherung möglicherweise eine ähnliche Form wie jene aus dem europäischen Rechtsraum annehmen.

Es lässt sich somit festhalten, dass eine Vorratsdatenspeicherung, wie sie ebenfalls bei einem Wechsel von Bargeld zu rCBDC aufkommen würde, einen Eingriff in das Grundrecht der informationellen Selbstbestimmung darstellt, jedoch dessen Rechtfertigung noch unklar ist. Daher stützt sich dieser Beitrag nicht auf die umstrittene Rechtsprechung des BGer zur Vorratsdatenspeicherung. Die erbrachte Argumentation, als auch die gegenteilige Rechtsprechung europäischer Gerichte gibt dem vorliegenden Beitrag den Anlass, die erläuterte Abwägungsfrage unter der Prämisse vorzunehmen, dass eine anlasslose und massenhafte Speicherung personenbezogener Daten einen ungerechtfertigten Eingriff in das Grundrecht der informationellen Selbstbestimmung darstellen würde.

Um dem entgegenzuwirken, können technische Ausgestaltungsmöglichkeiten verwendet werden, welche einen unterschiedlichen

Grad an Wahrung der Anonymität bei Transaktionen digitalen Geldes ermöglichen.⁸⁴ Anhand des aufgezeigten Bundesgerichtsentscheids zur Vorratsdatenspeicherung und der darin erfolgten Argumentation, kann jedoch festgestellt werden, dass die Bekämpfung von Delikten am Finanzplatz hochgewertet wird. Dies insbesondere in der Schweiz.⁸⁵ Daher lassen sich sowohl im Bargeldverkehr als auch im unbaren Zahlungsverkehr der Schweiz verschiedene Einschränkungen vorfinden. Da rCBDC ein digitales Äquivalent zum Bargeld bieten soll, wirft dies die Frage auf, welche dieser Einschränkungen auf einen künftigen rCBDC Anwendung finden sollen. Die Antwort auf diese Frage ist je nach Ausgestaltung des rCBDC unterschiedlich zu beantworten.⁸⁶ Dies wird im Rahmen einer Stellungnahme im Kapitel VI.B aufgezeigt.

C. Einschränkungen zur Bekämpfung von Delikten

Das BGer als auch der Schweizer Gesetzgeber bezeichneten den Finanzplatz als «Achillesferse»⁸⁷ zur Bekämpfung der illegalen Ökonomie.⁸⁸ Wie angedeutet, manifestiert sich dieses Interesse in grossem Umfang in der Schweiz.⁸⁹ Das Verhalten des Gesetzgebers im Bereich der Geldwäscherei stellt dies anschaulich dar.

So wurden die Geldwäschereibestimmungen in das Schweizerische Strafgesetzbuch (StGB) bereits vor der geplanten Gesamtrevision der Wirtschaftsdelikte infolge einer Dringlichkeitsmassnahme aufgenommen.⁹⁰ Acht Jahre später trat ergänzend das Bundesgesetz zur Bekämpfung der Geldwäsche-

⁸¹ REINLE MICHAEL/BÜHLMANN LUKAS, [BGer: Schweizer Vorratsdatenspeicherung ist verfassungsmässig](#), in: MLL-News vom 15. April 2018, passim.

⁸² ALDER KATHRIN, Bundesgericht: Speicherung von Telefondaten ist zulässig, in: NZZ 76 vom 03.04.2018, S. 11.

⁸³ [BGE 1C_598/2016](#), 2. 3. 2018, E. 5.2, 5.3.

⁸⁴ Bank of Canada, [Privacy in CBDC technology](#), 2020, S. 1, 2.

⁸⁵ BEURET (Fn. 25), N 353.

⁸⁶ Vgl. CHAUM DAVID/GROTHOFF CHRISTIAN/MOSER THOMAS, [How to issue a Central Bank Digital Currency](#), SNB Working Papers 2021/3, S. 28.

⁸⁷ [BGE 119 IV 242 E. 1e.](#)

⁸⁸ [BGE 119 IV 242 E. 1e.](#)

⁸⁹ BEURET (Fn. 25), N 353.

⁹⁰ BEURET (Fn. 25), N 361.

rei im Finanzsektor (GwG) in Kraft, das bereits zahlreiche Änderungen und zwei Revisionen erfahren hat.⁹¹ Die Finanzkriminalitätsbekämpfung ist jedoch nicht ein reines Schweizer Anliegen, sondern es bestehen Bestrebungen auf internationaler Ebene. So kam es zur Gründung der *Financial Action Task Force on Money Laundering* (FATF) im Jahre 1989.⁹² Diese erlässt Richtlinien zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung. Heute gehören ihr 39 Mitglieder an, u.a. auch die Schweiz, welche regelmässig auf die Einhaltung der Standards kontrolliert werden.⁹³

1. Beispiele zur Beschränkung des Bargeldverkehrs

Die Verwendung von Bargeld wirft betreffend der Kriminalitätsbekämpfung Diskussionen auf.⁹⁴ So wird argumentiert, dass dessen anonyme Eigenschaft kausal für die Förderung finanzkrimineller Aktivitäten sei.⁹⁵ Diese Meinung steht nicht allein im Raum, denn die Europäische Zentralbank (EZB) beschloss im Jahre 2016 die Abschaffung des 500-Euro-Scheines, u.a. mit der Begründung, dass dadurch die Terrorfinanzierung, Schwarzarbeit und Geldwäsche eingedämmt werden sollten.⁹⁶ Infolge der erst in jüngerer Zeit geschehenen Terroranschläge, wie bspw. die Attentate von Paris im Jahre 2015, kam dem Bargeld mehr Aufmerksamkeit hinzu.⁹⁷ So äusserte auch die Europäische Kommission, im Rahmen eines Aktionsplans zum Vorgehen gegen den Terrorismus, ihre Bedenken hinsichtlich der Bargeldnutzung.⁹⁸ Zahlreiche Staaten, wel-

che der EU angehören, haben bereits Bargeldobergrenzen eingeführt, wie z.B. Frankreich, wo der Grenzwert 1'000.- Euro beträgt.⁹⁹

Auf dem Schweizer Finanzplatz wurde vom Bundesrat ebenfalls eine Bargeldobergrenze vorgeschlagen, welche ein Barzahlungsverbot für Grundstück- und Fahrniskäufe vorsah, sollten diese einen Preis von 100'000.- CHF überschreiten.¹⁰⁰ Dieses Barzahlungsverbot stiess in den parlamentarischen Beratungen jedoch nicht auf Erfolg.¹⁰¹ Es kam lediglich zu einer Revision des GwG im Jahre 2016, welche neu vorsah, dass neben den Finanzintermediären ebenfalls Händlerinnen und Händler den gebotenen Sorgfaltspflichten zur Deliktsbekämpfung im finanziellen Bereich unterstehen, wenn sie im Rahmen einer Zahlung einen Bargeldbetrag von über 100'000.- CHF entgegennehmen.¹⁰²

2. Beispiele zur Beschränkung des unbaren Zahlungsverkehrs

Im Gegensatz zum eher hoch angelegten Schwellenwert im Bargeldverkehr bestehen deutlich schärfere Beschränkungen im unbaren Zahlungsverkehr der Schweiz. So besagt die Geldwäschereiverordnung der FINMA bspw., dass wenn es sich ausschliesslich um eine bargeldlose Bezahlung von Waren und Dienstleistungen im Bereich der Zahlungsmittel für den bargeldlosen Zahlungsverkehr handelt, der zuständige Finanzintermediär zur Einhaltung der gebotenen Sorgfaltspflichten verpflichtet wird, wenn die Zahlung einen Wert von 1'000.- CHF pro Transaktion und 5'000.- CHF pro Kalenderjahr überschreitet.¹⁰³

⁹¹ NOBEL (Fn. 19), § 6 N 12; Für einen detaillierten Einblick siehe <www.fedlex.admin.ch>.

⁹² NOBEL (Fn. 19), § 6 N 79.

⁹³ BEURET (Fn. 25), N 394.

⁹⁴ Bericht Digitales Zentralbankgeld (Fn. 9), S. 33.

⁹⁵ KÖNIG JORG, *Bares bleibt Wahres: Bargeld als Garant für Freiheit und Eigentum*, Research Report, Argumente zu Marktwirtschaft und Politik 2016/136, Berlin, S. 4.

⁹⁶ HIRDINA (Fn. 64), S. 1.

⁹⁷ VERNY (Fn. 53), S. 1.

⁹⁸ Europäische Kommission, *Ein Aktionsplan für ein intensiveres Vorgehen gegen Terrorismusfinanzierung*, Strassburg 2016, S. 11.

⁹⁹ KÖNIG (Fn. 95), S. 5.

¹⁰⁰ SCHOTT ANSGAR/KESSLER MARTINA A., in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), *Handkommentar zum Geldwäschereigesetz (GwG)*, Bern 2017, N 5 zu Art. 8a GwG.

¹⁰¹ SCHOTT/KESSLER (Fn. 100), N 5 zu Art. 8a GwG.

¹⁰² [Art. 8a GwG](#); SCHOTT/KESSLER (Fn. 100), N 6 zu Art. 8a GwG.

¹⁰³ [Art. 11 Abs. 1 lit. a GwV-FINMA](#).

Striktere Begrenzungen bestehen dabei in der Situation, in jener es sich nicht ausschliesslich um eine bargeldlose Bezahlung von Waren und Dienstleistungen im Bereich der Zahlungsmittel für den bargeldlosen Zahlungsverkehr handelt. Hierbei ist der zuständige Finanzintermediär bereits bei einer Schwelle von 200.- CHF verpflichtet, die gebotenen Sorgfaltspflichten einzuhalten, wenn für das betreffende Zahlungsmittel pro Monat ein höherer, als der genannte Betrag verfügbar gemacht werden kann.¹⁰⁴

Wie bereits angedeutet wurde, steht die Antwort auf die Frage, welche Beschränkungen auf einen rCBDC Anwendung finden sollten, in einem engen Zusammenhang mit dessen Ausgestaltungsmöglichkeiten.¹⁰⁵ Wie diese aussehen, wird im folgenden Kapitel aufgezeigt.

V. Ausgestaltungsmöglichkeiten der Infrastruktur eines rCBDC

Digitales Zentralbankgeld kann auf verschiedene Arten ausgestaltet werden. Je nachdem, was die Zentralbank mit der Einführung eines rCBDC erreichen möchte, fällt die Ausgestaltung unterschiedlich aus.¹⁰⁶ Sollte die Bekämpfung von Delikten am Finanzplatz im Vordergrund stehen, könnte mit der Ausgestaltung das Ziel verfolgt werden, möglichst umfassend Finanztransaktionsdaten zu erfassen.¹⁰⁷ Andererseits besteht das Interesse des Nutzers weiterhin darin, möglichst anonym Transaktionen tätigen zu können.¹⁰⁸ Es muss daher zwischen verschiedenen Bedürfnissen abgewogen werden, denn sowohl die Möglichkeit Daten umfassend zurückzuverfolgen als auch einen hohen Grad an Anonymität bei Zahlungsvorgängen zu bieten, können nicht gleichzeitig vollständig gewährleistet werden.¹⁰⁹

¹⁰⁴ Art. 11 Abs. 2 GwV-FINMA.

¹⁰⁵ Vgl. oben in Kapitel IV.B.

¹⁰⁶ Bericht Digitales Zentralbankgeld (Fn. 9), S. 21.

¹⁰⁷ TRONNIER (Fn. 1), S. 99.

¹⁰⁸ AUER/BÖHME (Fn. 8), S. 88.

¹⁰⁹ Bank of England (Fn. 29), S. 22.

A. Zentralisierte und dezentralisierte Register

Die technologische Infrastruktur hinter einem rCBDC kann entweder auf einem zentralen Register oder auf dezentralen Registern beruhen.¹¹⁰ Zentralisierte Register bilden die klassisch verwendete Infrastruktur.¹¹¹ Sie werden von einer Drittpartei geführt, welche eine Dokumentation von Finanztransaktionsdaten auf demselben Register vornimmt.¹¹² Diese Drittpartei wird heutzutage durch die Banken verkörpert.¹¹³

Eine neuere Form der Infrastruktur bilden die dezentral geführten Register.¹¹⁴ Die ihnen zugrunde liegende Technologie wird als *distributed ledger technology* (DLT) bezeichnet.¹¹⁵ Sie werden von privaten Mitgliedern geführt, ohne dass eine Drittpartei Zugang dazu hat.¹¹⁶ Jedes Mitglied unterhält dabei ihr eigenes Register.¹¹⁷ Durch ausgewählte Konsensmechanismen wird dafür gesorgt, dass alle Register auf demselben Dokumentationsstand bleiben.¹¹⁸ Im Bereich dieser Infrastruktur kann man zusätzlich eine Unterscheidung zwischen den sog. *public ledgers* und den *permissioned ledgers* vornehmen, wobei die Möglichkeit eher anonyme Transaktionen zu tätigen, sich in der letzteren Variante widerspiegelt.¹¹⁹

¹¹⁰ AUER/BÖHME (Fn. 8), S. 91.

¹¹¹ ZELLWEGER-GUTKNECHT CORINNE, [Digitale Landeswährung – Ein Überblick](#), in: Jusletter vom 31. Oktober 2016, N 22.

¹¹² REJEB ABDERAHMAN/REJEB KARIM/KEOGH JOHN G., [Centralized vs. decentralized ledgers in the money supply process: a SWOT analysis](#), in: *Quantitative Finance and Economics*, 2021/5 (1), S. 40 ff., S. 44.

¹¹³ ZELLWEGER-GUTKNECHT (Fn. 111), N 23.

¹¹⁴ ZELLWEGER-GUTKNECHT (Fn. 111), N 24.

¹¹⁵ ZELLWEGER-GUTKNECHT (Fn. 111), N 24; Bank of England (Fn. 29), S. 42.

¹¹⁶ REJEB/REJEB/KEOGH (Fn. 112), S. 45.

¹¹⁷ REJEB/REJEB/KEOGH (Fn. 112), S. 45.

¹¹⁸ Deutsche Bundesbank, [Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potenziale und Risiken](#), 2017, S. 37.

¹¹⁹ REJEB/REJEB/KEOGH (Fn. 112), S. 45; Deutsche Bundesbank (2017) (Fn. 118), S. 42.

Bei der Errichtung der technologischen Infrastruktur eines zentralen oder dezentralen Registers lassen sich unterschiedliche Techniken miteinbeziehen, die es ermöglichen, die zu beachtende Privatsphäre der Nutzer zu gewährleisten.¹²⁰ In Anbetracht einer rCBDC Einführung birgt die Verwendung dezentralisierter Register jedoch das Risiko eines Kontrollverlustes der Zentralbank. Die Steuerung der Finanztransaktionen würde in den Machtbereich der Entwickler der DLT fallen.¹²¹

B. Token-basierte und Saldo-basierte rCBDC

Es ist umstritten, ob die Unterscheidung zwischen einem Token-basierten und einem Saldo-basierten rCBDC möglich ist.¹²² Um nicht zu tief in diese Materie zu greifen, werden unter diesem Kapitel trotz der bestehenden Meinungsverschiedenheiten beide Ausgestaltungen kurz vorgestellt, um aufzuzeigen, welchen Einfluss auf die Privatsphäre, respektive auf die finanzielle Integrität diese Distinktion birgt.

Bei einer Transaktion eines Saldo-basierten rCBDC wird der Kontostand des Zahlenden belastet, während jener des Zahlungsempfängers entsprechend begünstigt wird.¹²³ Dies beinhaltet die Notwendigkeit einer Identifikation der Inhaber der zu aktualisierenden Konti zur Wahrung ihrer Identität.¹²⁴ Im Gegensatz zu Barzahlungen bedarf es hierbei der Zuschaltung eines Intermediär.¹²⁵ Dadurch wird es z.B. der Zentralbank ermöglicht, Transaktionen zu verfolgen und die entsprechenden Sorgfaltspflichten einzu-

halten, um der Finanzkriminalität entgegenzuwirken.¹²⁶

Bei einem Token-basierten rCBDC werden hingegen verschlüsselte Geldwerte in Form eines Tokens transferiert.¹²⁷ Im Gegensatz zum Saldo-basierten rCBDC müssen die Parteien ihre Identität nicht preisgeben, denn die Transaktion muss nicht protokolliert werden, da es ausreichend ist, im Besitz des Tokens zu sein.¹²⁸ Diesen erlangt man, indem digitale Signaturen mit Hilfe von Kryptographie entschlüsselt und auf ihre Echtheit hin überprüft werden, sodass eine Transaktion erfolgen kann.¹²⁹ Daraus kann abgeleitet werden, dass z.B. die Zentralbank nicht an Transaktionen beteiligt ist, ähnlich wie bei Bargeldtransaktionen.¹³⁰ Somit kann die Privatsphäre des Nutzers gewahrt werden, jedoch zu Lasten der Einhaltung der Vorschriften zur Deliktsbekämpfung.¹³¹

C. Ausgewählte Ansätze

In den folgenden Abschnitten werden zwei ausgewählte Modelle eines möglichen rCBDC zusammenfassend erläutert, sodass im anschließenden Kapitel eine Stellungnahme dazu vorgenommen werden kann, basierend auf dem bisher erlangten Wissen rundum der zentralen Fragestellung dieses Beitrags.

1. Modell des SNB Working Paper

Das Modell des SNB Working Paper vertritt den Ansatz, dass ein gleichgewichtiges Zusammenspiel zwischen anonymen Transaktionen und der Einhaltung von Richtlinien zur Deliktsbekämpfung, anhand der Verwendung eines Token-basierten rCBDC, welcher nicht auf einer dezentralen Infrastruktur aufbaut, gewährt werden kann.¹³²

¹²⁰ Bank of Canada (Fn. 84), S. 4.

¹²¹ REJEB/REJEB/KEOGH (Fn. 112), S. 54.

¹²² GROTHOFF CHRISTIAN/MOSER THOMAS, [How to issue a privacy-preserving central bank digital currency](#), in: SUERF Policy Briefs 2021/114, S. 2.

¹²³ BORDO/LEVIN (Fn. 31), S. 6.

¹²⁴ ATAKO (Fn. 39), S. 831.

¹²⁵ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 11.

¹²⁶ BORDO/LEVIN (Fn. 31), S. 6.

¹²⁷ GROTHOFF/MOSER (Fn. 122), S. 2.

¹²⁸ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 8.

¹²⁹ PwC (Fn. 22), S. 4.

¹³⁰ AUER/BÖHME (Fn. 8), S. 94.

¹³¹ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 11.

¹³² CHAUM/GROTHOFF/MOSER (Fn. 86), S. 1.

Die vorgeschlagene Software lautet auf dem sog. GNU Taler, welche mit einer *Free/Libre and Open Source Software* (FLOSS) in Verbindung zu setzen ist. Dies erlaubt es u.a. den Nutzern, die Software laufend anzupassen, sodass auf aktuelle Bedürfnisse eingegangen werden kann.

Diese Flexibilität sei vor allem im Bereich eines rCBDC nützlich, aufgrund der umfassenden Anzahl an Beteiligten.¹³³ Der Zentralbank wird es damit ermöglicht, die Software so auszugestalten, dass sie die nötige Transparenz bietet, welche es zur Bekämpfung von Delikten bedarf.¹³⁴ Sie beruht auf Kryptographie und verwendet blinde Signaturen zur Gewährleistung der Privatsphäre der Nutzer.¹³⁵

Sollte ein Nutzer es wünschen eine Transaktion von rCBDC-Token vorzunehmen, muss er diese zuerst von der Zentralbank beziehen, da nur sie zuständig für die Herstellung ist. Die zugehörige Geschäftsbank identifiziert innerhalb dieses Vorgangs den entsprechenden Nutzer.¹³⁶ Damit der zukünftige Zahlungsempfänger später von der Echtheit des rCBDC ausgehen kann, bringt die Zentralbank vor der Emission eine digitale Signatur auf dem Token an.¹³⁷ Dies erfolgt jedoch blind, was bedeutet, dass eine spezifische Nummer, welche den Token repräsentiert, verborgen bleibt.¹³⁸ Bei der anschließenden Verwendung des Tokens sind lediglich die Geschäftsbanken der Parteien beteiligt.¹³⁹

Als bald der Zahlungsempfänger den Token erhält, wird er von seiner Geschäftsbank ebenfalls identifiziert.¹⁴⁰ Danach wird der Token hinterlegt, sodass die Zentralbank anhand einer von ihr geführten Liste überprüfen kann, ob dieser nicht bereits verwen-

det worden ist. Hierbei kann jedoch keine Verbindung zum Zahlenden hergestellt werden, weil die Nummer, welche den Token repräsentiert, beim Bezug verborgen wurde.¹⁴¹ Da die beteiligten Parteien bei Bezug und Empfang der rCBDC-Token identifiziert werden, ermöglicht dies eine Einhaltung der Richtlinien zur Deliktsbekämpfung über die Geschäftsbanken.

Gleichzeitig bedarf es keiner Identifikation des Zahlenden bei der Nutzung seiner rCBDC-Token, insbesondere wenn man dies in Verbindung mit der verwendeten Methodik der blinden Signaturen setzt, kann seine Privatsphäre zu einem gewissen Grad gewahrt werden.¹⁴²

2. Modell der EZB

Dieses Modell beruht auf dem Konzept, welches das *European System of Central Bank's* (ESCB) *EUROchain* Forschungsnetzwerk erarbeitete.¹⁴³ Im Vordergrund stand dabei die Gewährleistung der Anonymität im Bereich des digitalen Zentralbankgeldes bei gleichzeitiger Einhaltung der Richtlinien zur Bekämpfung der Geldwäscherei und des Terrorismus.¹⁴⁴ Dem Konzept liegen vier Prinzipien zugrunde, welche beinhalten, dass das digitale Zentralbankgeld möglichst nahe an den Eigenschaften des Bargeldes festhalten sollte, dass es zur Nutzung von Intermediären kommt, dass nur die Zentralbank rCBDC ausgeben oder aus dem Umlauf nehmen darf und dass eine *Anti-money-laundering* (AML)-Autorität einbezogen wird, welche die Transaktionen auf ihre Vereinbarkeit mit den einzuhaltenden Richtlinien hin überprüft. Die AML-Autorität stellt somit eine Behörde dar, welche eine Compliance-Funktion im Transaktionsprozess ein-

¹³³ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 12.

¹³⁴ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 13.

¹³⁵ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 15.

¹³⁶ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 13.

¹³⁷ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 14.

¹³⁸ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 13.

¹³⁹ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 13.

¹⁴⁰ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 13.

¹⁴¹ CHAUM/GROTHOFF/MOSER (Fn. 86), S. 14.

¹⁴² CHAUM/GROTHOFF/MOSER (Fn. 86), S. 13, 14.

¹⁴³ ESCB's EUROchain Research network, [Exploring anonymity in central bank digital currencies](#), IN FOCUS 2019/4, S. 3.

¹⁴⁴ ESCB's EUROchain Research network (Fn. 143), S. 1.

nimmt, sodass rCBDC nicht an gesperrte Nutzer gelangt.¹⁴⁵

Die zugrunde liegende Infrastruktur basiert auf einer *distributed ledger technology* (DLT) namens Corda.¹⁴⁶ Eine weitere Eigenschaft des Modells besteht darin, dass den Nutzern anonyme Transaktionen durch die Verwendung von sog. *anonymity vouchers* ermöglicht werden, welche von der angesprochenen AML-Autorität in regelmässigen Zeitabständen emittiert werden. Jeder Nutzer erhält eine gewisse Anzahl an *anonymity vouchers*, welche er bei einer Transaktion von rCBDC verwenden kann, sodass die AML-Autorität keinen Einblick in die Transaktionsdaten erhält. Die Nutzer können sie nicht unter sich verteilen, dazu kann lediglich ein *voucher* pro rCBDC-Einheit verwendet werden. Wenn diese aufgebraucht sind, entfällt die Möglichkeit, anonyme Transaktionen zu tätigen.¹⁴⁷

Eine Transaktion zeichnet sich zwischen dem Zusammenspiel der jeweiligen Intermediären, der Nutzer und der AML-Autorität aus, wobei die Zentralbank nicht in diesem Prozess involviert ist. Der Zahlende gibt seinem zuständigen Intermediär den Auftrag, den gewünschten Betrag an rCBDC-Einheiten dem Zahlungsempfänger über dessen Intermediär weiterzuleiten. Dabei gibt er auch an, ob die Transaktion anonym vollzogen werden soll oder nicht.¹⁴⁸

Sollte der Zahlende eine anonyme Transaktion wünschen, so überprüft dessen Intermediär, ob ihm ausreichende *anonymity vouchers* zur Verfügung stehen. Wenn dies der Fall ist, wird dem Zahlenden die entsprechende Anzahl an *vouchers* abgezogen und seiner Transaktion angehängt, sodass der Intermediär des Zahlungsempfängers Si-

cherheit darüber erlangt, dass die AML-Autorität nicht eingeschaltet werden muss.¹⁴⁹

Sollten hingegen nicht genügend *vouchers* vorhanden sein oder wünscht der Zahlende keinen Vollzug einer anonymen Transaktion, so wird diese über den Intermediär des Zahlenden zur AML-Autorität weitergeleitet, welche eine entsprechende Prüfung vornimmt. Im Falle einer Bewilligung der Transaktion, steht es anschliessend dem Intermediär des Zahlungsempfängers offen diese zu akzeptieren, sollte weder ein Limit an verfügbaren rCBDC Transaktionen noch die vorgesehen erlaubte Menge an rCBDC, welche der Zahlungsempfänger besitzen darf, überschritten sein.¹⁵⁰

VI. Interessenabwägung

In den folgenden Abschnitten wird zuerst dargestellt, welche Absichten die Autoren der beiden Modelle verfolgen. Anschliessend wird anhand einer Studie der BIZ aufgezeigt, wie die rCBDC Thematik in den weltweiten Zentralbanken vermehrt auf Beachtung stösst. Schliesslich folgt eine persönliche Stellungnahme des Autors zu den beiden erläuterten Modellen.

A. Übersicht der vertretenen Ansätze

Vorweg gilt es festzuhalten, dass die EZB mit dem erarbeiteten Modell keine weiteren Absichten verfolgt. Es eigne sich nicht für eine tatsächliche Umsetzung, sondern trüge lediglich zur aktuellen Diskussion der Zentralbanken bei, welche sich mit einem rCBDC beschäftigen.¹⁵¹ Ähnliches gilt für das Modell des SNB Working Paper.

Im Gegensatz zur EZB wird jedoch zusätzlich die Ansicht vertreten, dass das erarbeite-

¹⁴⁵ ESCB's EUROchain Research network (Fn. 143), S. 4.

¹⁴⁶ ESCB's EUROchain Research network (Fn. 143), S. 4.

¹⁴⁷ ESCB's EUROchain Research network (Fn. 143), S. 6.

¹⁴⁸ ESCB's EUROchain Research network (Fn. 143), S. 7.

¹⁴⁹ ESCB's EUROchain Research network (Fn. 143), S. 7.

¹⁵⁰ ESCB's EUROchain Research network (Fn. 143), S. 8.

¹⁵¹ ESCB's EUROchain Research network (Fn. 143), S. 1.

te Modell den interessierten Zentralbanken als Vorlage dienen könne, sollte eine tatsächliche Einführung beabsichtigt werden.¹⁵²

Daraus kann implizit abgeleitet werden, dass die Autoren das vorgestellte Modell für eine praktische Umsetzung als geeignet ansehen.

Dass verschiedene Zentralbanken sich mit der Einführung eines rCBDC befassen, kann anhand der im Kapitel III.C erwähnten Studie der BIZ aus dem Jahre 2020 aufgezeigt werden. Sie trägt die Antworten von 65 Zentralbanken zusammen, welche zu verschiedenen Aspekten im Bereich der CBDC-Thematik befragt wurden.¹⁵³ Die Studie ergab, dass 86% der Beteiligten sich in einer gewissen Weise mit der Thematik auseinandersetzten, wobei dem Bereich des rCBDC seit dem Jahre 2018 bis 2020 zunehmende Beachtung zukam.¹⁵⁴ Diese widerspiegelt sich stärker in der Erstellung von Modellen als in der Entwicklung von Pilotprojekten zur Erforschung der praktischen Tauglichkeit eines rCBDC.¹⁵⁵

Einige Beispiele bilden dabei das *e-krona*-Projekt der *Sveriges Riksbank*, der digitale *yuan* der *People's Bank of China*, auch als *Digital Currency Electronic Payment* (DCEP) bezeichnet, und der *Sand Dollar*, welcher von der *Central Bank of the Bahamas* etabliert wurde.¹⁵⁶ Im Gegensatz zu diesen und zahlreichen weiteren Beispielen, haben die aufgezeigten Modelle der EZB und des SNB Working Paper gemeinsam, dass sie sich intensiv mit der Gewährleistung der Privatsphäre für die potenziellen Nutzer befassen. Lediglich die *Bank of Canada* teilt denselben Ansatz, ansonsten wird dieser eher vernachlässigt.¹⁵⁷

B. Persönliche Stellungnahme des Autors

Die Arbeiten im Bereich eines rCBDC verschiedener Zentralbanken sind auf die beiden festgestellten Erscheinungen der Abnahme der Bargeldnutzung in weiten Teilen der Bevölkerung und der zunehmenden Involvement des privaten Sektors im Geldwesen durch die Einführung verschiedener Kryptowährungen zurückzuführen.¹⁵⁸ Damit ein rCBDC als neue Ausprägung einer umlaufenden Währung dem entgegenwirken kann, soll er sich u.a. möglichst nahe an der einzigartigen Eigenschaft des Bargeldes binden, welches vollständig anonyme Transaktionen ermöglicht.

Dass dies jedoch nicht im ausschliesslichen Interesse der Zentralbanken liegt, konnte anhand der Bestrebungen im Bereich der Bekämpfung von Delikten auf dem Finanzplatz erkannt werden.¹⁵⁹ Dieser Fakt widerspiegelt sich noch anschaulicher in der erwähnten Feststellung, dass die meisten Zentralbanken in ihren Modellen und Pilotprojekten eines rCBDC die Gewährleistung der Privatsphäre der Nutzer nicht explizit beachten.¹⁶⁰

Die Stellungnahme bezieht sich auf die Frage, wie die Abwägung zwischen der begehrten Privatsphäre und dem Interesse an der Rückverfolgung von Finanztransaktionsdaten i.S. der Bekämpfung der Finanzkriminalität vorzunehmen ist, sodass sowohl die Bedürfnisse der Nutzer als auch jene der Emittenten bestmöglich befriedigt werden können. Als Vorlage dienen die beiden behandelten Modelle der EZB und des SNB Working Paper.

Die Lösung der Abwägungsfrage im Modell der EZB stützt sich auf *anonymity vouchers*, welche die Nutzer zugute haben, um Transaktionen möglichst anonym vornehmen zu können. Die zugrunde liegende technische

¹⁵² CHAUM/GROTHOFF/MOSER (Fn. 86), S. 1.

¹⁵³ BOAR/WEHRLI (Fn. 44), S. 4, 5.

¹⁵⁴ BOAR/WEHRLI (Fn. 44), S. 6.

¹⁵⁵ BOAR/WEHRLI (Fn. 44), S. 6.

¹⁵⁶ ATAKO (Fn. 39), S. 824.

¹⁵⁷ TRONNIER (Fn. 1), S. 97.

¹⁵⁸ Vgl. oben in Kapitel III.

¹⁵⁹ Vgl. oben in Kapitel IV.C.

¹⁶⁰ Vgl. oben in Kapitel VI.A.

Infrastruktur basiert auf einer DLT, auf welche jedoch nicht näher eingegangen wird.¹⁶¹ Die Gewährleistung der Anonymität bei Zahlungsabwicklungen wird somit nicht anhand der verschiedenen technischen Ausgestaltungsmöglichkeiten auf der infrastrukturellen Ebene wahrgenommen, sondern unabhängig davon über die *anonymity vouchers* gewährleistet.¹⁶²

Meines Erachtens scheint es daher unklar, weshalb eine DLT verwendet wurde. Dies birgt das Risiko eines Kontrollverlustes der Zentralbank, ohne ersichtlichen Nutzen der verwendeten Infrastruktur.¹⁶³ Einen Rückgriff auf zentrale Register würde dieses Risiko beseitigen.¹⁶⁴

Die Gewährleistung der Privatsphäre durch die Verwendung von *anonymity vouchers* ist ein interessanter Ansatz. Zwar ermöglicht dies nicht unbeschränkt anonyme Transaktionen zu tätigen, jedoch besteht die Möglichkeit des Nutzers frei zu wählen, wann er sie einsetzen möchte. Es wird daher den Interessen des Nutzers als auch jenen des Emittenten Rechnung getragen. Eine ähnliche Situation widerspiegelt sich im derzeitigen Zahlungsverkehr, indem der Zahlende frei entscheiden kann, ob er anonyme Zahlungen anhand der Nutzung von Bargeld tätigen möchte oder auf elektronische Bezahlsysteme zurückgreift.¹⁶⁵

Gleichzeitig erübrigt sich meiner Ansicht nach, die Klärung der Frage, welche der bestehenden Beschränkungen im baren und unbaren Zahlungsverkehr auf einen rCBDC anzuwenden sind. Die lediglich beschränkte Anzahl an *anonymity vouchers* legt implizit einen Schwellenwert fest.¹⁶⁶ Die zusätzliche Beachtung von Sorgfaltspflichten im bereits

beschränkten Anwendungsbereich würde das Konzept vereiteln.

Der Grad an gewährter Anonymität scheint meines Erachtens jedoch etwas fragwürdig. Um einen rCBDC anonym verwenden zu können, muss der Nutzer sich zuerst mit seinem Intermediär in Kontakt setzen, damit dieser überprüfen kann, ob genügend *anonymity vouchers* vorhanden sind. Während die AML-Autorität folglich am Transaktionsmechanismus bei ausreichend vorhandenen *vouchers* nicht beteiligt ist, sind es hingegen die Intermediäre der Parteien, aufgrund der zu verfolgenden Anweisungen ihrer Kunden.¹⁶⁷ Dass, wie eines der vier Grundprinzipien dieses Modells festhält, dieser rCBDC sich möglichst an den Eigenschaften des Bargeldes orientieren sollte, wird daher meiner Ansicht nach nicht eingehalten.

Die Lösung der Abwägungsfrage im Modell des SNB Working Paper baut hingegen nicht auf einer dezentralen Infrastruktur unter der Verwendung einer DLT auf. Vielmehr setzt sie sich mit einer ausgewählten technischen Ausgestaltung der zugrundeliegenden Software auseinander. Der Vorteil der Verwendung eines zentralen Registers wurde bereits in der Stellungnahme zum Modell der EZB als auch im Kapitel V.A dargestellt, weshalb es meiner Ansicht nach nichts an dieser Auswahl auszusetzen gibt.

Der umlaufende rCBDC nimmt die Form eines Tokens an, wobei die dahinterstehende GNU Taler-Software es den Nutzern gebietet, bei der Verwendung des Tokens in direktem Kontakt miteinander zuzustehen, ohne dass ein Intermediär eine Identifikation des Zahlenden vornehmen muss.¹⁶⁸ Wie beim Bargeld wird es meines Erachtens somit ermöglicht, anonyme Transaktionen zu tätigen, weil die Einschaltung der Intermediäre lediglich beim Bezug und Empfang des Tokens stattfindet.

¹⁶¹ Vgl. oben in Kapitel V.C.2.

¹⁶² Siehe dazu auch TRONNIER (Fn. 1), S. 109.

¹⁶³ Vgl. oben in Kapitel V.A.

¹⁶⁴ Mit weitergehenden Hinweisen und Vorschlägen für die Praxis vgl. GROTHOFF/MOSER (Fn. 122), S. 3.

¹⁶⁵ Vgl. oben in Kapitel IV.B.

¹⁶⁶ Siehe dazu auch CHAUM/GROTHOFF/MOSER (Fn. 86), S. 28.

¹⁶⁷ Vgl. oben in Kapitel V.C.2.

¹⁶⁸ Vgl. oben in Kapitel V.C.1.

Meiner Ansicht nach besteht jedoch ein Nachteil in der Effizienz der Nutzung des Tokens. Die gewünschte Menge an rCBDC muss zuerst bei der Zentralbank bezogen werden, bevor es verwendet werden kann. Beim anschließenden Empfang des Zahlungsempfängers wird dieser hinterlegt, um zu prüfen, ob der Token nicht bereits verwendet wurde. Da sich diese Stellungnahme jedoch auf das Zusammenspiel zwischen Privatsphäre und finanzielle Integrität bezieht, ist die Effizienz für sich genommen kein gewichtiger Nachteil. Sie leidet lediglich darunter, dass die Interessen aller Parteien hinsichtlich der Privatsphäre und der finanziellen Integrität bestmöglich gewahrt werden.

Dieser mangelnden Effizienz kann dazu entgegengewirkt werden, unter Anbetracht der zur Auswahl stehenden Implementierung der Obergrenzen im Barzahlungsverkehr und im unbaren Zahlungsverkehr. Der hoch angelegt Schwellenwert im Bereich des Bargeldes erlaubt es den Nutzern dieses Zahlungsmittel bequemer zu verwenden. Die Implementierung dieser Obergrenze könnte meines Erachtens dazu beitragen, dass die Akzeptanz der Nutzer in der Verwendung des rCBDC gefördert würde, trotz der zu bemängelnden Effizienz.

In Anbetracht der beiden behandelten Modelle eines rCBDC scheint meiner Ansicht nach das Modell des SNB Working Paper geeigneter einen Ersatz des Bargeldes darzustellen. Die vorgenommene Abwägung der Autoren trägt sowohl den Interessen der Nutzer als auch jenen der Emittenten Rechnung, ohne dass eine der beteiligten Parteien vernachlässigt wird. Es wurde zusätzlich bereits festgehalten, dass die EZB ihr Modell nicht für eine praktische Umsetzung empfiehlt. Die verfolgten Ansätze sind jedoch wertvoll, insbesondere die Idee der Verwendung von *anonymity vouchers*.

Eine Ergänzung dieses Konzepts durch eine zusätzliche Auseinandersetzung mit der zugrunde liegenden Infrastruktur des rCBDC könnte meiner Ansicht nach in Zukunft eine

weitere Option bieten, welche in eine praktische Verwendung münden könnte. Somit kann festgestellt werden, dass es verschiedene Möglichkeiten gibt, einen entsprechenden rCBDC zu erstellen, wobei es meines Erachtens keine einzige korrekte Lösung geben kann.

VII. Schlusswort

Mit dem sich im Wandel befindenden Geldwesen sehen mehrere Zentralbanken den Bedarf, die derzeitigen gesetzlichen Zahlungsmittel anzupassen, respektive zu ergänzen. Damit ist eine Verlagerung in den digitalen Bereich beabsichtigt, welche durch die Einführung eines rCBDC erreicht werden soll. Die damit verbundenen Folgen, welche sich u.a. in der Tangierung der informationellen Selbstbestimmung zeitigen, stellen diesen Schritt jedoch vor gewisse Herausforderungen. Um dem entgegenzuwirken, bieten sich auf der digitalen Ebene verschiedene Techniken an. Das staatliche Interesse an der finanziellen Integrität, welches sich in der Bekämpfung der Finanzkriminalität manifestiert, schränkt die Anwendbarkeit solcher Techniken jedoch ein.

Auf der internationalen Ebene haben verschiedene Zentralbanken bereits Modelle und Pilotprojekte eines rCBDC erarbeitet, wobei nicht alle Zentralbanken denselben Bedarf dafür sehen. In Anbetracht der vorhandenen Ansätze scheint die Einbeziehung der Abwägungsfrage zur informationellen Selbstbestimmung und finanziellen Integrität rar. Eine einschlägige Lösung ist noch inexistent.

Anhand der zunehmenden Bemühungen verschiedener Zentralbanken im Bereich eines rCBDC, besteht meines Erachtens jedoch die Möglichkeit, dass die in diesem Beitrag behandelte Thematik in Zukunft vermehrt auf Gehör stossen wird.