Magdalena Boškić* / Sebastian Hepp**

zkKYC in Decentralized Finance (DeFi)

Unter besonderer Berücksichtigung des Geldwäschereigesetzes

Inhaltsübersicht

I. Einleitung

Der Finanzsektor ist ein Bereich, welcher sich derzeit in einer Transformation befindet und durch die Blockchain-Technologie herausgefordert wird. Dabei entstehen neue Formen dezentraler Transaktionsabwicklung, welche programmgesteuert und selbstausführend sind. Sie sind komplett Blockchain-basiert und schaffen neue Möglichkeiten sowie Herausforderungen, sowohl für die Nutzer als auch für die bestehende Rechtsordnung. Dieser Aufsatz wird dieses Phänomen anhand von Decentralized Finance, Zero-Knowledge Proof und geldwäschereirechtlichen Anforderungen beleuchten. Der vorliegende Aufsatz widmet sich einleitend den Wesensmerkmalen von Decentralized Finance sowie dessen Herausforderungen und anschliessend werden verschiedene Lösungsansätze mittels Anwendung neuer Technologien analysiert.

II. Decentralized Finance (DeFi)

1. Einführung

Decentralized Finance («DeFi») hat seit dem Sommer 2020 (als «DeFi-Sommer» bezeichnet)[1] ein spektakuläres Wachstum erlebt, als der Gesamtwert der im DeFi-System hinterlegten Krypto-Assets[2] (sog. Total Value

* Head RegTech & Crypto Compliance Services bei der Sygnum Bank AG.
** Rechtsanwalt bei der MME Legal AG.

Die Autoren bedanken sich bei Dr. iur. Luka Müller, Partner bei der MME Legal AG für die kritische Durchsicht und die wertvollen Hinweise. Die Ausführungen stellen die persönlichen Ansichten der Autoren dar.

1 OECD (2022), Why Decentralised Finance (DeFi) Matters and the Policy Implications, OECD Paris, 15, https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm (zuletzt besucht am 4. April 2023).

2 Vorliegend umfasst der Begriff «Krypto-Assets» Payment Tokens, Utility Tokens, Asset Tokens sowie Hybride Tokens, vgl. Eidgenössische Finanzmarktaufsicht «FINMA», Wegleitung für Unter-

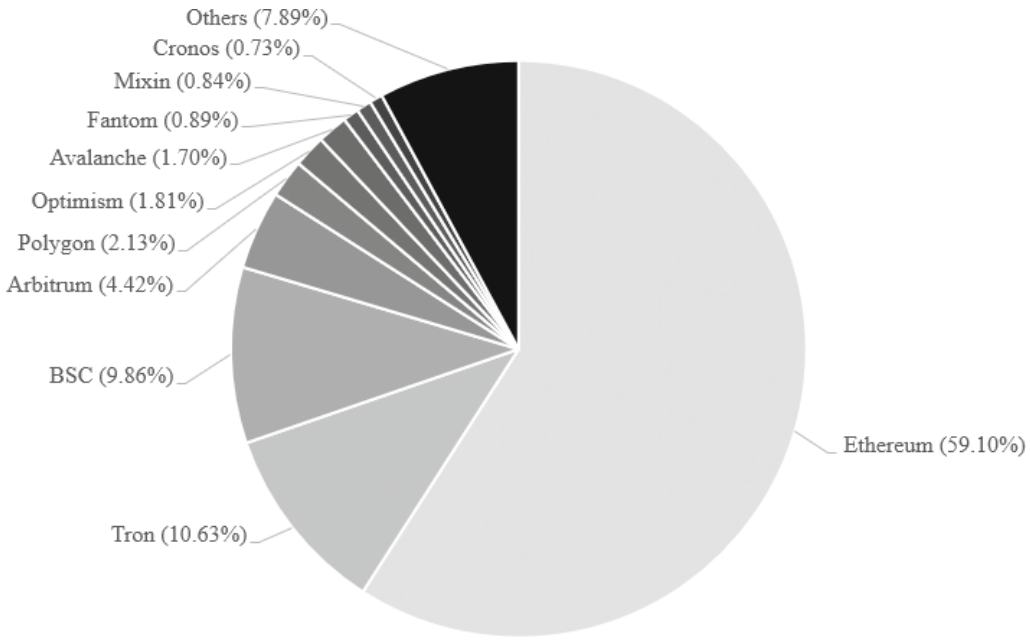

Abbildung 1. TVL in DeFi in den wichtigsten Blockchains[6]

Locked [TVL][3]) innert weniger Monate um das 50-fache anwuchs – von USD 1.9 Mrd. im Juli 2020 auf über USD 100 Mrd. im Mai 2021.[4] Im April 2023 lag der Wert aller in DeFi hinterlegten Krypto-Assets bei ca. USD 50 Mrd., wobei nahezu 60 % auf der Ethereum Blockchain basieren.[5]

DeFi ist ein aufstrebender und sich rasch entwickelnder Bereich an der Schnittstelle zwischen Blockchain, Krypto-Assets und Finanzdienstleistungen.[7] DeFi-Anwendungen ermöglichen die Bereitstellung von Finanzprodukten sowie -dienstleistungen, die als dezentrale Anwendungen auf einer öffentlichen Blockchain aufgebaut sind. Solche Anwendungen basieren hauptsächlich auf der Ethereum Blockchain, die 2015 eingeführt wurde und die Erstellung von Smart Contracts ermöglicht.[8]

Mittels der in DeFi verwendeten Smart Contracts werden Protokolle erstellt, die bestehende Finanzdienstleistungen offener, interoperabler und transparenter auf der Blockchain replizieren.[9] DeFi-Protokolle zielen auf eine Disintermediation von Finanzdienstleistungen ab, d.h. es wird auf Intermediäre wie z.B. Banken oder Vermögensverwalter verzichtet.[10] Dezentrale DeFi-Anwendungen basieren ausschliesslich auf Smart Contracts und werden automatisch ausgeführt. Es gibt eine Vielzahl potenzieller Anwendungsfälle, welche durch DeFi ermöglicht werden. Dazu zählen unter anderem (keine abschliessende Aufzählung):[11]

- Die Ermöglichung von Krediten mit Krypto-Assets (Kreditvermittlung);[12]
- Die Vermögensverwaltung für Krypto-Assets;[13]

stellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018, 2 ff.; Bei einem Token handelt es sich um eine digitale Abbildung eines Wertes in einem dezentralen Register wie z.B. eine Blockchain, vgl. Yves Mauchle, Token als Effekte, GesKR 1/2022, 183 ff., 183.

3 Total Value Locked (TVL) ist eine quantitative Kennzahl, welche den Gesamtwert aller Krypto-Assets misst, die in DeFi-Protokollen über Smart Contracts hinterlegt sind; vgl. Total Value Locked (TVL) Bitcoin2Go Wiki (bitcoin-2go.de) (zuletzt besucht am 10. April 2023).

4 OECD (FN 1), 16.

5 Https://defillama.com/chains (zuletzt besucht am 10. April 2023).

6 Https://defillama.com/chains (zuletzt besucht am 10. April 2023).

7 Claude Humbel, Decentralized Finance, GesKR 1/2022, 9 ff., 9.

8 OECD (FN 1), 15; Reto Luthiger/Hans Kuhn, Aufsichtsrechtliche Rahmenbedingungen, in: Weber/Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 221, Rz. 69 f.; siehe Ziff. II.3 nachstehend zu weiteren Ausführungen zu Smart Contracts.

9 Fabian Schär, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, 103 Federal Reserve Bank of St. Louis Review 2021, 153 ff., 153.

10 David Gogel, DeFi Beyond the Hype, Wharton Blockchain and Digital Asset Project, University of Pennsylvania, May 2021, 1, DeFi Beyond the Hype (upenn.edu) (zuletzt besucht am 10. April 2023).

11 Humbel (FN 7), 12.

12 Dabei handelt es sich um dezentrale Kreditmärkte, welche es den Nutzern erlauben, ihre Krypto-Assets für Kredite zu nutzen und dafür einen Zins zu erhalten bzw. zu bezahlen. Beispiele hierfür sind Aave, https://aave.com (zuletzt besucht am 10. April 2023), oder Compound, https://compound.finance (zuletzt besucht am 10. April 2023).

13 Ein Beispiel ist Babylon Finance, welches ein von der Community geführtes Asset-Management-Protokoll ist, das es den Nutzern ermöglicht, gemeinsam in DeFi zu investieren, https://docs.babylon.finance/getting-started/master (zuletzt besucht am 10. April 2023).

- Die Emission von Stable Coins;[14]
- Der Handel mit Krypto-Assets auf dezentralen Handelsplattformen (sog. DEXs).[15]

2. DeFi[16] Definition und Komposition

Eine allgemein anerkannte Definition von DeFi hat sich bisher nicht etabliert.[17] Gemäss Fabian Schär setzt sich DeFi im Wesentlichen aus den folgenden Komponenten zusammen: «The term generally refers to an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms, […].»[18]

Dezentralität («decentralized») ist die erste begriffsinhärente Komponente dieser Definition. Ferner zeichnet sich DeFi dadurch aus, dass es grundsätzlich offen und frei zugänglich («open, permissionless») ist sowie einen schichtartigen Aufbau der technischen Infrastruktur («highly interoperable protocol stack») aufweist. Schliesslich basiert DeFi auf Smart Contracts («built on public smart contract platforms»). Nachfolgend wird auf die einzelnen Komponenten näher eingegangen.

2.1. Dezentralität

Dezentralität lässt sich als Intermediationsfreiheit verstehen, was bedeutet, dass es zur Abwicklung von Transaktionen bzw. für den Zugang zu einer Infrastruktur keines Intermediärs bedarf. Bei DeFi ersetzt die neuartige Technologie die herkömmliche Finanzintermediation und erlaubt es dem Nutzer, mittels Software-Protokollen direkt mit der Infrastruktur zu interagieren und direkt mit anderen Nutzern Transaktionen abzuwickeln (sog. Peer-to-Peer), ohne die Zwischenschaltung oder gar den Einbezug eines Intermediärs.[19] In der Regel verwenden die Nutzer von DeFi eine Non-Custody-Struktur, was bedeutet, dass der jeweilige Nutzer, also der Inhaber, direkt und ausschliesslich über die Krypto-Assets in seinem eigenen Wallet verfügt.[20] Ein Wallet kann als eine Art digitales Portemonnaie verstanden werden, in welchem die Krypto-Assets aufbewahrt werden.[21] Jedes Wallet (sog. Public Key, vergleichbar mit einer IBAN im traditionellen Banking) verfügt neben der Protokolladresse über einen Private Key[22], was der Zugangsschlüssel zum Wallet ist und womit Transaktionen initiiert und ausgeführt werden können. Mittels Private Key hat der Nutzer die ausschliessliche Kontrolle und Verantwortung über seine Krypto-Assets. Im Gegensatz dazu überlässt der Nutzer bei einem Custody-Wallet den Private Key einem Wallet-Anbieter, welcher die Verwahrung der Krypto-Assets für den Nutzer übernimmt.[23] Der Nutzer kann im Rahmen eines Custody-Wallets Transaktionen initiieren, welche der Custody-Wallet-Anbieter für ihn ausführt. Obwohl die Intermediationsfreiheit typischerweise mit Dezentralität einhergeht, ist sie nicht zwangsläufig erforderlich. Stattdessen ermöglicht Dezentralität lediglich die Option, Intermediäre nach Bedarf auszuschliessen. Es ist jedoch durchaus möglich, dass Nutzer sich dafür entscheiden, Intermediäre bei der Nutzung oder dem Betrieb einer DeFi-Anwendung zu involvieren.[24] Als Beispiel können an dieser Stelle zentrale Krypto-Handelsplattformen wie Binance oder Coinbase genannt werden, welche ihren Kun-

---

14 Stable Coins sind Krypto-Assets, die ihren Wert an einen unterliegenden Vermögenswert bzw. Basiswert, wie zum Beispiel den US-Dollar, binden. Stable Coins erleichtern den Handel auf Krypto-Handelsplattformen, dienen als zugrunde liegender Vermögenswert für viele Krypto-Kredite und ermöglichen es Marktteilnehmern, Ineffizienzen zu vermeiden, die aus der Konvertierung von Krypto-Trades in Fiat-Währungen resultieren. Sie dienen im Wesentlichen sowohl als Zahlungsmittel als auch als Wertaufbewahrungsmittel für Krypto-Transaktionen, vgl. The Fed – The stable in stablecoins (federalreserve.gov) (zuletzt besucht am 16. April 2023).

15 Decentralized Exchanges; z.B. ist Uniswap eine 2018 gegründete DEX, die auf der Ethereum Blockchain operiert und es Nutzern ermöglicht, Krypto-Assets zu handeln, ohne dass ein zentraler Vermittler erforderlich ist, https://uniswap.org/ (zuletzt besucht am 10. April 2023).

16 Im April 2023 hat die US-Börsenaufsichtsbehörde (SEC) einen Vorschlag aus dem letzten Jahr wieder aufgegriffen, der nun ausdrücklich Plattformen für Krypto-Transaktionen als regulierungsbedürftige Handelsplattformen ins Visier nehmen will. Der aktualisierte Vorschlag verwendet nun eine direkte Formulierung, die DeFi in die erweiterte Definition der regulierten Handelsplattformen einbezieht. Die Kommentatoren unterscheiden sich in ihren Definitionen von «DeFi», oder was ein Produkt, eine Dienstleistung, eine Vereinbarung oder eine Aktivität «dezentralisiert» macht. Handelssysteme für Krypto-Assets, die umgangssprachlich als «dezentral» bezeichnet werden, kombinieren in der Regel traditionellere Technologien (wie webbasierte Systeme, die Aufträge annehmen und anzeigen, und Server, die Aufträge speichern) mit Distributed-Ledger-Technologie (wie mit «Smart Contracts» versehene Blockchains – selbstausführender Code, der auf Distributed-Ledger-Systemen ausgeführt wird und Berechnungen vom Typ «wenn/dann» vornimmt), https://www.coindesk.com/policy/2023/04/14/us-sec-poised-to-move-toward-defi-oversight-as-it-reopens-proposed-regulations/, Proposed Rule: Rule 3b-16 Reopening of Comment Period (sec.gov) (zuletzt besucht am 16. April 2023).

17 Benedikt Maurenbrecher/Benjamin Leisinger, Decentralized Finance (Teil 1), SJZ 118/2022, 647 ff., 648.

18 Schär (FN 9), 153.

19 Maurenbrecher/Leisinger (FN 17), 648 ff.

20 Vgl. World Economic Forum (WEF), Decentralized Finance (DeFi) Policy-Maker Toolkit, White Paper vom Juni 2021.pdf, 2 (zuletzt besucht am 10. April 2023).

21 Daniel Rutishauser/Ralf Kubli/Rolf H. Weber, Grundlagen, in: Weber/Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 17, Rz. 28 f.

22 Public und Private Key beziehen sich auf zwei Gruppen von alphanumerischen Zeichen, die mathematisch miteinander verbunden sind: Diese mathematisch gepaarten Schlüssel fungieren als öffentliche Adresse (Public Key), bei der Nutzer Krypto-Assets annehmen können, und ein privates Passwort (Private Key) ermöglicht dem Nutzer auf seine Krypto-Assets zuzugreifen und sie zu verwenden, vgl. Barbara Anita Möri, Blockchain und Datenschutz, Jusletter IT vom 23. Mai 2019, 9.

23 Michael Kunz, Provision of Custody Services for Digital Assets under Swiss Law, MME Compliance AG Magazinbeitrag vom 26. Oktober 2020, https://www.mme.ch/en/magazine/articles/provision-of-custody-services-for-digital-assets-under-swiss-law (zuletzt besucht am 10. April 2023).

24 Maurenbrecher/Leisinger (FN 17), 648 ff.

den DeFi-Produkte und -Dienstleistungen anbieten und dabei über eine Custody-Wallet-Struktur verfügen.

2.2. Offen und frei zugänglich

DeFi funktioniert grundsätzlich offen und ist frei zugänglich («open, permissionless»). Permissionless bedeutet, dass DeFi für jedermann zugänglich ist und es für den Zugang keiner aktiven Anerkennung durch einen Systemadministrator bedarf.[25] Es ist teilweise möglich, dass defensive Zugangsbeschränkungen (z.B. durch Disclaimer, Geoblocker) bestehen, ohne dass dadurch die Einstufung als permissionless beeinträchtigt wird.[26] Die Blockchain-Technologie beruht auf dem Open-Source-Prinzip, was bedeutet, dass der Quellcode der zugrunde liegenden Software komplett öffentlich zugänglich ist und jedermann ihn ohne Einschränkungen kopieren und bearbeiten kann. Ferner erfolgt die Weiterentwicklung der Software in einem öffentlichen Prozess, der transparent ist.[27]

2.3. Technische Infrastruktur

DeFi weist einen schichtartigen Aufbau der technischen Infrastruktur («highly interoperable protocol stack») auf.[28] Dabei besteht DeFi aus einem Stapel (sog. Stack) von verschiedenen Schichten (sog. Layers), die aufeinander aufbauen und hierarchisch sind.[29] Jede Schicht erfüllt einen bestimmten Zweck. Somit schaffen sie eine offene und hochgradig kombinierbare Infrastruktur, die es jedem ermöglicht, auf anderen Teilen des DeFi Stacks aufzubauen oder diese zu verwenden.[30] Aufgrund der Hierarchie ist ein Layer nur so sicher, wie die darunter liegenden Layers. Wenn beispielsweise die Blockchain im untersten Layer (sog. Settlement Layer; siehe nachfolgende Ausführungen unter Ziff. a) kompromittiert wird, wären alle nachfolgenden Layers nicht sicher. Der DeFi Stack lässt sich gemäss Fabian Schär in fünf Layers unterteilen, namentlich Settlement, Asset, Protocol, Application und Aggregation Layer:

a. Settlement Layer

Der Settlement Layer (Layer 1) besteht aus der Blockchain und dem zugehörigen Protokoll-Asset.[31] Die betreffende Blockchain dient als Transaktionssystem sowie -register und gewährleistet die Transparenz, Unveränderlichkeit und Sicherheit aller Transaktionen der darüberliegenden Layers.[32] Damit stellt der Settlement Layer das Fundament einer Blockchain dar, auf welchem die oberen Layers aufbauen.[33] Will ein Nutzer eine Transaktion vornehmen, ist er darauf angewiesen, dass diese validiert und in der Folge in einem neuen Blockchain-Block abgebildet wird. Transaktionen werden grundsätzlich zu unveränderlichen Blöcken zusammengefasst und mit einer kryptografischen Signatur versehen. Diese einzelnen Blöcke werden auf der Blockchain in einer unveränderlichen Kette aneinandergereiht, welche parallel in einem Netzwerk von tausenden Computern (sog. Nodes) abgespeichert werden.[34] Bei der Validierung von Transaktionen muss unter den Betreibern von Nodes ein Konsens darüber herrschen, dass die betreffende Transaktion «korrekt» ist und sie bspw. nicht manipuliert wurde oder eine doppelte Ausgabe der gleichen Einheiten eines Krypto-Assets (sog. Double Spending) zugrunde liegt.[35] Es lassen sich im Wesentlichen zwei Konsensverfahren unterscheiden:

Proof-of-Work («PoW»)

Beim Konsensverfahren mit der PoW-Methode muss ein kryptografisches Rätsel mittels Rechenleistung gelöst werden, um Transaktionen zu validieren und neue Token[36] generieren zu können (sog. Mining). Der Nodes Betreiber, welcher das kryptographische Rätsel als Erstes löst, bekommt eine Belohnung in Form von Tokens der Blockchain.[37] Als Konsensverfahren ermöglicht Proof-of-Work es dem dezentralen Netzwerk, einen Konsens zu finden oder sich auf Dinge wie Kontostände und die Reihenfolge von Transaktionen zu einigen. Die PoW-Methode wird in der Bitcoin Blockchain verwendet, steht aber immer wieder in der Kritik wegen den hohen Energiekosten für die Rechenleistung, um das Rätsel zu lösen.

Proof-of-Stake («PoS»)

Während die Ethereum Blockchain ursprünglich der PoW-Methode unterlag, findet seit der Umstellung (sog. Ethereum Merge) im September 2022 der Proof-of-Stake Konsensmechanismus Anwendung. Beim PoS handelt es sich um einen Konsensmechanismus, der von Blockchain-Netzwerken benutzt wird, um einen verteilten Konsens zu erreichen. Dieser verlangt von Nutzern die Hinterlegung ihrer ETH[38], um ein Validator im Netzwerk zu werden. Validatoren sind verantwortlich für die

---

25 Johannes Rude Jensen/Victor von Wachter/Omri Ross, An Introduction to Decentralized Finance (DeFi), Complex Systems Informatics and Modeling Quarterly 2021, 46 ff., 47; Rutishauser/Kubli/Weber (FN 21), 15, Rz. 20 f.

26 Maurenbrecher/Leisinger (FN 17), 648 ff.

27 Nicolas Jacquemart, Offene Blockchainsysteme und die Schutzziele des schweizerischen Finanzmarktrechts,
Unter Berücksichtigung möglicher Ansatzpunkte einer Regulierung, Diss. Zürich 2020, Rz. 164.

28 Maurenbrecher/Leisinger (FN 17), 648 ff.

29 Humbel (FN 7), 11; vgl. WEF (FN 20), 7.

30 Thomas Jutzi/Andri Abbühl, Fintech und DLT, Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023, 401.

31 Schär (FN 9), 155 ff.

32 Maurenbrecher/Leisinger (FN 17), 650.

33 Humbel (FN 7), 11.

34 Maurenbrecher/Leisinger (FN 17), 650; Jutzi/Abbühl (FN 30), 18 ff.

35 Humbel (FN 7), 17.

36 Vgl. FN 1 vorstehend.

37 Rutishauser/Kubli/Weber (FN 21), 16, Rz. 23 f.

38 Ether (ETH) ist der native Token der Ethereum Blockchain; vgl. Stephan D. Meyer/Bendedikt Schuppli, «Smart Conracts» und deren Einordnung in das schweizerische Vertragsrecht, recht 2017, 204 ff., 208.

Validierung von Transaktionen und dem Erstellen von neuen Blöcken, sodass alle Nodes mit dem Status des Netzwerks übereinstimmen. In der Ethereum Blockchain müssen Nutzer 32 ETH hinterlegen (sog. staken), um ein Validator zu werden. Validatoren werden zufällig ausgewählt, um Blöcke zu erstellen, und sind für die Überprüfung und Validierung von Blöcken, die andere Nodes erstellt haben, verantwortlich. Der Einsatz eines Nutzers wird auch als Anreiz für ein gutes Validator-Verhalten verwendet. Beispielsweise kann ein Nutzer seinen Einsatz ganz oder teilweise verlieren (sog. Slashing), wenn dieser bösartig Blöcke attestiert oder offline geht (Fehlversuch der Validierung). Im Gegensatz zum Proof-of-Work müssen Validatoren keine erheblichen Mengen an Rechenleistung für die Lösung von Rechenaufgaben verwenden, sondern lediglich ihre ETH hinterlegen, wobei die Validatoren zufällig ausgewählt werden und nicht miteinander konkurrieren wie in der Bitcoin Blockchain. Sie müssen nicht unentwegt Blocks minen (schürfen), sondern nur dann, wenn sie ausgewählt werden, und vorgeschlagene Blöcke validieren, wenn sie nicht ausgewählt sind (sog. Attestieren).[39] Das PoS Konsensverfahren ermöglicht es jedem Nutzer, die Korrektheit der einzelnen Transaktionen zu verifizieren, und gewährleistet die Integrität der Blockchain.[40]

b. Asset Layer

Der Asset Layer (Layer 2) besteht aus allen Krypto-Assets, die über den Settlement Layer generiert und ausgegeben werden. Dazu gehören die protokollinhärenten Krypto-Assets (sog. native Tokens), beispielsweise Bitcoin (BTC) auf der Bitcoin Blockchain oder Ether (ETH) auf der Ethereum Blockchain, sowie alle zusätzlichen Krypto-Assets (sog. non-native Tokens), die auf dieser Blockchain generiert und ausgegeben werden,[41] z.B. ERC-20 oder ERC-721 Token.[42]

c. Protocol Layer

Der Protocol Layer (Layer 3) bietet Standards für bestimmte Anwendungsfälle auf der Blockchain wie dezentrale Handelsplattformen, Kreditvermittlung und on-chain Vermögensverwaltung. Diese Standards werden in der Regel in Form von Smart Contracts auf der Blockchain implementiert und sind für jeden Nutzer (oder jede DeFi-Anwendung) zugänglich.

d. Application Layer

Der Application Layer (Layer 4) erstellt nutzerorientierte Anwendungen, die mit einzelnen Protokollen verbunden sind. Die Interaktion mit Smart Contracts wird in der Regel durch ein webbasiertes Frontend abstrahiert, was die Nutzung der Protokolle erleichtert.[43] Das Frontend umfasst alles, was auf dem Bildschirm eines Computers zu sehen ist, sowie die Ebenen, die für die Gestaltung verantwortlich sind. Das Graphical User Interface («GUI»), also die grafische Benutzeroberfläche, ist sozusagen das visuelle Produkt des Frontends.[44]

e. Aggregation Layer

Der Aggregation Layer (Layer 5) ist eine Erweiterung des Application Layers. Aggregatoren schaffen benutzerorientierte Plattformen, die eine Integration von mehreren Anwendungen und Protokollen ermöglichen. Sie bieten i.d.R. Tools für den Vergleich und die Bewertung von Diensten, ermöglichen es den Nutzern, ansonsten komplexe Aufgaben auszuführen, indem sie sich gleichzeitig mit mehreren Protokollen verbinden, und fassen relevante Informationen auf klare und präzise Weise zusammen.[45]

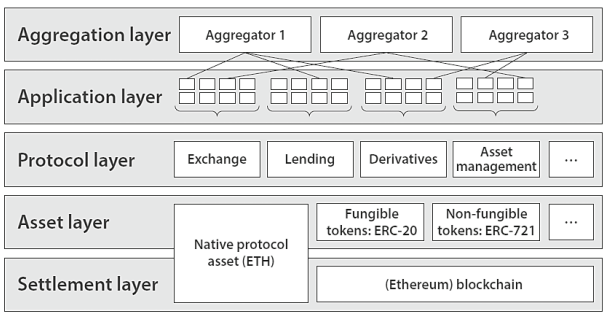

Abbildung 2. DeFi Stack nach Fabian Schär[46]

3. Smart Contracts

Bei Smart Contracts handelt es sich um softwarebasierte Protokolle, d.h. Computerprogramme, welchen vorbestimmte Regeln und Bedingungen zugrunde liegen, um autonom Aktionen auszuführen, zu kontrollieren sowie zu

---

39 Vgl. https://ethereum.org/de/developers/docs/consensus-mechanisms/pos/ (zuletzt besucht am 6. April 2023).

40 Maurenbrecher/Leisinger, (FN 17), 653.

41 Schär (FN 9), 156.

42 ERC steht für «Ethereum Request for Comments» und hat die Aufgabe, Funktionen für Ethereum anzubieten. Die Ethereum Blockchain unterscheidet nicht zwischen ERC-20 und ERC-721 Tokens. Stattdessen sind Token lediglich Variablen, die in Smart Contracts auf der Ethereum Blockchain festgelegt werden. ERC-20 repräsentieren vertretbare (sog. fungible Tokens) und ERC-721 sind nicht vertretbare (sog. non-fungible Tokens) Vermögenswerte, vgl. https://101blockchains.com/erc20-vs-erc721/, https://www.blockchain-council.org/ethereum/erc20-vs-erc721/^t:~:text=The%20main%20distinction%20between%20ERC20%20and%20ERC721%20tokens,collection%20of%20assets.%20Furthermore%2C%20ERC721%20is%20not%20divisible (zuletzt besucht am 16. April 2023).

43 Schär (FN 9), 156.

44 CMS-Revolution: Vom Backend zum Frontend, https://blog.hubspot.de/website/frontend-backend (zuletzt besucht am 16. April 2023).

45 Schär (FN 9), 156.

46 Schär (FN 9), 156.

dokumentieren.[47] Smart Contracts können diverse externe Inputdaten (sog. Orakel) verarbeiten (bspw. Geldeingang, Angabe einer Zahlungsadresse, Wechselkursdaten, Outputdaten anderer Smart Contracts), wobei diese vordefinierten Inputdaten dann Programmfunktionen auslösen können.[48] Die nachfolgenden Ausführungen erläutern gewisse Eigenschaften und Besonderheiten von Smart Contracts, die insbesondere im DeFi-Bereich von Relevanz sind.

3.1. Automatisierung

Smart Contracts ermöglichen eine Automatisierung, weil bestimmte (bzw. vorprogrammierte) Transaktionen automatisch abgewickelt werden, basierend auf Governance-Regeln und Geschäftslogiken, welche direkt im Programmcode niedergelegt sind. Ferner unterliegt ein Nutzer keiner Dependenz einer natürlichen oder juristischen Person, eine Transaktion korrekt auszulösen oder abzuwickeln. Anstatt einer Gegenpartei oder einem Intermediär vertrauen zu müssen, verlassen sich die Nutzer auf die Smart Contracts und deren Funktionen. Durch die Automatisierung, welche mittels Smart Contracts erzielt werden kann, können die Prozess- und Transaktionskosten reduziert werden.

3.2. Kontroll- und Korrekturmöglichkeiten

DeFi zielt auf autonome Abläufe ab, wobei die Autonomie so weit gehen kann, dass sogar fehlerhafte Ergebnisse, wie bspw. unerwünschte, aber dem Protokoll entsprechende Transaktionen, nicht korrigiert werden können. Bei fehlerhaften Programmcodes wird eine Transaktion dennoch ohne Weiteres abgewickelt und ist grundsätzlich unumkehrbar, sogar wenn sie einen gesetzeswidrigen Zweck hat oder eine beteiligte Person handlungsunfähig war. DeFi-Anwendungen liegen vordefinierten Programmcodes zugrunde, welche nicht selbständig auf unvorhergesehene Entwicklungen reagieren bzw. sich nicht selbst korrigieren. Aus diesem Grund werden teilweise Kontroll- und Korrekturmöglichkeiten in die Smart Contracts integriert, sowohl auf der Transaktionsebene als auch auf der Code-Ebene (Governance[49]).[50] Ferner ist es auch möglich, in Form von Admin Keys Kontrolle über einen Smart Contract zu halten, da Admin Keys die Kontrolle über Benutzerkonten oder das Funktionieren des Protokolls geben können. Es ist nicht unüblich, dass einige Gründer oder Softwareentwickler in den frühen Stadien des Protokolllebens einen Admin Key behalten, um Fehler im Protokoll zu beheben oder das Protokoll aktualisieren oder pausieren/herunterfahren zu können.[51]

3.3. Governance

Mittels sog. Governance Token ist es oftmals möglich, strategische und operative Weiterentwicklungen des betreffenden Codes in einem Smart Contract zu beeinflussen. Governance Token verleihen den Inhabern bestimmte Mitbestimmungsmöglichkeiten, wie bspw. Anpassungen des Protokolls oder der Gebührensätze. Folglich funktionieren DeFi-Anwendungen oftmals nicht völlig autonom, sondern unterliegen zumindest teilweise Eingriffsmöglichkeiten, welche mehr oder weniger dezentral ausgestaltet werden können. Es kann gar zu einer Zentralisierung kommen, wenn bspw. die Entwickler einer DeFi-Anwendung einen grösseren Teil der Governance Token halten, was in einer Konzentration der Entscheidungsmacht resultiert, womit auch das Risiko steigt, dass diese den Smart Contract zu ihren Gunsten beeinflussen. Viele DeFi-Anwendungen weisen eine Dezentrale Autonome Organisationen (DAOs) Struktur auf, welche es einer Vielzahl von Nutzern ermöglicht, an den Governance-Prozessen von Protokollen mitzuwirken und so kollektiv die künftige Entwicklung der DeFi-Anwendung zu beeinflussen. Durch den Erwerb von Governance Token erhält der Nutzer gewisse Mitbestimmungsrechte. Die Ausübung der entsprechenden Rechte erfolgt rein regelbasiert auf der Grundlage von Smart Contracts, wobei sämtliche möglichen Fälle von Mitbestimmungsrechten im Voraus bestimmt sowie im Softwarecode einprogrammiert sind und nach einem vorprogrammierten Abstimmungsverfahren durchgeführt werden.[52]

III. Zero-Knowledge Proofs

1. Konzept

Derzeit herrscht die noch weit verbreitete Auffassung, dass Transaktionen auf einer Blockchain anonym sind. Allerdings sind Transaktionen auf Blockchains wie Bitcoin und Ethereum pseudonymisiert und nicht anonymisiert. So ist in der Regel die Wallet-Adresse bzw. der Public Key ein Pseudonym für die Person, die den entsprechenden Private Key besitzt und die Transaktion auf der Blockchain ausgelöst hat.[53] Bei jeder Transaktion, die von einer Wallet-Adresse ausgeführt wird, können grundsätzlich, in Kombination mit anderen Parametern, Rückschlüsse auf die Person hinter einer Transaktion gezogen werden.[54] Da in öffentlichen und permissionless

---

47 Maurenbrecher/Leisinger (FN 17), 651 ff.; Rutishauser/Kubli/Weber (FN 21), 18, Rz. 32.

48 Andreas Furrer, Die Einbettung von Smart Contracts in das schweizerische Privatrecht, Anwaltsrevue 2018, 103 ff., 103.

49 Vgl. Ziff. II.3.3 nachstehend.

50 Maurenbrecher/Leisinger (FN 17), 652.

51 Schär (FN 9), 156.

52 Maurenbrecher/Leisinger (FN 17), 653.

53 Vgl. Ziff. II.2.3a. vorstehend.

54 Matthias Plattner, Datenschutzrechtliche Herausforderungen der Distributed-Ledger-Technologie, Impulse zur praxisorientierten Rechtswissenschaft 60/2021, 35 ff., Rz. 67; Jörn Erbguth, Datenschutz auf öffentlichen Blockchains, Jusletter IT vom 22. Februar 2018, Ziff. 3.1.1.

Blockchains alle Transaktionen in der Blockchain gespeichert werden und von jedem im Netzwerk eingesehen werden können, ist es grundsätzlich für jeden möglich, diese zurückzuverfolgen, auch wenn diese Transaktionen weit in der Vergangenheit liegen.[55] Die Bestimmbarkeit der Personen, welche eine Transaktion auf einer Blockchain ausgeführt haben, stellt ein immer grösseres Problem dar. So gibt es immer mehr spezialisierte Unternehmungen, die Personen hinter einer Transaktion auf einer Blockchain identifizieren können und die Re-Identifizierung als Dienstleistung anbieten (z.B. Chainalysis).[56] Eigenschaften von Blockchains (z.B. die Dezentralität oder die Unveränderbarkeit von Transaktionen) sowie die Prinzipien des Datenschutzes (z.B. Recht auf Berichtigung) sind in der Regel nicht miteinander vereinbar.

Aus diesem Grund sind alternative Lösungsansätze gefragt. Eine mögliche Lösung zur Verbesserung der Privatsphäre bei Transaktionen auf der Blockchain sind sog. Zero-Knowledge Proofs («ZKP»[57]). Das Konzept von Zero-Knowledge Proofs ist nicht neu und wurde bereits 1985 von Shafi Goldwasser, Silvio Micali und Charles Rackoff im Rahmen einer Arbeit mit dem Titel «The Knowledge Complexity of Interactive Proof-Systems» vorgestellt.[58] Bei der Zero-Knowledge Proof Technologie handelt es sich um ein kryptografisches bzw. mathematisches Verfahren zwischen zwei Parteien, dem Beweiser und dem Verifizierer, das es ermöglicht, den Wahrheitsgehalt einer Aussage zu beweisen, ohne dabei die Aussage selbst offenlegen zu müssen.[59] Mit dieser Methode kann der Beweiser gegenüber dem Verifizierer beweisen, dass etwas wahr ist, ohne weitere Informationen als rein den Fakt preiszugeben, dass diese spezifische Aussage wahr ist.[60] Um dies zu ermöglichen, stützen sich ZKP-Protokolle auf Algorithmen, die Daten als Input nehmen und diese als Output «wahr» oder «falsch» wiedergeben.[61] ZKP eignen sich zur formellen Überprüfung der Korrektheit von Daten, ohne dass der Inhalt der Daten bekannt sein muss. Mit ZKP kann z.B. eine Person nachweisen, dass sie eine bestimmte Altersgrenze überschritten hat (z.B. Mindestalter von 18 Jahren), ohne ihr tatsächliches Alter preisgeben zu müssen.[62]

Die ZKP-Technologie kann die Privatsphäre durch Minimierung von Daten in einer Transaktion auf einer Blockchain verbessern.[63] Besonders in der Blockchain-Technologie ist der Nachweis von Informationen mittels ZKP nützlich. In Blockchains validieren in den meisten Fällen alle teilnehmenden Nodes alle Transaktionen. Das bedeutet, dass im Prinzip alle Nodes alle Transaktionen sehen. Mit ZKP könnten alle Nodes Transaktionen validieren und die Privatsphäre der Nutzer würde trotzdem gewährleistet bleiben, da die Transaktionen keine persönlichen Informationen enthalten.[64]

2. Verschiedene Arten von Zero-Knowledge Proofs

2.1. Interaktive Zero-Knowledge Proofs

Bei interaktiven ZKP kommunizieren zwei Parteien miteinander, die den Beweis erbringen und verifizieren. Die Partei, die den Beweis erbringt, stellt dabei eine Reihe von Fragen, die von der verifizierenden Partei beantwortet werden müssen. Durch diesen interaktiven Austausch kann die verifizierende Partei überzeugt werden, dass der Beweis korrekt ist, ohne tatsächlich die vertraulichen Informationen zu kennen.[65]

Ein bekanntes Beispiel zur Veranschaulichung eines interaktiven Zero-Knowledge Proofs ist die «Höhle von Alibaba», bei welchem eine Höhle zwei Ausgänge hat, zwischen welchen es eine mittels einem geheimen Code verschlossene Türe hat. Der Beweiser kann beweisen,

---

55 Eine Ausnahme stellen sog. Privacy Coins dar, die durch Kryptografie echte Anonymität ermöglichen. Transaktionen können hier nicht mit einzelnen Wallet-Adressen verknüpft werden, https://blockchain-academy.hs-mittweida.de/courses/blockchain-introduction-technical-beginner-to-intermediate/lessons/lesson-4-privacy-in-blockchain-2/topic/anonymity-vs-pseudonymity/ (zuletzt besucht am 11. April 2023).

56 Die Blockchain-Datenplattform – Chainalysis (zuletzt besucht am 15. März 2023).

57 Nachfolgend kann nur die Grundidee der ZKP-Technologie aufgezeigt werden, da eine Auseinandersetzung mit der kryptographischen Technologie und Mathematik dahinter den Rahmen des vorliegenden Aufsatzes sprengen würde.

58 Shafi Goldwasser/Silvio Micali/Charles Rackoff, The Knowledge Complexity of Interactive Proof Systems, SIAM Journal on Computing 1/1989.

59 Cornelia Stengel/Roman Aus der Au, Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 2018, 439 ff., 451.

60 Pieter Pauwels, zkKYC, A solution concept for KYC without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs, June 2021, Version 1.0, 6; Plattner (FN 54), 59; Wang Huqing/Sun Zhixin, Research on Zero-Knowledge Proof Protocol, International Journal of Computer Science Issues (IJCSI), 10/2013, 188 ff., 194, verwenden für die bildhafte Veranschaulichung der ZKP-Technologie folgendes Beispiel: Es gibt einen Verifizierer (V), der farbenblind ist, und einen Beweiser (B), der farbfähig ist. Der farbfähige B möchte dem farbenblinden V beweisen, dass zwei Bälle, die bis auf ihre Farbe (Rot und Grün) identisch sind, unterschiedliche Farben haben und dass er dies erkennen kann. Es gibt eine Methode, die dafür angewendet werden kann: V erhält beide Bälle in jeweils eine Hand, ohne zu wissen, welcher Ball in welcher Hand ist. B kann die Farben der Bälle sehen und weiss, welcher Ball in welcher Hand ist. Dann versteckt V seine Hände hinter dem Rücken und tauscht gegebenenfalls die Bälle aus. Anschliessend zeigt V die Bälle wieder, und B kann anhand ihrer Farben erkennen, ob sie vertauscht wurden. Wenn man diesen Vorgang mehrmals wiederholt, wird V, obwohl er die Farben nicht sehen kann, erkennen, dass die Bälle unterschiedliche Farben haben müssen und dass B die Farben erkennen kann. Hierbei handelt es sich um einen sog. interaktiven ZKP (vgl. Ziff. III.2.1 nachstehend).

61 Vgl. Zero-knowledge proofs | ethereum.org (zuletzt besucht am 28. März 2023).

62 Tommy Koens/Coen Ramaekers/Cees van Wijk, Efficient Zero-Knowledge Range Proofs in Ethereum, 2, zero-knowledge-range-proof-whitepaper.pdf (zyxec.ee) (zuletzt besucht am 15. April 2023); Stengel/Aus der Au (FN 59), 451.

63 Plattner (FN 54), 62.

64 Koens et al. (FN 62), 2.

65 Koens et al. (FN 62), 3.

dass er den geheimen Code kennt, indem er jeweils bei dem vom Verifizierer gewünschten Höhlenausgang erscheint.[66] Bei diesem Beispiel handelt es sich um einen interaktiven Zero-Knowledge Proof, da eine fortlaufende Kommunikation zwischen Beweiser und Verifizierer notwendig ist, um den Verifizierer zu überzeugen.

Bei den interaktiven ZKP muss für jede Beweiserbringung (d.h. auch gegenüber jedem neuen Verifizierer) der interaktive Austausch wiederholt werden. Im Zusammenhang mit Blockchain-Anwendungen sind interaktive Zero-Knowledge Proofs nicht praktikabel, da sie aufgrund des interaktiven Informationsaustausches langsam sind und aufgrund der erhöhten Rechenleistung für die Interaktionen hohe Kosten verursachen.[67]

2.2. Nicht-interaktive Zero-Knowledge Proofs

Im Gegensatz zu interaktiven Zero-Knowledge Proofs ist bei nicht-interaktiven Zero-Knowledge Proofs nur ein einmaliger Informationsaustausch zwischen dem Beweiser und dem Verifizierer erforderlich. Der Beweiser übergibt die geheimen Informationen an einen speziellen Algorithmus, der einen Zero-Knowledge Proof berechnet.[68] Dieser Beweis wird an den Verifizierer gesendet, der mit Hilfe eines anderen Algorithmus überprüft, ob der Beweiser die geheimen Informationen kennt.[69] Aufgrund dieses Beweises kann der Verifizierer zweifelsfrei prüfen, ob der Beweiser über das entsprechende Wissen verfügt. Im Zusammenhang mit Blockchain-Anwendungen basiert der Beweis beim nicht-interaktiven ZKP auf Annahmen von kryptographischen Hash-Funktionen.[70]

Der Hauptvorteil von nicht-interaktiven ZKP besteht darin, dass sie in Situationen verwendet werden können, in denen es keine Möglichkeit der Interaktion zwischen dem Beweiser und dem Verifizierer gibt, wie z. B. bei Online-Transaktionen, bei denen die beiden Parteien nicht in Echtzeit kommunizieren. Dies macht nicht-interaktive ZKP besonders nützlich in dezentralen Systemen wie Blockchains, wo Transaktionen von einem Netzwerk von Nodes verifiziert werden und es keine zentrale Stelle gibt, die den Verifizierungsprozess überwacht.

3. Anwendungsbeispiele von ZKP auf der Blockchain

Im Folgenden werden einige mögliche Anwendungsbeispiele von ZKP auf der Blockchain aufgezeigt:

Verifizierung von Transaktionen

Wie vorstehend bereits erwähnt wurde[71], sind normalerweise alle Transaktionen auf einer Blockchain öffentlich und können von jedermann eingesehen werden. Mit der ZKP-Technologie kann jedoch der Beweis dafür erbracht werden, dass tatsächlich eine bestimmte Transaktion durchgeführt wurde, ohne Details wie den Betrag, das Wallet oder den Public Key offenzulegen.[72]

Identitätsverifizierung

ZKP kann auch zur Identitätsverifizierung eingesetzt werden. Hierbei wird die Identität einer Person überprüft, ohne dabei sensible Informationen wie Namen, Adresse, Geburtsdatum oder Sozialversicherungsnummer offenzulegen.[73] Anstatt solche persönlichen Informationen zu teilen, kann eine Person ein ZKP verwenden, um zu beweisen, dass sie tatsächlich die Person ist, die sie vorgibt zu sein. Eine andere Partei kann dann mit dem ZKP überprüfen und bestätigen, dass die Person tatsächlich die Person ist, ohne zusätzliche Informationen zu benötigen.[74]

Vermögensnachweis

ZKP kann auch dazu verwendet werden, den Nachweis von Vermögenswerten auf der Blockchain zu erbringen, ohne dass die genaue Höhe des Vermögens offengelegt werden muss (z.B. um gegenüber einer Bank zu beweisen, dass man über genügend Kapital/monatliches Einkommen für einen Kredit verfügt: vgl. die ING Bank verwendet hierfür Zero-Knowledge Range Proofs).[75]

Verbesserung der Skalierbarkeit

ZKP kann auch zur Verbesserung der Skalierbarkeit auf der Blockchain eingesetzt werden, indem es die benötigte Rechenleistung reduziert, die zur Überprüfung von Transaktionen und Smart Contracts erforderlich ist (z.B. durch sog. zkRollups auf der Ethereum Blockchain, wobei Transaktionen off-chain gebündelt werden und

---

66 Jean-Jacques Quisquater, How to explain Zero-Knowledge Protocols to Your Children, Conference Paper August 1989, How_to_Explain_Zero-Knowledge_Protocols_to_Your_Ch.pdf (zuletzt besucht am 25. März 2023).

67 Koens et al. (FN 62), 2.

68 Zero-knowledge proofs | ethereum.org (zuletzt besucht am 26. März 2023).

69 Erbguth (FN 54), Ziff. 2.4.1.

70 Koens et al. (FN 62), 4 ff.

71 Vgl. Ziff. III.1 vorstehend.

72 Als Beispiele sind hier Monero oder Zcash zu nennen. Zcash nutzt dabei sog. zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), wobei diese Technologie Transaktionen auf der Blockchain ohne Angabe eines Betrages oder des Empfängers ermöglicht; vgl. Eduardo Morais/Cees van Wijk/Tommy Koens, Zero Knowledge Set Membership, October 2018, 2, zero-knowledge-set-membership_whitepaper.pdf (ingwb.com) (zuletzt besucht am 25. März 2023); Koens et al. (FN 62), 4; Stengel/Aus der Au (FN 59), 451.

73 Morais et al. (FN 72), 2.

74 Zero-knowledge proofs | ethereum.org (zuletzt besucht am 30. März 2023).

75 Koens et al. (FN 62), 4.

anschliessend als eine Transaktion in einen Block aufgenommen werden).[76]

Zusammenfassend sind die Anwendungsbeispiele von ZKP auf der Blockchain vielfältig und es ist zu erwarten, dass ZKP in Zukunft eine immer wichtigere Rolle in dezentralen Systemen wie Blockchains spielen wird. Ein weiteres Anwendungsbeispiel ist der Zero-Knowledge Proof in Know-Your-Customer-Verfahren, auf welches nachfolgend näher eingegangen werden soll.

4. Zero-Knowledge Proof in KYC-Verfahren

4.1. KYC-Verfahren

Know-Your-Customer («KYC»[77]) hat sich als allgemeiner Überbegriff für Verfahren entwickelt, bei dem Unternehmen die Identität ihrer Kunden überprüfen und verifizieren, um Geldwäscherei, Terrorismusfinanzierung und andere illegale Aktivitäten zu verhindern. Das KYC-Verfahren ist in vielen Branchen und Ländern gesetzlich vorgeschrieben, um sicherzustellen, dass bei der Kundenakquise und der Aufnahme von neuen Geschäftsbeziehungen die gesetzlichen Bestimmungen eingehalten werden. Die Bedeutung von KYC ist in den letzten Jahren gestiegen, da die Globalisierung die grenzüberschreitende Zusammenarbeit und den Online-Handel erleichtert hat.

Das KYC-Verfahren findet beim Onboarding eines neuen Kunden statt, also wenn ein Unternehmen mit einem Kunden eine neue Geschäftsbeziehung eingehen möchte. Das KYC-Verfahren umfasst die Überprüfung von Identifikationsdokumenten wie Pass oder Identitätskarte sowie die Überprüfung von Adressen und anderen wichtigen Informationen eines potentiellen Kunden. Die gesetzeskonforme Durchführung von KYC-Verfahren stellt für Finanzmarktteilnehmer einen grossen Kosten- und Zeitaufwand dar. Um diese Verfahren zu vereinfachen, könnte die Blockchain-Technologie in Verbindung mit ZKP zum Einsatz kommen.

4.2. Zero-Knowledge Proof in KYC-Verfahren

Zero-Knowledge Know-Your-Customer («zkKYC») ist eine neue Technologie, die von Unternehmungen (wie z.B. Finanzintermediäre) eingesetzt werden könnte, um die Identität ihrer Kunden zu überprüfen, ohne unnötige persönliche Daten zu sammeln oder zu speichern.[78] zkKYC könnte dazu beitragen, die Herausforderungen von Privatsphäre auf der Blockchain zu bewältigen, indem es die Überprüfung von Identitäten ermöglicht, ohne dass sensible persönliche Informationen auf der Blockchain übertragen oder gespeichert werden müssen. Privatsphäre und die Sicherheit der einzelnen Kunden würden so erhöht. Bei herkömmlichen KYC-Verfahren müssen Kunden oft eine grosse Menge an persönlichen Informationen angeben, die anfällig für Datenmissbrauch, Hacks, Datenleaks usw. sein können. zkKYC ermöglicht die Überprüfung von Informationen, ohne dass jeder einzelne Kunde sensible persönliche Daten preisgeben muss, wodurch das Risiko von Identitätsdiebstahl und anderen Formen des Betrugs verringert werden kann.

Ein weiterer Vorteil von zkKYC ist, dass es das KYC-Verfahren rationalisieren und für Unternehmungen um ein Vielfaches vereinfachen könnte. Wie bereits ausgeführt wurde, müssen Finanzinstitute bei herkömmlichen KYC-Verfahren grosse Mengen an persönlichen Informationen von ihren Kunden sammeln und speichern, was zeitaufwendig und kostspielig ist. zkKYC könnte dazu beitragen, den KYC-Prozess zu vereinfachen, indem es die Menge der zu erfassenden und zu überprüfenden Informationen der Kunden reduziert bzw. egalisiert, was letztendlich zu Kosteneinsparungen bei den Unternehmungen führen würde.

An dieser Stelle ist darauf hinzuweisen, dass es noch keine Standards für die Umsetzung von zkKYC in der Praxis gibt und es – soweit ersichtlich – auch noch keine Jurisdiktion gibt, welche eine Identitätsprüfung von Kunden im Rahmen eines gesetzlich vorgeschriebenen KYC-Verfahrens auf der Blockchain mittels ZKP zulassen würde. Insgesamt hat zkKYC aber das Potenzial, ein wertvolles Instrument für Unternehmungen zu sein, die ihre KYC-Verfahren verbessern und vereinfachen sowie gleichzeitig die Privatsphäre und Sicherheit ihrer Kunden besser schützen und erhöhen würden.

Nachfolgend wird analysiert, ob zkKYC-Verfahren beim Onboarding von Neukunden im DeFi-Bereich Anwendung finden könnte und ob dadurch auch die gesetzlichen Anforderungen an KYC-Verfahren unter Schweizer Recht eingehalten werden würden.

---

76 Zero-knowledge proofs | ethereum.org (zuletzt besucht am 5. April 2023).

77 Für den vorliegenden Aufsatz wird das KYC-Verfahren als Verfahren zur Identifizierung der Vertragspartei bei der Aufnahme einer neuen Geschäftsbeziehung verstanden. Demgemäss handelt es sich beim KYC-Verfahren ausschliesslich um die Identifizierung der Vertragspartei beim ersten Kontakt zwischen Neukunden und der Unternehmung (sog. Onboarding). Hingegen werden für den vorliegenden Aufsatz die Pflichten während laufenden Geschäftsbeziehungen (z.B. laufendes Transaktionsmonitoring, fortlaufende Überprüfungen zwecks Risikoeinschätzung der Kunden usw.) nicht als KYC-Verfahren verstanden und im Nachfolgenden auch nicht weiter behandelt.

78 Morais et al. (FN 72), 3.

IV. Geldwäschereibekämpfung und DeFi

1. Die Geldwäschereigesetzgebung in der Schweiz

Die Geldwäschereibekämpfung soll den Eingang von Geldern verbrecherischen Ursprungs in den ordentlichen Geldkreislauf verhindern. Die Schweiz hat einen starken internationalen Finanzplatz und ist damit grundsätzlich mit der Gefahr von Geldwäscherei konfrontiert. Um dieser Gefahr zu begegnen, müssen Finanzintermediäre in der Schweiz die geldwäschereirechtlichen Pflichten einhalten.[79] Auf Schweizer Ebene sind die folgenden Erlasse für die Geldwäschereibekämpfung von Bedeutung:

- Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG) vom 10. Oktober 1997, SR 955.0.
- Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereiverordnung, GwV) vom 11. November 2015, SR 955.01.
- Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor (Geldwäschereiverordnung-FINMA, GwV-FINMA) vom 3. Juni 2015, SR 955.033.0.
- Des Weiteren präzisieren Reglemente von Selbstregulierungsorganisationen die gesetzlichen Bestimmungen.[80]

Das GwG findet gemäss Art. 2 Abs. 1 GwG Anwendung auf (i) Finanzintermediäre sowie auf (ii) natürliche und juristische Personen, die gewerbsmässig mit Waren handeln und Bargeld von mehr als CHF 10'000.00 annehmen (Händler). Des Weiteren unterteilt das GwG unterstellte Finanzintermediäre in prudenziell beaufsichtigte (Art. 2 Abs. 2 GwG) und übrige (Art. 2 Abs. 3 GwG) Finanzintermediäre. Als Finanzintermediäre gelten damit einerseits die spezialgesetzlich regulierten Finanzintermediäre nach Art. 2 Abs. 2 GwG (z.B. Banken, Versicherungen, Vermögensverwalter usw.) sowie seit dem 1. August 2021 auch DLT-Handelssysteme (Art. 2 Abs. 2 lit. d^{quater} GwG) und Personen nach Art. 1*b* Bankengesetz (sog. FinTech-Unternehmen; Art. 2 Abs. 1 lit. a GwG).[81] Andererseits werden natürliche oder juristische Personen als Finanzintermediäre qualifiziert, die berufsmässig[82] fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen.[83] Zu diesen Finanzintermediären zählen insbesondere Personen, die Dienstleistungen für den Zahlungsverkehr erbringen, etwa für Dritte elektronische Überweisungen vornehmen oder Zahlungsmittel wie Kreditkarten oder Reiseschecks ausgeben oder verwalten (Art. 2 Abs. 3 lit. b GwG).[84]

Aus territorialer Sicht werden Finanzintermediäre dann vom schweizerischen GwG erfasst, wenn sie in der Schweiz oder von der Schweiz aus tätig sind. Gemäss FINMA-Praxis ist dies in der Regel der Fall, wenn der Finanzintermediär in der Schweiz seinen Wohnsitz hat oder im Handelsregister eingetragen ist, oder er in der Schweiz eine faktische Zweigniederlassung begründet (Art. 2 Abs. 1 lit. a GwV).[85]

2. Anwendung des GwG in DeFi

Die Herausforderung in der DeFi-Welt besteht darin, dass die Akteure nicht über einen zentralen Intermediär zusammenarbeiten, sondern auf Basis von Smart Contracts und individuellen Interaktionen mit ihren Wallet-Adressen Transaktionen auf der Blockchain tätigen.[86] Da DeFi hauptsächlich auf Peer-to-Peer-Modellen basiert, spielen traditionelle Intermediäre wie Banken oder Wertpapierhäuser im Grunde keine Rolle.[87] Im Gegensatz zu traditionellen Finanzdienstleistungen gibt es bei echten DeFi-Anwendungen keinen einzelnen Betreiber, der bestimmbar ist und Autorität, Kontrolle oder Einfluss über das Protokoll hat.[88]

Bei vollständig dezentralen DeFi-Protokollen findet die schweizerische Geldwäschereigesetzgebung grundsätzlich keine Anwendung, sofern keine dauernde Geschäftsbeziehung zu den Nutzern vorliegt.[89] Dies ist auch verständlich, da es sich bei solchen Infrastrukturen um vollständig automatisierte Smart Contracts handelt, die keine Rechtssubjekte im Sinne des Gesetzes sind und deshalb auch nicht Adressaten von Gesetzbestimmungen sein können. Transaktionen werden bei vollständig

---

79 Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17. Juni 1996, BBl 1996 III 1101, 1996, 1102.

80 Z.B. das Reglement der Selbstregulierungsorganisation nach Geldwäschereigesetz vom Verein zur Qualitätssicherung von Finanzdienstleistungen («VQF»), Stand: 30. Januar 2023 (zit. VQF-Reglement).

81 Jutzi/Abbühl (FN 30), 197.

82 Vgl. Art. 7 GwV.

83 Bundesrat, Bericht vom 14. Dezember 2018, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz, Eine Auslegeordnung mit Fokus auf dem Finanzsektor, 140 (zit. DLT-Bericht).

84 BSK GwG-Greter, Art. 2 Abs. 3 N 1.

85 FINMA Rundschreiben 2011/1 Tätigkeit als Finanzintermediär nach GwG vom 3. November 2020, Rz. 28.1 f.

86 Regulatorische Gedanken zum Aufstieg von DeFi | Bitcoin Suisse (zuletzt besucht am 5. April 2023).

87 FINMA-Jahresbericht 2021, 20 ff.; Decentralized Finance (DeFi) | FINMA (zuletzt besucht am 8. April 2023).

88 Pieter Pauwels/Joni Pirovich/Peter Braunz/Jack Deeb, zkKYC in DeFi – An approach for implementing the zkKYC solution concept in Decentralized Finance, 4, Pieter Pauwels et al_ zkKYC in DeFi.pdf (zuletzt besucht am 12. April 2023).

89 Eidgenössisches Finanzdepartement (EFD), Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Erläuterungsbericht vom 18. Juni 2021, 22 f. (zit. Erläuterungsbericht DLT-Verordnung).

dezentralen DeFi-Protokollen ohne Zwischenschaltung eines Intermediärs direkt zwischen den Nutzern Peer-to-Peer abgewickelt.[90]

Tatsächlich ist aber die in DeFi erwähnte Dezentralität oft mehr Schein als Sein. Was oft als dezentralisiert angepriesen wird, ist *de facto* zentralisiert und wird von Einzelpersonen oder kleinen Gruppen kontrolliert. So beziehen DeFi-Protokolle häufig ihre Daten von zentralen Stellen und/oder können von zentralen Stellen oder einzelnen Personen beeinflusst werden. Wie oben erwähnt[91], ist es möglich, durch Verfügungsmacht über die Mehrheit von Governance Tokens oder Admin Keys Transaktionen zu kontrollieren, zu verhindern oder freizugeben.[92] Durch einen Admin Key kann eine zentrale Stelle u.U. einen Smart Contract aktualisieren und damit in dessen Funktionsweise eingreifen.

Zentral organisierte und kontrollierte DeFi-Protokolle werden in der Schweiz mit traditionellen Finanzmarktteilnehmern gleichgestellt, weshalb diese auch in den Geltungsbereich des Finanzmarktrechts fallen. Die FINMA geht bei der Frage, ob es sich um dezentralisierte oder zentralisierte DeFi-Protokolle handelt, jeweils von folgenden Ansätzen aus:

- Die bestehenden Regeln werden von der FINMA auch im DeFi-Bereich angewendet. Dabei wird der Grundsatz der Technologieneutralität verfolgt.
- Erbringt eine DeFi-Anwendung dieselbe Dienstleistung und birgt sie dieselben Risiken wie Finanzintermediäre im traditionellen Finanzmarkt, wendet die FINMA auch dieselben Regeln an (Grundsatz *«same risks, same rules»*).
- Erbringt eine DeFi-Anwendung wirtschaftlich betrachtet eine finanzmarktrechtliche Tätigkeit, die bewilligungspflichtig wäre, geht die FINMA auch bei neuartiger technischer oder rechtlicher Umsetzung von einer Bewilligungspflicht aus (Grundsatz der wirtschaftlichen Betrachtungsweise).[93]

Der Geltungsbereich der schweizerischen Geldwäschereigesetzgebung wird immer mehr auf dezentrale Infrastrukturen im Blockchain-Bereich erweitert. So wurde per 1. August 2021 in der Geldwäschereiverordnung eine neue Bestimmung für virtuelle Währungen[94] in Kraft gesetzt. Gemäss Art. 4 Abs. 1 lit. b GwV liegt eine Dienstleistung für den Zahlungsverkehr im Sinne von Art. 2 Abs. 3 lit. b GwG neu insbesondere auch dann vor, wenn ein Finanzintermediär hilft, virtuelle Währungen an eine Drittperson zu übertragen, sofern er mit der Vertragspartei eine dauernde Geschäftsbeziehung unterhält oder sofern er für die Vertragspartei Verfügungsmacht über virtuelle Währungen ausübt, und er die Dienstleistung nicht ausschliesslich gegenüber angemessen beaufsichtigten Finanzintermediären erbringt.

Ausgangspunkt für die Einführung der neuen Bestimmung in der GwV war gemäss Gesetzesmaterialien, dass bei den immer dezentraleren Modellen der Vermögensübertragung der Finanzintermediär nicht mehr in allen Geschäftsmodellen die alleinige Verfügungsmacht über Vermögenswerte hat. Die schnelle Entwicklung von Geschäftsmodellen im Distributed-Ledger-Technologie («DLT»)-Bereich führe dazu, dass es für Aufsichtsbehörden sehr schwierig und unverhältnismässig aufwendig abzuklären sei, ob im Rahmen einer technischen Lösung keine geldwäschereirechtlich relevante Verfügungsmacht bestehe. Aufgrund dessen erachtete der Bundesrat die Verfügungsmacht als alleiniges Kriterium zur Abgrenzung von unterstellten und nicht-unterstellten Dienstleistungen im DLT-Bereich als nicht mehr sachgerecht.[95]

Eine unterstellungspflichtige Dienstleistung für den Zahlungsverkehr ist im DeFi-Bereich insbesondere im Rahmen einer Hilfe zur Übertragung virtueller Währungen an eine Drittpartei i.S.v. Art. 4 Abs. 1 lit. b GwV zu verzeichnen. In Bezug auf die neue Unterstellung von dezentralen Geschäftsmodellen im Blockchain-Bereich sind folgende Beispiele zu erwähnen:

Dezentrale Handelsplattformen

Dezentrale Handelsplattformen ermöglichen den Transfer von Krypto-Assets über einen von der Handelsplattform betriebenen Smart Contract.[96] Im Gegensatz zu zentralen Handelsplattformen verfügen dezentrale Handelsplattformen weder über eine zentrale Instanz noch eine Verwahrungsstelle. Stattdessen nehmen Smart Contracts diese Aufgaben wahr und die Nutzer behalten damit stets die Kontrolle über ihre Krypto-Assets.[97]

Unter die neue Bestimmung in der GwV fallen auch dezentrale Handelsplattformen, die nicht im Besitz des Private Keys der Kunden sind, die Übertragung der virtuellen Währungen jedoch mittels Smart Contract ermöglichen und dabei die Aufträge bestätigen, freigeben

---

90 Maurenbrecher/Leisinger (FN 17), 648.

91 Vgl. Ziff. II.3.3 vorstehend.

92 Jutzi/Abbühl (FN 30), 406.

93 Vgl. Decentralized Finance (DeFi) | FINMA (zuletzt besucht am 3. April 2023).

94 Virtuelle Währungen sind kryptobasierte Vermögenswerte und zeichnen sich besonders dadurch aus, dass sie als Zahlungsmittel eingesetzt werden können (sog. Payment Tokens wie z.B. Bitcoin); vgl. Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Erläuterungen vom 18. Juni 2021, 23 f.

95 Erläuterungsbericht DLT-Verordnung (FN 89), 11 und 22; die Erläuterungen zur Einführung der neuen Bestimmung in der GwV sowie der damit erweiterte Geltungsbereich des GwG wurden in der Lehre kritisiert; vgl. Cornelia Stengel/Luca Bianchi, Geldwäscherei und Terrorismusfinanzierung, in: Weber/Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 223 ff., Rz. 21; BSK GwG-Bachelard/Hess, Art. 2 Abs. 3 N 13 ff.

96 Beispiele von DEXs sind Uniswap, SushiSwap, Curve oder PancakeSwap, Was sind dezentrale Börsen (DEXs)? | Bitcoin Suisse (zuletzt besucht am 14. April 2023).

97 Jutzi/Abbühl (FN 30), 161 ff.

oder sperren können oder anderweitig Kontrolle über den Smart Contract haben. Solche dezentralen Handelsplattformen werden als Hilfe zur Übertragung von Vermögenswerten und insbesondere als Dienstleistung für den Zahlungsverkehr angesehen[98] und fallen somit unter die neue Bestimmung in der GwV.[99]

Non-Custody-Wallet-Anbieter

Im Gegensatz zu den Custody-Wallet-Anbietern verwahren die Anbieter von Non-Custody-Wallets die Private Keys der Nutzer nicht und verfügen damit über keine Verfügungsmacht über fremde Vermögenswerte. Der Nutzer kann unabhängig vom Non-Custody-Wallet-Anbieter seine Krypto-Assets verwalten und transferieren.[100] Da der Non-Custody-Wallet-Anbieter keine Verfügungsmacht (weder eine rechtliche noch eine faktische) über fremde Vermögenswerte hat, waren diese Wallet-Services – bis vor der Gesetzesrevision – keine Finanzintermediation und demzufolge wurden Non-Custody-Wallet-Anbieter nicht dem GwG unterstellt.[101]

Dies hat sich mittlerweile geändert. Mit der neuen Bestimmung in der GwV fallen neu auch Non-Custody-Lösungen unter das GwG, wenn der Anbieter Dienstleistungen zur Aufbewahrung von Private Keys erbringt, auch wenn Letztere verschlüsselt sind und grundsätzlich nur vom Kunden entschlüsselt werden können. Dies dürfte beispielsweise bei Wallet-Anbietern der Fall sein, welche die Speicherung von Private Keys in einer Cloud anbieten, da der Nutzer darauf angewiesen ist, jederzeit auf die Cloud des Anbieters zugreifen zu können und damit vom Funktionieren der Infrastruktur des Anbieters abhängig ist. D.h. Anbieter von Non-Custody-Wallet-Lösungen können in den Geltungsbereich des GwG fallen, auch wenn sie keine Verfügungsmacht über die Vermögenswerte haben. Gemäss den Gesetzesmaterialien seien die Risiken gerade bei derartigen Wallets, die weder reine Custody- noch reine Non-Custody-Wallets sind, grundsätzlich vergleichbar mit denjenigen von Money Transmittern.[102]

Folgende Geschäftsmodelle im DeFi-Bereich werden hingegen weiterhin nicht dem GwG unterstellt:[103]

- **Software-Anbieter**: Anbieter, die bloss eine Software und die erforderliche Lizenzierung, nicht aber Zusatzleistungen zur Auslösung oder Durchführung von Zahlungen zur Verfügung stellen, werden weiterhin nicht dem GwG unterstellt.
- **Vollständig dezentrale DLT-Systeme**: Vollständig dezentrale DLT-Systeme ohne dauernde Geschäftsbeziehung zu den Kunden sind weiterhin nicht dem GwG unterstellt.
- **Handelsplattformen**: Weiterhin sind Handelsplattformen nicht dem GwG unterstellt, die lediglich Käufer und Verkäufer zusammenführen und die Abwicklung der Transaktion ohne Smart Contract mit Zugriffsmöglichkeit der Handelsplattform erfolgt. Dabei handelt es sich um eine reine Vermittlungstätigkeit ohne Hilfe bei der Übertragung von virtuellen Währungen.[104]

Zusammenfassend kann festgehalten werden, dass wenn Smart Contracts von DeFi-Protokollen die Verfügungsmacht über Vermögenswerte ermöglichen oder damit eine dauernde Geschäftsbeziehung begründet wird, die Betreiber solcher Infrastrukturen bei berufsmässiger Ausübung grundsätzlich eine unterstellungspflichtige Hilfe zur Übertragung virtueller Währungen als Dienstleistung für den Zahlungsverkehr im Sinne des GwG ausüben dürften, sofern es sich nicht um vollständig dezentrale DLT-Systeme handelt. Eine Unterstellung als berufsmässiger Finanzintermediär hat die Einhaltung weitrechender Sorgfaltspflichten zur Folge, deren Umsetzung im DeFi-Bereich eine massive Herausforderung darstellt.[105]

3. GwG-Pflichten im KYC-Verfahren

Findet das GwG Anwendung, so haben unterstellungspflichtige Finanzintermediäre verschiedene Sorgfaltspflichten zur Verhinderung von Geldwäscherei einzuhalten. Im Rahmen des KYC-Verfahrens müssen Finanzintermediäre bei der Aufnahme neuer Geschäftsbeziehungen mit potentiellen Neukunden folgende GwG-Pflichten erfüllen:

3.1. Identifizierung der Vertragspartei (Art. 3 GwG)

Gemäss Art. 3 GwG sind alle Finanzintermediäre dazu verpflichtet, bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei zu identifizieren. Durch diese Gesetzesbestimmung wird das «Know-Your-Customer»-Prinzip kodifiziert. Damit soll die Grundlage für die erfolgreiche Bekämpfung von Geldwäscherei und Terrorismusfinanzierung geschaffen werden. Die Identifizierung der Vertragspartei alleine genügt allerdings nicht, da eine juristische oder natürliche Person einfach als formelle Vertragspartei vorgeschoben werden könnte, ohne dass Informationen über die dahinterstehende

---

98 Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019, BBI 2020 233, 270 f.

99 Erläuterungsbericht DLT-Verordnung (FN 89), 22 f.

100 Stefan Kramer/Dominic Wyss, Verwahrung von digitalen Aktiven, in: Weber/Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 149, Rz. 9 f.

101 DLT-Bericht (FN 83), 145 f.; Stengel/Bianchi (FN 95), 236, Rz. 22.

102 Erläuterungsbericht DLT-Verordnung (FN 89), 22 f.

103 Erläuterungsbericht DLT-Verordnung (FN 89), 22 f.

104 Erläuterungsbericht DLT-Verordnung (FN 89), 22 f.

105 Luca Bianchi, FinTech Regulation 2.0 – An Overview on the Proposed Three Element Solution, CapLaw 2/2017, FinTech Regulation (2.0): An Overview on the Proposed Three Element Solution – CapLaw (zuletzt besucht am 2. April 2023).

Person gemäss Art. 3 GwG für den Finanzintermediär oder letztlich die Ermittlungsbehörden zugänglich wären. Erst die Feststellung der wirtschaftlich berechtigten Person gemäss Art. 4 GwG führt somit zum gewünschten Ergebnis (siehe Ziff. 3.2 nachstehend).[106]

Nach der gesetzlichen Bestimmung muss ein Finanzintermediär seine Vertragspartei bei der Aufnahme der Geschäftsbeziehung aufgrund eines beweiskräftigen Dokuments identifizieren. Als «beweiskräftiges Dokument» gilt jedes Identifikationsdokument, das mit einer Fotografie versehen und von einer schweizerischen oder ausländischen Behörde ausgestellt wurde. Hierzu gehören z.B. Pass, Identitätskarte, Führerausweis usw.[107] Im Rahmen der Identifizierung der Vertragspartei ist der Name, Vorname, das Geburtsdatum, die Wohnsitzadresse (effektiver Wohnsitz) sowie die Staatsangehörigkeit der natürlichen Person festzustellen.[108]

Die Identifizierung einer Vertragspartei kann im Rahmen einer **persönlichen Vorsprache** durchgeführt werden, wobei bei einem physischen Treffen ein amtlicher Ausweis mit Foto (z.B. Identitätskarte, Führerausweis, Pass) der Vertragspartei eingesehen und eine Kopie dieses Ausweises zu den Akten genommen wird (vgl. Art. 45 ff. GwV-FINMA).[109] Alternativ kann die Geschäftsbeziehung auf dem **Korrespondenzweg** aufgenommen werden, wobei in diesem Fall der Finanzintermediär eine echtheitsbestätigte Kopie eines Identifikationsdokuments einzuholen hat. Schliesslich kann eine Identifizierung der Vertragspartei auch auf digitalem Weg durchgeführt werden. So ist z.B. eine **Video-Identifizierung** möglich, bei welcher die Identifizierung mittels audiovisueller Kommunikation in Echtzeit (Liveschaltung) zwischen der Vertragspartei und dem Finanzintermediär erfolgt.[110]

Bei juristischen Personen muss der Finanzintermediär die Bevollmächtigungsbestimmungen der Vertragspartei zur Kenntnis nehmen und die Identität der Personen überprüfen, die im Namen der juristischen Person die Geschäftsbeziehung aufnehmen kann. Auch hier hat die Identifizierung mittels eines «beweiskräftigen Dokumentes» zu erfolgen (Art. 3 Abs. 1 GwG), wobei bei juristischen Personen darunter ein Auszug aus dem Handelsregister oder ein gleichwertiges Dokument (z.B. certificate of incorporation) zu verstehen ist.[111]

3.2. Feststellung der wirtschaftlich berechtigten Person (Art. 4 GwG)

Finanzintermediäre müssen mit der nach den Umständen gebotenen Sorgfalt die wirtschaftlich berechtigte Person feststellen und deren Identität überprüfen, um sich zu vergewissern, wer die wirtschaftlich berechtigte Person ist. Bei dieser Bestimmung ist zu beachten, dass bei der Feststellung des Kontrollinhabers oder der wirtschaftlich berechtigten Person im Gegensatz zur Vertragspartei keine formale Identifizierung erforderlich ist, sondern lediglich eine «Feststellung». In der Regel holt der Finanzintermediär hierfür eine schriftliche Erklärung der Vertragspartei ein (Art. 4 Abs. 2 GwG). In der Schweiz gibt es aber keine gesetzliche Verpflichtung, ein Identifikationsdokument (z.B. eine Passkopie) der wirtschaftlich berechtigten Person zu verlangen.[112]

Wenn es um Geschäftsbeziehungen mit Kunden geht, die im Blockchain-Bereich tätig sind, so kann die Kontrolle über Krypto-Assets beispielsweise durch eine Bestätigung einer Transaktion mittels digitaler Signatur durchgeführt werden oder bei der Ausgabe von Tokens kann eine Mikrotransaktion von der öffentlichen Adresse des Emittenten gesendet und dieser Vorgang dokumentiert werden, um die wirtschaftlich berechtigte Person festzustellen.[113]

3.3. Dokumentationspflicht (Art. 7 GwG)

Die im Rahmen des KYC-Verfahrens gesammelten Informationen zur Identifizierung der Vertragspartei sowie Feststellung der wirtschaftlich berechtigten Person sind Gegenstand der Dokumentationspflicht gemäss Art. 7 Abs. 1 GwG. Zu dokumentieren und aufzubewahren sind die zu diesem Zweck erhobenen Unterlagen (z.B. Passkopien, Registerauszüge, Erklärungen etc.).[114] Um die Dokumentationspflicht gesetzeskonform zu erfüllen, muss der Finanzintermediär eine Kopie des Identifikationsdokuments, das im Original eingesehen wurde, in seinen Akten aufbewahren. Falls er stattdessen eine echtheitsbestätigte Kopie des Originals eingesehen hat, kann er diese in das Kundendossier aufnehmen (vgl. Art. 48 Abs. 2 GwV-FINMA).[115]

Für die Erfüllung der Dokumentationspflicht nach Art. 7 GwG könnte auch die Blockchain-Technologie zum Einsatz kommen. Grundsätzlich sind zwei Varianten für die Speicherung der Dokumentation auf der Blockchain denkbar: Die gesamte Dokumentation oder lediglich ein Hashwert von den Dokumenten wird auf der Blockchain gespeichert.[116] Die Dokumente könnten so gehasht werden, damit statt der Daten selbst nur ihr Hashwert in der

---

106 BSK GwG-Landolt/Gemperli, Art. 3 N 2.

107 Günther Dobrauz-Saldapenna/Corsin Derungs, Art. 3 N 14, in: Kunz/Jutzi/Schären (Hrsg.), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Stämpflis Handkommentar, Bern 2017.

108 BSK GwG-Landolt/Gemperli, Art. 3 N 44.

109 Stengel/Bianchi (FN 95), 238, Rz. 27.

110 FINMA Rundschreiben 2016/7 Video- und Online-Identifizierung vom 20. Juni 2018, Rz. 6; Stengel/Bianchi (FN 95), 238; Jutzi/Abbühl (FN 30), 216.

111 SHK GwG-Dobrauz-Saldapenna/Derungs (FN 107), Art. 3 N 26 ff.

112 Stengel/Bianchi (FN 95), 239, Rz. 31 ff.

113 Vgl. Leitfaden der SBVg zur Eröffnung von Firmenkonti für DLT Unternehmen (2019), 12; BSK GwG-Meyer/Ryhner, Art. 4 N 78.

114 BSK GwG-Lötscher/Sievi, Art. 7 N 18.

115 BSK GwG-Landolt/Gemperli, Art. 3 N 49.

116 BSK GwG-Lötscher/Sievi, Art. 7 N 99.

Blockchain gespeichert wird, wodurch die Authentizität der Daten nachweisbar wird.[117] Wird auf der Blockchain nur ein Hashwert gespeichert, so müssen die Dokumente vom Finanzintermediär aber anderweitig aufbewahrt werden. Denkbar wäre z.B. eine off-chain Aufbewahrung der Dokumentation.[118]

3.4. Delegation an Dritte

Der Beizug von Dritten im KYC-Verfahren für die Identifizierung der Vertragspartei sowie die Feststellung der wirtschaftlich berechtigten Person ist unter bestimmten Voraussetzungen erlaubt. Grundsätzlich kann ein Finanzintermediär einen Dritten mittels einer schriftlichen Vereinbarung mit Erfüllung der Sorgfaltspflichten im GwG beauftragen, wenn er die beauftragte Person sorgfältig auswählt, diese über ihre Aufgabe instruiert und kontrollieren kann, ob die beauftragte Person die Sorgfaltspflichten einhält oder nicht (vgl. Art. 28 Abs. 1 GwV-FINMA).[119] Auf eine schriftliche Vereinbarung kann hingegen grundsätzlich verzichtet werden, wenn der Finanzintermediär diese Pflichten einem anderen Finanzintermediär überträgt, sofern dieser einer gleichwertigen Aufsicht und Regelung in Bezug auf die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung untersteht und Massnahmen getroffen hat, um die Sorgfaltspflichten in gleichwertiger Weise zu erfüllen.[120] Auch wenn ein Finanzintermediär seine Pflichten aus dem GwG an einen Dritten delegiert, so bleibt er trotzdem verantwortlich für die pflichtgemässe Erfüllung dieser Pflichten.[121]

Auch die Dokumentationspflicht nach Art. 7 GwG kann ein Finanzintermediär grundsätzlich an einen Dritten delegieren. Demnach muss der Dritte die Belege und Unterlagen aufbewahren, welche zur Identifizierung der Vertragspartei sowie Feststellung der wirtschaftlich berechtigten Person im Rahmen des KYC-Verfahrens eingeholt wurden.[122]

V. zkKYC in DeFi

Im Folgenden wird untersucht, ob es aus rechtlicher Sicht möglich wäre, die gesetzlichen Anforderungen an ein KYC-Verfahren bei der Aufnahme einer neuen Geschäftsbeziehung durch einen Finanzintermediär im DeFi-Bereich mithilfe der ZKP-Technologie zu erfüllen.

1. Erfüllung der GwG-Pflichten mittels zkKYC

Eines der Hauptmerkale eines zkKYC-Verfahrens ist, dass keine Informationen über Personen offengelegt und hierzu auch keine Unterlagen wie z.B. Passkopie eingereicht werden müssen. Das Ziel von zkKYC besteht gerade darin, dass solche Personendaten eben nicht mehr ausgetauscht werden müssen. Dies widerspricht der heutigen Gesetzeslage sowie den Prinzipien in der Bekämpfung der Geldwäscherei in der Schweiz diametral. Wie oben ausgeführt wurde, sind Finanzintermediäre gesetzlich dazu verpflichtet, neue Kunden mit einem beweiskräftigen Dokument zu identifizieren (Art. 3 Abs. 1 GwG) und diese Dokumente auch aufzubewahren (Art. 7 GwG).[123] Hierzu steht den Finanzintermediären die persönliche Vorsprache mit einem amtlichen Identifikationsdokument, der Korrespondenzweg mit echtheitsbestätigter Kopie eines Identifikationsdokuments oder die digitale Identifizierung der Vertragspartei zur Verfügung.[124] Demnach ist die Anwendung eines zkKYC-Verfahrens für die Aufnahme einer Geschäftsbeziehung mit einem Kunden, ohne Identifizierung und ohne Dokumentation von beweiskräftigen Identifikationsunterlagen, nach aktueller Rechtslage im schweizerischen Geldwäschereibereich grundsätzlich nicht möglich.

Es wäre aber grundsätzlich denkbar, dass sich die ZKP-Technologie eines Tages so weit als Verifizierungs-Tool etabliert hat, dass der Zero-Knowledge Proof als Ersatz eines beweiskräftigen Dokumentes angesehen werden könnte. Davon ist aber der Schweizer Gesetzgeber sowie auch die internationale Gemeinschaft noch weit entfernt. So hat sich die Financial Action Task Force («FATF») erst kürzlich mit den Konsequenzen von Anonymisierungstechniken auf der Blockchain auseinandergesetzt und diese Techniken gemäss einem Bericht der FATF vom September 2020 als Red-Flag-Indikatoren im Geldwäschereibereich eingestuft.[125]

Zusammenfassend kann festgehalten werden, dass nach aktueller Gesetzeslage in der Schweiz ein zkKYC-Verfahren zur Erfüllung der GwG-Pflichten (Identifizierung der Vertragspartei sowie Feststellung der wirtschaftlich berechtigten Person) grundsätzlich nicht möglich ist. Nachfolgend werden alternative Lösungsansätze für mögliche Anwendungsbereiche von zkKYC aufgezeigt.

---

117 Stengel/Aus der Au (FN 59), 445.
118 BSK GwG-Lötscher/Sievi, Art. 7 N 99.
119 BSK GwG-Landolt/Gemperli, Art. 3 N 36.
120 Vgl. Art. 28 Abs. 2 GwV-FINMA; Art. 85 Abs. 2 lit. b VQF-Reglement.
121 SHK GwG-Dobrauz-Saldapenna/Derungs (FN 107), Art. 3 N 62.
122 BSK GwG-Lötscher/Sievi, Art. 7 N 17.
123 Vgl. Ziff. IV.3. vorstehend.
124 Vgl. Ziff. IV.3.1 vorstehend.
125 Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (fatf-gafi.org) (zuletzt besucht am 10. April 2023).

2. Alternative Lösungsansätze für die Anwendung von zkKYC

2.1. Compliance Orakel

Ein Lösungsansatz für eine Umsetzung von zkKYC in Übereinstimmung mit den heutigen GwG-Pflichten könnte sein, dass ein vertrauenswürdiges Unternehmen die für die Überprüfung eines Kunden erforderlichen Identitätsdokumente ausserhalb der Blockchain aufbewahrt und verifiziert, ohne die Originaldokumente offenlegen zu müssen (mittels Anwendung der ZKP-Technologie).

Das vertrauenswürdige Unternehmen könnte u.U. selbst als Finanzintermediär der GwG-Regulierung unterstehen und bei diesem Konzept als Orakel fungieren. Ein Orakel ist eine Brücke zwischen der Blockchain und der realen Welt und kann Informationen in die Blockchain übertragen, sodass diese im Smart Contract verwendet und/oder angepasst werden können.[126] Dies kann alles sein, von Informationen über Personen (Name, Geburtsdatum, Wohnort usw.) bis hin zu Vermögensausweisen. In diesem Fall würden die Daten der Kunden off-chain beim vertrauenswürdigen Unternehmen als sog. Compliance Orakel zentral abgespeichert werden. Durch die off-chain Datenspeicherung wären keine Rückschlüsse auf die Daten des Kunden über die Blockchain möglich. Sofern ein Finanzintermediär eine neue Geschäftsbeziehung mit einem Kunden aufnehmen möchte, könnte das vertrauenswürdige Unternehmen gegenüber dem Finanzintermediär über die Blockchain mittels Signatur verifizieren, dass bestimmte Informationen und Dokumente (Pass, Identitätskarte, Vermögensausweise usw.) bei ihm vorliegen und die Korrektheit bestätigen. Unter Anwendung der ZKP-Technologie könnte der Finanzintermediär als Verifizierer beim vertrauenswürdigen Unternehmen prüfen, ob die erforderlichen Informationen gemäss GwG vorliegen, ohne Einzelheiten über die Person erfahren zu müssen. Natürlich müsste auch bei diesem Lösungsansatz sichergestellt werden, dass der Finanzintermediär im Ernstfall auf die beim vertrauenswürdigen Unternehmen gespeicherten und abgelegten Dokumente jederzeit und uneingeschränkt Zugriff hat (z.B. bei Editionsbegehren in Strafverfahren).

Wie vorstehend aufgezeigt wurde, ist es gemäss schweizerischer Geldwäschereigesetzgebung grundsätzlich möglich, die Pflichten im KYC-Verfahren (Identifizierung der Vertragspartei sowie Feststellung der wirtschaftlich berechtigten Person) an einen Dritten mit Sitz in der Schweiz zu delegieren.[127] Hierbei ist aber zu beachten, dass auch wenn die GwG-Pflichten rechtlich an einen Dritten ausgelagert werden können, der Finanzintermediär für die Einhaltung der GwG-Pflichten verantwortlich bleibt, für die der Dritte beauftragt wurde.[128]

Aus diesem Grund ist es unter Berücksichtigung der aktuellen Gesetzeslage fraglich, ob sich ein Finanzintermediär auf die Bestätigung über das Vorliegen von Identifikationsdokumenten über einen neuen Kunden durch das vertrauenswürdige Unternehmen verlassen würde, ohne je Einsicht in diese Dokumente erhalten zu haben (so werden bei der Anwendung der ZKP-Technologie wie erwähnt keine Informationen offengelegt). Da schlussendlich der Finanzintermediär dafür verantwortlich ist, die GwG-Pflichten einzuhalten und den Kunden zu identifizieren, ist gemäss heutigem Stand zu bezweifeln, dass ein Finanzintermediär hierfür das zkKYC-Verfahren als genügend erachten würde. Hierfür müsste sich zuerst eine breite Akzeptanz der ZKP-Technologie etabliert haben, bevor ein Finanzintermediär eine neue Geschäftsbeziehung mit einem Kunden mittels zkKYC aufnehmen würde. Rechtlich sowie technisch wäre dies aber unter gegebenen Voraussetzungen grundsätzlich möglich und es gibt auch schon Unternehmungen, die auf dieses Ziel hinarbeiten.[129]

Trotz dieser Rechtsunsicherheiten sollen nachstehend kurz die Nachteile an der heutigen Gesetzeslage in Bezug auf KYC-Verfahren im GwG-Bereich sowie die möglichen Vorteile eines zkKYC-Verfahrens aufgezeigt werden.

Zunächst besteht ein grosser Nachteil an der heutigen Gesetzeslage darin, dass neue Kunden das KYC-Verfahren mit jedem neuen Finanzintermediär erneut durchlaufen müssen, da Finanzintermediäre untereinander keine Informationen austauschen dürfen, sodass jeder Kunde dieselben Informationen mehrmals offenlegen und einreichen muss. Des Weiteren handelt es sich bei den Finanzintermediären um ein zentralisiertes System, wobei jeder einzelne Finanzintermediär eine enorme Menge an personenbezogenen Daten über Kunden gesetzeskonform verwalten und aufbewahren muss. Die Einhaltung der Geldwäscherei- sowie der Datenschutzbestimmungen sind für Finanzintermediäre sehr zeit- und kostenintensiv. Zudem hat der Kunde keine Kontrolle darüber, wie diese Daten aufbewahrt und tatsächlich geschützt werden und ob alle gesetzlichen Bestimmungen vom Finanzintermediär auch effektiv eingehalten werden.

Mit dem zkKYC-Verfahren könnten diese Probleme gelöst werden, da der Kunde seine Identität hierbei nur einmal bei einem vertrauenswürdigen Finanzintermediär verifizieren müsste und dann seine Identität gegenüber anderen Finanzintermediären bestätigen könnte, ohne

---

126 Martin Hanzl, Handbuch Blockchain und Smart Contracts, Wien 2019, 13.

127 BSK GwG-Landolt/Gemperli, Art. 3 N 36 f.; vgl. Ziff. IV.3.4 vorstehend.

128 Stengel/Bianchi (FN 95), 248, Rz. 62.

129 Z.B. bietet die KYC Spider AG bereits solche Dienstleistungen im E-Commerce-Bereich an.

ständig seine persönlichen Daten erneut offenlegen zu müssen. Darüber hinaus würde sich für Finanzintermediäre das Risiko drastisch verringern, die gesetzlichen Pflichten zur Aufbewahrung von Dokumenten zu verletzen, da gar keine Informationen mehr offengelegt bzw. Dokumente aufbewahrt werden müssten. Schliesslich würden sich die Kosten und der Aufwand für die Aufbewahrung von Kundendaten um ein Vielfaches verringern.

2.2. Zugang zu vollständig dezentralen Infrastrukturen über regulierte Finanzintermediäre

Ein weiterer möglicher Anwendungsbereich von zkKYC wäre beispielsweise, wenn ein regulierter Finanzintermediär seinen Kunden den Zugang auf ein vollständig dezentrales DeFi-Protokoll ermöglichen möchte. Dies wäre der Fall, wenn z.B. eine regulierte Schweizer Krypto-Handelsplattform ihren Kunden über das von ihr zur Verfügung gestellte Custody-Wallet den Zugang zu einem vollständig dezentralen Liquidity Pool[130] (z.B. Uniswap) ermöglichen möchte. Es gibt regulatorische Tendenzen, welche darauf abzielen, dass Finanzintermediäre grundsätzlich jeden einzelnen Nutzer bzw. jede Adresse in einem solchen Liquidity Pool identifizieren müssen, bzw. dass sichergestellt ist, dass nur identifizierte Nutzer teilnehmen, bevor den eigenen Kunden der Zugang zu solchen DeFi-Protokollen gewährt werden darf. Der Gedanke dahinter ist wohl, dass Finanzintermediäre sicherstellen sollen, dass z.B. keine sanktionierten Personen oder kontaminierte Wallet-Adressen den gleichen Liquidity Pool verwenden und so kontaminierte Vermögenswerte in den ordentlichen Geldkreislauf gelangen können.

Auch hier könnte sich die Anwendung der ZKP-Technologie anbieten. So muss ein Finanzintermediär, welcher seinen Kunden den Zugang zu einem vollständig dezentralen DeFi-Protokoll gewähren möchte, grundsätzlich nicht jeden einzelnen Namen der Nutzer und/oder Adresse kennen, welche den Liquidity Pool nutzen. Für den Finanzintermediär wäre es theoretisch ausreichend, wenn er weiss, dass die anderen Nutzer und/oder Adressen eines DeFi-Protokolls nicht kontaminiert sind (z.B. nicht auf einer Sanktionsliste stehen). Unter Anwendung der ZKP-Technologie könnte der Finanzintermediär überprüfen, ob alle Nutzer eines Liquidity Pools identifiziert wurden und die Wallet-Adressen nicht kontaminiert sind, ohne Einzelheiten über die Person und/oder Wallet-Adressen erfahren zu müssen. Der Smart Contract des entsprechenden DeFi-Protokolls müsste allerdings technisch so aufgesetzt werden, dass nur identifizierte und verifizierte Personen und/oder Wallet-Adressen Zugang zum Liquidity Pool erhalten und dass diese Informationen durch andere Nutzer (z.B. Finanzintermediäre) mittels der ZKP-Technologie überprüft werden können. Die eigenen Kunden müsste der Finanzintermediär selbstverständlich weiterhin gesetzeskonform identifizieren und überprüfen.

Aber auch bei diesem Lösungsansatz stellen sich viele offene Rechtsfragen. Fraglich ist z.B., ob es überhaupt eine gesetzliche Grundlage dafür gibt, regulierte Finanzintermediäre aufgrund des GwG dazu zu verpflichten, sämtliche Nutzer und/oder Wallet-Adressen eines vollständig dezentralen DeFi-Protokolls identifizieren zu müssen und falls dies zu bejahen ist, ob diese Pflichten durch die Anwendung der ZKP-Technologie erfüllt werden könnten.

Zusammenfassend bleibt aber festzuhalten, dass es auch bei diesem Lösungsansatz letztlich offenbleibt, ob die Regulatoren einen ZKP als genügend erachten würden, damit regulierte Finanzintermediäre ihren Kunden den Zugang zu vollständig dezentralen DeFi-Protokollen ermöglichen können.

VI. Fazit und Ausblick

DeFi als ein Anwendungsfall der Blockchain-Technologie im Finanzsektor birgt neue Möglichkeiten, bringt aber auch neue Herausforderungen mit sich. So stehen die Eigenschaften von Blockchains (z.B. die Dezentralität oder die Unveränderbarkeit von Transaktionen) mit den Prinzipien des Datenschutzes (z.B. Recht auf Berichtigung) in einem grundsätzlichen Konflikt. Mit Zero-Knowledge Proofs gibt es eine neue Technologie, welche bei Transaktionen in Blockchains die Anonymität der Nutzer grundsätzlich gewährleisten kann. Die ZKP-Technologie könnte aber auch in KYC-Prozessen zur Anwendung kommen, um die Identität von Kunden zu überprüfen, ohne unnötige persönliche Daten sammeln und speichern zu müssen. Allerdings lassen es die heutigen Pflichten aus der Geldwäschereigesetzgebung grundsätzlich nicht zu, dass Finanzintermediäre eine neue Geschäftsbeziehung aufnehmen, ohne den Kunden anhand eines beweiskräftigen Dokumentes zu identifizieren. Aus diesem Grund dürfte der Anwendungsbereich von zkKYC im GwG-Bereich unter der heutigen Gesetzeslage begrenzt sein.

Im vorliegenden Aufsatz konnte allerdings aufgezeigt werden, dass bereits heute durchaus Anwendungsmöglichkeiten für zkKYC bestehen (z.B. Compliance Ora-

---

130 Liquidity Pools sind Pools für Krypto-Assets, die in einem Smart Contract blockiert sind und dezentralen Handelsplattformen die notwendige Liquidität zur Verfügung stellen; vgl. Alexander Wherlock/Daniel Haeberli, Use of liquidity pools on DEX and the application of Swiss regulations to liquidity tokens, IFLR vom 8. Dezember 2021, Use of liquidity pools on DEX and the application of Swiss regulations to liquidity tokens | IFLR (zuletzt besucht am 15. April 2023).

kel oder Zugang zu DeFi-Protokollen über regulierte Finanzintermediäre). Aber auch bei diesen Lösungsansätzen handelt es sich lediglich um theoretische Anwendungsbeispiele und es bleibt offen, wie Regulatoren auf die Anwendung der ZKP-Technologie in Zusammenhang mit DeFi-Anwendungen reagieren werden.

Abschliessend lässt sich festhalten, dass zkKYC-Verfahren das Potenzial haben, ein wertvolles Instrument für Unternehmungen zu werden, die ihre KYC-Prozesse verbessern und vereinfachen sowie gleichzeitig die Privatsphäre und Sicherheit ihrer Kunden besser schützen wollen. Mit der immer höheren Akzeptanz sowie Etablierung von Blockchain-Anwendungen im Finanzsektor darf man somit auf die zukünftigen Entwicklungen gespannt bleiben.

Aus Gründen der Praktikabilität und mit Blick in die Zukunft ist es notwendig, dass für eine erfolgreiche Bewältigung der geldwäschereirechtlichen Herausforderungen im Rahmen von DeFi die gemeinsame Nutzung eines Smart Contracts in den Vordergrund rückt. Dies würde bedeuten, dass der Application Layer (Layer 4) sowie Aggregation Layer (Layer 5) für finanzintermediäre Tätigkeiten und folglich die GwG-Pflichten als Anknüpfungspunkt dienen. Demnach würden diejenigen, welche Zugang zu DeFi ermöglichen, sei es durch ein webbasiertes Frontend zu einem Smart Contract (Layer 4), oder als Aggregatoren (Layer 5), welche durch benutzerorientierte Plattformen eine Verbindung zu mehreren DeFi-Anwendungen und Protokollen herstellen, für eine GwG-Unterstellung in Frage kommen. Natürlich unter der Voraussetzung, dass Verfügungsmacht besteht oder im Rahmen einer dauernden Geschäftsbeziehung bei der Übertragung von virtuellen Währungen Hilfe geleistet wird. Folglich würden Layer 4 bzw. Layer 5 Finanzintermediäre unter anderem die Pflicht haben, ihre Nutzer zu identifizieren. Je mehr Anbieter im 4. und 5. Layer Zugang zu DeFi-Anwendungen anbieten, umso mehr identifizierte Nutzer würde es geben. Mittels ZKP liesse sich verifizieren, ob ein Nutzer bereits eine Identifikation durchlaufen hat. Dieser Anwendungsfall von ZKP würde eine Nutzung von DeFi ermöglichen, welche gleichzeitig das Risiko minimiert, dass sanktionierte Nutzer es verwenden. Eines der Hauptargumente von Regulatoren gegen DeFi heutzutage ist nämlich, dass sanktionierte Nutzer DeFi derzeit ohne grosse Einschränkungen verwenden können, weil i.d.R. nicht bekannt ist, wer der Nutzer einer DeFi-Anwendung ist. Eine unrealistische Erwartung wäre es, die DeFi Nutzung zu verbieten, weil nicht alle Nutzer, welche mit einem Smart Contract interagieren, bekannt sind, oder gar zu fordern, dass ein einzelner Finanzintermediär alle Nutzer kennt. Es sollte darauf abgestellt werden, dass ein Finanzintermediär, welcher seinen Nutzern Zugang zu DeFi ermöglicht, seine Nutzer kennt.

Der heutige regulatorische Ansatz zu DeFi trifft keine ausreichende Unterscheidung, wenn es um mögliche Anknüpfungspunkte für die Regulierung von DeFi geht. Dies sorgt für Rechtsunsicherheit, was die Handhabung von DeFi betrifft. Zukünftige regulatorische Ansätze für DeFi sollten die Eigenheiten der neuen Technologie reflektieren und differenzierte, praktikable regulatorische Lösungsansätze für DeFi ermöglichen, ohne dadurch deren Innovationspotenzial zu hindern.