# Das Bitcoin Lightning Netzwerk – Einführung und rechtliche Einordnung von LNBTC und der Teilnahme am Netzwerk

Written by me@wordpress in AML, Blockchain, Crypto, FinTech, Money

*Der vorliegende Beitrag ist eine überarbeitete Fassung des in iusNet BR-KR 22.12.2022 erschienenen zweiteiligen Aufsatzes.*

Das Lightning Netzwerk ist eine technische Skalierungslösung für die Bitcoin Blockchain. Es bietet in erster Linie die Möglichkeit, effizient, kostengünstig und mit technischer Finalität bitcoins (BTC) in Form von Lightning bitcoins (LNBTC) zu übertragen. Das Lightning Netzwerk wird als eine der Schlüsselinfrastrukturen des heutigen Bitcoin Ökosystems betrachtet.

Trotz seiner zentralen Stellung hat das Netzwerk bisher nur vereinzelt

Beachtung in der juristischen Literatur gefunden.[1] Primär stellt sich in diesem Zusammenhang die Frage, ob das Lightning Netzwerk aufgrund seines Hauptzwecks als Zahlungsnetzwerk ein unterstellungspflichtiges Zahlungssystem darstellt oder ob die Teilnahme am Netzwerk einer regulierten Tätigkeit entspricht. Dabei ist v.a. die Anwendbarkeit des Geldwäschereigesetzes (GwG)[2], Finanzmarktinfrastrukturgesetzes (FinfraG)[3] und Bankengesetzes (BankG)[4] zu prüfen. Dieser Beitrag widmet sich demgegenüber nicht der Fragestellung, ob Dienstleister, die Kunden über ihre Wallet-Software Zugang zum Lightning Netzwerk verschaffen, gegebenenfalls eine unterstellungspflichtige Tätigkeit ausüben.

# I. Das Lightning Netzwerk

## A. Übersicht

Der Begriff «Lightning» steht je nach Blickwinkel für (i) ein Computerprotokoll bzw. mehrere solche Protokolle, (ii) eine Software-Implementierung (bzw. Client) des erwähnten Computerprotokolls oder (iii) das Netzwerk selbst, deren Teilnehmer den Code einer Software-Implementierung ausführen. Es bestehen mehrere voneinander unabhängige Open-Source-Implementierungen, die unterschiedliche Funktionalitäten aufweisen können, jedoch alle die Standards mit der Bezeichnung «Basis of Lightning Technology» (BOLT) einhalten.[5] Sowohl das Protokoll als auch die unterschiedlichen Implementierungen befinden sich in kontinuierlicher Weiterentwicklung durch eine globale Entwicklergemeinschaft.

Das Lightning Protokoll knüpft unmittelbar an das Bitcoin Protokoll an, wobei andere Blockchains ebenfalls vom Konzept Gebrauch machen können.[6] Entsprechend wird Lightning auch als «Second Layer» bzw. «Layer 2» von Bitcoin bezeichnet. Technisch betrachtet bedeutet dies, dass das Lightning Netzwerk im Wesentlichen das Sicherheits- und Vertrauensmodell des Bitcoin Netzwerks erbt, gleichzeitig aber eigenständige Funktionalitäten implementieren kann.[7] Lightning Transaktionen erfolgen anders als in Bitcoin «off-chain», d.h., Daten werden überwiegend ausserhalb der Bitcoin Blockchain verarbeitet und abgespeichert. Das Lightning Protokoll trägt dadurch den Kapazitätsgrenzen der Blockchain Rechnung.[8] Als Grundlage für Lightning Transaktionen dienen Zahlungskanäle, welche die Netzwerkteilnehmer in bidirektionaler Weise miteinander unterhalten (sog. *Payment Channels*). Befinden sich die BTC nach Eröffnung eines Zahlungskanals erst einmal im Netzwerk, findet die Abwicklung einer LNBTC-Übertragung innert weniger Sekunden statt. Eine (zusätzliche) Abwicklung auf der Bitcoin Blockchain ist für technische Finalität grundsätzlich nicht notwendig, kann aber bei Bedarf von jeder der beiden

an einem Kanal beteiligten Personen initiiert werden. Insoweit fungiert das verteilte Register von Bitcoin als ultimativer Abwicklungsmechanismus für Lightning.

Das Konzept hinter Lightning wurde bereits 2015 vorgestellt.[9] Seit 2018 ist das Netzwerk live. Kurz vor Veröffentlichung dieses Beitrags betrug die Netzwerkkapazität rund 5'000 BTC, d.h. rund 87 Millionen US-Dollar. Etwa 16'000 Netzwerkteilnehmer (sog. *Nodes*) betreiben rund 75'000 sichtbare Zahlungskanäle.[10] Mit anderen Worten unterhält ein Netzwerkteilnehmer in aller Regel mehr als einen Kanal.

Aufgrund des Charakters als offenes (d.h. *permissionless*) Netzwerk verändern sich Anzahl und Zusammensetzung der Teilnehmer laufend.[11] Eintritts- und Austrittsbarrieren sind rein technischer Natur, namentlich das Vorliegen eines Internetanschlusses. Das «Gatekeeper-Modell» traditioneller Zahlungsnetzwerke ist in Lightning obsolet bzw. technisch und spieltheoretisch substituiert.[12] Wer will, kann also nach der Lektüre dieses Beitrages eine Softwareimplementierung[13] des Protokolls herunterladen, diese auf dem privaten Computer zur Ausführung bringen und somit am Lightning Netzwerk partizipieren. Daraus lässt sich schliessen, dass das Netzwerk über keinen zentralen Betreiber verfügt. Zwar können sich aus mikroökonomischen Gründen einzelne «Hubs» bilden, welche als Knotenpunkte Zahlungskanäle mit dutzenden, ja hunderten oder sogar tausenden weiteren Teilnehmern unterhalten, doch sind auch solche Hubs technisch betrachtet letztlich gewöhnliche Netzwerkteilnehmer bzw. Nodes. Sie verfügen mit anderen Worten über keine besonderen Rechte, Privilegien und/oder Aufgaben innerhalb der Netzwerks. Dieser Punkt ist zentral für die rechtliche Einordnung von Lightning.

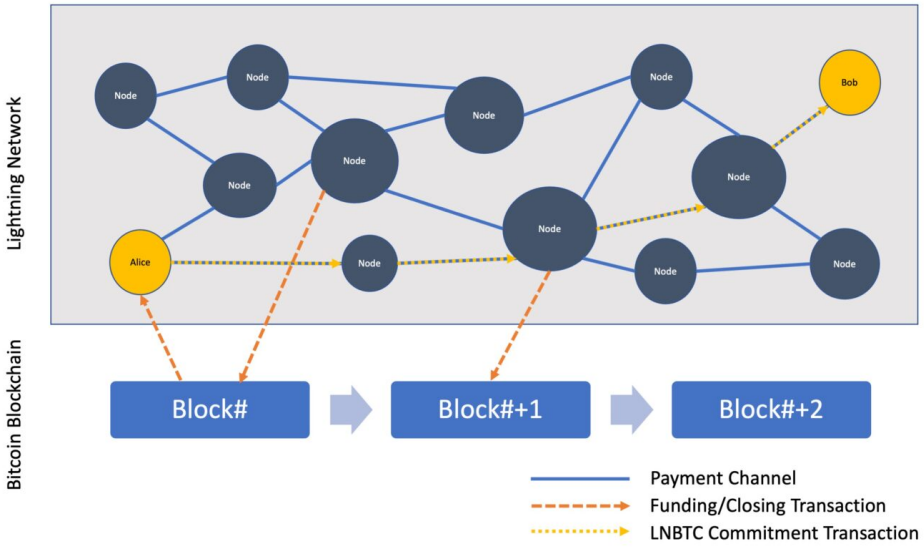
## B. Aufbau und Funktionsweise

Das Lightning Netzwerk weist mehrere Ebenen auf, die jeweils informationstechnisch miteinander verknüpft sind («von unten nach oben»):[14]

- *Netzwerkebene* zwecks Interaktion mit TCP/IP, Tor, DNS etc.;
- *Nachrichten-Ebene* zwecks Verhandlung etwa des Nachrichtenformats;
- *Peer-to-Peer (P2P)-Ebene* zwecks Kommunikation etwa der Öffnung und Schliessung von Zahlungskanälen;
- *Routing-Ebene* zwecks Übermittlung von Zahlungen zwischen Netzwerkteilnehmern;
- *Zahlungs-Ebene* zwecks Darstellung etwa von Zahlungsaufforderungen (sog. *Invoices*).

Das Lightning Protokoll führt keinen neuen «Coin» oder «Token» ein, sondern setzt auf die eingeschränkten Smart Contract-Fähigkeiten des Bitcoin Protokolls. Technisch vereinfacht dargestellt werden bereits bestehende BTC auf der Bitcoin Blockchain (d.h. on-chain) innerhalb von Smart Contracts «gesperrt». Als Folge entstehen LNBTC, welche technisch den gesperrten BTC entsprechen.[15] Die Sperrung ändert an den quantitativen Eigenschaften der betreffenden BTC nichts (z.B. 0.1 LNBTC = 0.1 BTC) und verhindert entsprechend bis zu ihrer Aufhebung, dass die gesperrten BTC auf der Bitcoin Blockchain übertragen werden können. Nichtjuristisch gesprochen können LNBTC am ehesten als «codiertes» Lieferversprechen für die gesperrten BTC beschrieben werden.

Als technische Primitive werden u.a. sog. *State Channels*, *Multisig-Adressen* und *Hash-Time Lock(ed) Contracts (HTLCs)* verwendet.[16] Lightning etabliert mithilfe dieser Primitive topologisch ein *Multi-Hop*-Netzwerk aus unzähligen Zahlungskanälen, deren primärer Zweck in der Weiterleitung von LNBTC-Zahlungen besteht. An einem einzelnen Zahlungskanal sind immer (und maximal) zwei Netzwerkteilnehmer beteiligt.




Wie bereits erwähnt, erhalten Netzwerkteilnehmer durch die Ausführung einer Software-Implementierung des Lightning Protokolls die Möglichkeit, Zahlungskanäle mit anderen Nodes zu eröffnen (sog. *Funding Transactions*). Einmal eröffnete Zahlungskanäle können hiernach dazu verwendet werden, LNBTC an Netzwerkteilnehmer zu übertragen bzw. solche von Netzwerkteilnehmern zu empfangen sowie LNBTC im Netzwerk zu routen (sog. *Commitment Transactions*). Während die Eröffnung eines Zahlungskanals on-chain auf der Bitcoin Blockchain erfolgt und dort zu einem sog. *Shared State* der am Zahlungskanal beteiligten Parteien führt, wird der Zahlungskanal von den Teilnehmern off-chain innerhalb des Lightning Netzwerks unterhalten. Zahlungskanäle

werden schliesslich on-chain entweder kooperativ oder durch technisches Erzwingen einer der beiden Netzwerkteilnehmer geschlossen (sog. *Closing Transactions*).[17] Die Schliessung eines Zahlungskanals auf der Bitcoin Blockchain kann mit dem im traditionellen Finanzsystem existierenden «Batching» von Handels- oder Zahlungsaufträgen zu bestimmten Tageszeitpunkten basierend auf dem Nettoprinzip verglichen werden.

Typischerweise initiiert der Empfänger einer Zahlung die Transaktion mit dem Absender. Absender und Empfänger müssen einen Zahlungskanal nicht direkt miteinander unterhalten, sondern können für eine Übertragung auch Kanäle anderer Netzwerkteilnehmer in Anspruch nehmen (sog. *Routing*). Zu diesem Zweck erstellt der Empfänger eine Zahlungsaufforderung (sog. *Invoice*), welche einen sog. *Payment Hash* beinhaltet, der dafür verantwortlich ist, dass die vom Absender ausgelöste Zahlung tatsächlich beim Empfänger ankommt.[18] Der Zahlungsprozess erfolgt informationstechnisch gesehen in *atomistischer* Weise (sog. *Atomic Swaps*). D.h., es kommt entweder zur erfolgreichen Übertragung an den intendierten Empfänger oder es kommt gar keine Übertragung zustande (auch nicht an eine dazwischengeschaltete Node). Teilübertragungen sind somit technisch ausgeschlossen.[19] Bei erfolgreichem Routing werden auch alle vom Routing tangierten Zahlungskanäle aufgrund einer entsprechenden Commitment Transaction automatisch aktualisiert. Kanalbetreiber veranschlagen für das Routing von Transaktionen eine (in aller Regel sehr geringe) Gebühr, deren Höhe – gleich wie das sog. *Mining* der Bitcoin Blockchain – der Logik eines Anbietermarkts folgt.[20]

Die on-chain gesperrten BTC dienen als Vermögenswerte im Lightning Netzwerk. Übertragungen bzw. Transaktionen werden vom Lightning Protokoll *ad hoc* an den beabsichtigten Empfänger geroutet. Die Teilnehmer des Netzwerks haben im Rahmen des Routings keine Zugriffmöglichkeit auf die Vermögenswerte der übrigen Teilnehmer des Netzwerks.[21] Selbst die eigenen BTC, deren Private Key vollumfänglich und ausschliesslich sie kontrollieren, sind ihnen bis zur Schliessung des Zahlungskanals «vorenthalten». Netzwerkteilnehmer haben aufgrund der Verschlüsselung der Transaktionsdaten ferner auch keine Kenntnis über den ursprünglichen Absender und den finalen Empfänger einer Zahlung (sog. *Onion Routing*).[22]

## C. Nutzungsformen

Wie eingangs erwähnt, ist die Nutzung des Lightning Netzwerks relativ niederschwellig möglich. Die dafür erforderlichen technischen Kenntnisse und Hardware-Anforderungen sind je nach Nutzungsart unterschiedlich.[23] Im Wesentlichen können zwei Formen der Nutzung unterschieden werden, wobei Mischformen in der Praxis existieren:

- Nutzer können einerseits selbständig eine Lightning Node betreiben. Diese Form der Nutzung kann als eigentliche bzw. direkte Teilnahme am Netzwerk bezeichnet werden. Nutzer halten in diesem Fall die verwendeten BTC bzw. LNBTC in einem Wallet, dessen Private Key sie selbst kontrollieren (sog. *Self-Hosted* bzw. *Non-Custodial Wallets*). Sie signieren Transaktionen mit dem Private Key und versenden sie sodann selbständig an das Netzwerk. Sie verwalten in der Regel auch die Zahlungskanäle und sind gegebenenfalls für weitere Aspekte des Protokolls selbst verantwortlich. Die Nutzung erfolgt typischerweise entweder über einen stationären Computer (z.B. «myNode» oder «Umbrel») oder eine Wallet-Applikation (z.B. «Phoenix») auf dem Mobiltelefon.
- Demgegenüber greifen Nutzer, die keine Lightning Node betreiben wollen oder können, auf die Dienste von Drittpersonen zurück, die ihrerseits eine Node betreiben. Typischerweise werden in diesem Fall Wallet-Anbieter verwendet, welche in unterschiedlichem Ausmass die technische Komplexität für die Nutzer abstrahieren. Eine solche Applikation wird typischerweise auf dem Mobiltelefon (z.B. «BlueWallet») oder webbasiert innerhalb des Internetbrowsers ausgeführt. Solche Wallet-Anbieter führen zum Zweck der technischen Auslösung von Transaktionen für ihre Kunden im Wesentlichen zwei Wallet-Typen:
    - Im Falle von Self-Hosted Wallets übernimmt der Wallet-Anbieter in der Regel lediglich die technische Auslösung einer Transaktion; er verfügt hingegen nicht über den Private Key des Nutzers.
    - Im Falle von sog. *Hosted* bzw. *Custodial Wallets* kontrolliert der Wallet-Anbieter darüber hinaus auch den Private Key. In letzterem Fall signiert der Wallet-Anbieter die Transaktion für seinen Kunden mit dem Private Key, nachdem dieser den Service Provider rechtsgeschäftlich zur Signierungshandlung instruiert hat.

Nutzer, die keine eigene Node betreiben, sind mit anderen Worten auf die Dienste eines Wallet-Anbieters angewiesen, müssen jedoch diesen nicht zwingend die Verwahrung der Vermögenswerte anvertrauen. Neben der technischen Auslösung von Transaktionen bieten solche Anbieter den Nutzern regelmässig auch die Verwaltung der Zahlungskanäle und weitere Dienstleistungen an.

| Übersicht der Nutzungsformen *(vereinfacht)* |
| --- |

| | «Teilnahme» am Netzwerk | «Nutzung» des Netzwerks | |
|---|---|---|---|
| Lightning Node | Eigene Node | Fremde Node | |
| Aufbewahrung Private Key | Nutzer | Nutzer | Wallet-Anbieter |
| Auslösung von Transaktionen | Nutzer | i.d.R. Wallet-Anbieter | Wallet-Anbieter |
| Verwaltung Zahlungskanäle (usw.) | i.d.R. Nutzer | Wallet-Anbieter | Wallet-Anbieter |

## D. Herausforderungen

Die direkte Teilnahme am Lightning Netzwerk ist mit gewissen Anstrengungen verbunden:

- Eine Node hat einerseits immer online zu sein, um mögliche Betrugsversuche im Rahmen der Schliessung von Zahlungskanälen durch die Gegenseite abwehren zu können. In der Praxis schaffen sog. *Watchtowers* Abhilfe, an welche die Beobachtung und Sanktionierung solcher Handlungen delegiert werden können.[24]
- Andererseits ist je nach den mit dem Betrieb einer Node verfolgten Ziele darauf zu achten, dass die Zahlungskanäle liquiditätsmässig so verwaltet werden, dass eingehende und ausgehende Transaktionen kontinuierlich möglich sind.[25]
- Generell ist es wichtig, dass die Node innerhalb des Netzwerks eine verlässliche Anbindung geniesst, damit Transaktionen ihren Weg ans Ziel finden.[26]
- Ferner muss auch beachtet werden, dass die im Smart Contract gesperrten BTC permanent online sind, was im Extremfall eines Cyberangriffs zum Verlust der Kryptovermögenswerte führen kann.[27]
- Programmier- und Designfehler können schliesslich nie vollständig ausgeschlossen werden, wie praktische Erfahrungen zeigen.[28] Wie immer bei Software sind darum regelmässige Aktualisierungen und Verbesserungen notwendig.

Nach dem Gesagten ist klar, dass die Komplexität der direkten Teilnahme am Lightning Netzwerk nicht zu unterschätzen ist. Entsprechend nehmen viele Nutzer die Dienstleistungen von Wallet-Anbietern in Anspruch.

# E. Anwendungsgebiete und Ausblick

Aufgrund der Nähe zu Bitcoin ist es wenig überraschend, dass Lightning in erster Linie ein globales Zahlungs- bzw. Transaktionsnetzwerk darstellt. Dabei sind die Entwicklungsmöglichkeiten zahlreich: So können Händler LNBTC genauso wie BTC oder Fiatwährungen als Zahlungsmittel für ihre Waren und Dienstleistungen akzeptieren. Sodann bestehen Anwendungen im Mikrozahlungsbereich, die namentlich das Geben von Trinkgeldern an Twitter-Nutzer (z.B. «tippin.me»), das Bezahlen von Streaming- (z.B. über «Breez») oder von Social-Media-Inhalten (z.B. «Sphinx») ermöglichen.

Ferner erlauben die technischen Primitive von Lightning die Etablierung vollständig dezentralisierter Handelsplattformen. Mithilfe der zugrundeliegenden Smart Contracts können etwa LNBTC gegen andere Kryptovermögenswerte in atomistischer Weise und ohne Rückgriff auf einen Intermediär, der für die Handelsparteien die Vermögenswerte vorhält, getauscht werden.[29]

Schliesslich wird sodann mit «Taro» ein Protokoll entwickelt, das die Herausgabe und Übertragung realer Vermögenswerte, wie etwa von Stablecoins, Aktien und Rechten an Kunstwerken in Form von Non-Fungible Tokens (NFTs), über das Lightning Netzwerk realisieren will.[30] Taro greift somit das Bedürfnis der Tokenisierung von Vermögenswerten auf, die auf anderen Blockchains, wie namentlich Ethereum, bereits grosse Verbreitung gefunden hat. Ähnlich zu früheren Protokollen, wie etwa «Colored Coins»[31] oder «Counterparty»[32], nutzt Taro die Bitcoin Blockchain für die Herausgabe von Vermögenswerten, setzt aber neu für deren Übertragung auf das Lightning Netzwerk. Ein Grossteil der für die Identifikation der tokenisierten Vermögenswerte notwendigen Informationen speichert Taro off-chain und somit in effizienter Form ausserhalb der Bitcoin Blockchain ab.[33] Neben einer Taro-fähigen Wallet ist typischerweise eine weitere Voraussetzung für einen erfolgreichen Versand und Empfang der tokenisierten Vermögenswerte, dass darauf ausgerichtete Lightning Nodes eine Übersetzung bzw. Rückübersetzung zu LNBTC sicherstellen.[34] Im Übrigen folgen Taro-basierte Transaktionen denselben Regeln wie herkömmliche LNBTC-Transaktionen. Sie sind insbesondere atomistisch. Allerdings erkennen in der Regel gewöhnliche Lightning Routing Nodes nicht, dass eine spezifische LNBTC-Transaktion die Übertragung eines tokenisierten Vermögenswerts (mit)beinhaltet. Taro soll darum mehr Privatsphäre im Vergleich zu den erwähnten Vorläuferprotokollen gewährleisten.

Solche und weitere Applikationen auf Lightning machen deutlich, dass das Netzwerk letztlich als *Infrastruktur* für davon unabhängige Geschäftsmodelle fungiert. Lightning ermöglicht wie Bitcoin aufgrund

offener Standards die freie und interoperable Innovation. Solche offenen Systeme sind – anders als die meisten proprietären Systeme der heutigen Finanzwelt – gegenüber dem konkreten Verwendungszweck «agnostisch».

# II. Rechtliche Einordnung

## A. Qualifikation von LNBTC

### 1. Einleitung

Der erste Teil der rechtlichen Einordnung des Lightning Netzwerks befasst sich mit der finanzmarktrechtlichen Qualifikation von LNBTC unter Berücksichtigung der zu sog. *Initial Coin Offerings (ICOs)* entwickelten Praxis der FINMA.

### 2. Keine Effekte

Als Effekten i.S.v. Art. 2 lit. b FinfraG i.V.m. Art. 2 Abs. 1 FinfraV gelten vereinheitlichte und zum massenweisen Handel geeignete Wertpapiere, Wertrechte, insbesondere einfache Wertrechte nach Art. 973c OR und Registerwertrechte nach Art. 973d OR, sowie Derivate und Bucheffekten. Effekten gelten als vereinheitlicht und zum massenweisen Handel geeignet, wenn sie in gleicher Struktur und Stückelung öffentlich angeboten oder bei mehr als 20 Kunden platziert werden, sofern sie nicht für einzelne Gegenparteien besonders geschaffen werden. Der Effektenbegriff hat somit eine formale (Erscheinungsform) und eine inhaltliche Seite (Recht). Die Rechte haben zudem einen Bezug zum *Kapitalmarkt* aufzuweisen.[35]

Anlage-Token treten nach der Praxis der FINMA insbesondere im wertpapierrechtlichen Kleid des (einfachen) Wertrechts (bzw. neu des Registerwertrechts) auf. Zudem weisen Anlage-Token einen Anlagezweck auf.[36] Ein rein subjektiver spekulativer Erwerbszweck des Tokeninhabers, der sich eine Preissteigerung erhofft, genügt für sich alleine nicht, um den Anlagezweck zu begründen (so werden namentlich auch Bitcoin, gute Bordeaux-Rotweine und Oldtimer-Fahrzeuge mit ähnlicher Motivation erworben und gehalten). Anlage-Token sind nach Auffassung der FINMA Effekten.[37] Allerdings sind Anlage-Token ohne Effektennatur ohne Weiteres denkbar (z.B. für einzelne Gegenparteien besonders geschaffene Derivate[38] oder tokenisierte «physische Wertgegenstände»[39], die nicht dem Kapitalmarkt zuzuordnen sind).[40] Obschon für die FINMA die wirtschaftliche Funktion eines Token im Vordergrund steht,[41] weist der gesetzliche Effektenbegriff eindeutige Konturen auf: Auf jeden Fall muss im Token ein Recht verkörpert sein, das Ausfluss einer rein privatautonom – explizit oder implizit – geregelten oder aber gesetzlichen Rechtsbeziehung (z.B. tokenisierte Aktie) ist. Die

Rechtsbeziehung manifestiert sich darin, dass ein Token dann nicht als Effekte qualifiziert, wenn die Existenz der Emittentin eine Bedingung für die Durchsetzbarkeit des Rechtsanspruchs darstellt. Letztlich ist darum grundsätzlich weiterhin – und damit kumulativ – von der Notwendigkeit eines (irgendwie gearteten) Rechtsanspruchs (gegen eine irgendwie geartete Rechtspersönlichkeit oder Gruppe von Rechtspersönlichkeiten) auszugehen.[42] Der Wert eines solchen emittentenspezifischen Tokens leitet sich im Wesentlichen aus der operativen Tätigkeit des Emittenten oder aus dem Wert der vom Emittenten gehaltenen Vermögenswerte (z.B. Grundstücke) ab. Allerdings sind Token, die ein Recht verkörpern, aber *keinen* Anlage- oder Finanzierungszweck aufweisen, gerade im Zahlungsmittelbereich ohne Weiteres vorstellbar (z.B. ein Stablecoin in Form einer Publikumseinlage oder Schuldverschreibung). Zusammenfassend müssen Anlage-Token nicht nur einen Anlage- bzw. Finanzierungszweck und somit einen Kapitalmarktbezug aufzuweisen, sondern vom Herausgeber auch mit einem Recht verbunden werden. Darüber hinaus muss für das Vorliegen einer Effekte das Recht bzw. der Anspruch fungibel und somit (frei) übertragbar bzw. handelbar sein, andernfalls fehlt es an der Eignung zum massenweisen Handel i.S.v. Art. 2 lit. b FinfraG.[43]

LNBTC stellen namentlich aus zwei Gründen keine Effekten dar: Erstens verkörpern LNBTC keine Rechte, auch nicht zwischen den an einem Kanal beteiligten Personen. Die an einem Kanal beteiligten Nodes wissen regelmässig nicht um die Identität der anderen Seite; gleichzeitig fehlt es auch am Willen, sich rechtlich zu binden. Mit anderen Worten, vorbehaltlich besonderer Vereinbarungen, kommt trotz technischer Nähe kein Vertragsverhältnis zwischen den Node-Betreibern zustande. Ohne besondere Vorkehrungen verbinden sich Nodes zufälligerweise nach den im Protokoll vorgegebenen Regeln.[44] Unter diesen Umständen ist regelmässig nicht vom Vorliegen eines Rechts bzw. Anspruchs auszugehen. Zweitens ist mit LNBTC kein Anlage- und/oder Finanzierungszweck[45] verbunden, wie er insbesondere mit der Ausgabe und dem Erwerb von Aktien und Obligationen verfolgt wird. Es fehlt somit an einem Kapitalmarktbezug, wie er für den Effektenbegriff vorauszusetzen ist.

### 3. Kein Derivat

Derivate oder Derivatgeschäfte i.S.v. Art. 2 lit. c FinfraG i.V.m. Art. 2 Abs. 2 FinfraV sind Finanzkontrakte, deren Wert von einem oder mehreren Basiswerten abhängt und die kein Kassageschäft darstellen. Es handelt sich dabei um bilaterale Verträge, deren Preis von (i) Vermögenswerten, wie Aktien, Obligationen, Rohstoffen und Edelmetallen, oder (ii) Referenzwerten, wie Währungen, Zinsen und Indizes, abgeleitet wird. Die derivative Komponente besteht in der Regel aus einer Termin- oder Optionskomponente.[46] Bei lediglich *teilweisem* Vorliegen eines

derivativen Elements bei einem Finanzinstrument ist hingegen regelmässig nicht von einem Derivatkontrakt auszugehen (so z.B. Wandelanleihen).[47] Nicht als Derivate gelten u.a. Kassageschäfte und somit Geschäfte, die innerhalb kurzer Frist abgewickelt werden (Art. 2 Abs. 3 lit. a und Abs. 4 FinfraV). Ebenso wenig gelten als Derivate Konstrukte rechtlicher oder faktischer Natur, die ein bestehendes Recht lediglich abbilden, repräsentieren bzw. spiegeln.[48] Das derivative Finanzinstrument muss sodann nach richtiger Auffassung seinerseits handelbar sein, so dass parallel ein Markt für das Derivat und den Basiswert existiert. Die beiden Märkte, die eine gewisse Liquidität und somit regelmässige Preisstellung aufweisen müssen, bedingen und beeinflussen sich gegenseitig.[49]

Derivate können sodann als Effekten qualifizieren, wenn sie vereinheitlicht und zum massenweisen Handel geeignet sind. Letztlich verkörpern Derivate mit Effektenqualität ein Forderungsrecht gegenüber dem Emittenten des Finanzinstruments.[50]

Es ist nicht ausgeschlossen, dass Token bzw. der ihnen zugrundeliegende Smart Contract einen «handelbaren Leistungsanspruch»[51] bzw. sogar ein gesamtes Vertragsverhältnis[52] abbilden und somit ein Derivatgeschäft darstellen. Hinsichtlich LNBTC fehlt es allerdings bereits an der Verkörperung eines Rechtsanspruchs. Denn LNBTC sind, wie unten noch ausgeführt wird, BTC gleichzustellen; es handelt sich bei ihnen namentlich um BTC, die in einem Smart Contract gesperrt sind. In diesem Sinne werden die gesperrten BTC durch die LNBTC lediglich «gespiegelt». LNBTC weisen sodann keine vertraglichen Konditionen auf, wonach ihr Preis von der gegebenenfalls zeitlich bedingten Preisentwicklung von BTC abgeleitet wird. Da es sich in beiden Fällen letztlich um *dieselbe* Kryptowährung handelt, fehlt es bereits an einem Basiswert und somit an einer derivativen Komponente. Hinzukommt auch, dass in vertraglicher Hinsicht weder eine Termin- noch eine Optionskomponente besteht.

Die Annahme, dass zwischen den an einem Kanal beteiligten Nodes ein (auf Dauer angelegtes) bilaterales Derivatgeschäft zustande kommt, ist nach vorliegender Ansicht ebenfalls abzulehnen. Namentlich ist das Bestehen von vertraglichen Leistungspflichten, deren Wert von einem Basiswert abhängt, nicht gegeben.[53] Das Lightning Protokoll vermittelt den Netzwerkteilnehmern keine Ansprüche gegenüber anderen Teilnehmern beispielsweise auf Lieferung von BTC oder einen allfälligen Barausgleich zwischen LNBTC und BTC. Die Routing-Gebühren stehen sodann ohne besondere Vorkehrungen in einer Beziehung zum gerouteten Transaktionswert (und nicht etwa zu einem allfälligen Basiswert).[54] Bei Bedarf können die gesperrten BTC durch eine entsprechende Closing Transaction lediglich wieder on-chain verfügbar

gemacht werden. Die entsperrten BTC werden in diesem Fall nicht von dem am Kanal beteiligten Netzwerkteilnehmer oder einem Dritten geliefert, sondern entsprechend dem Kontostand gemäss letzter Commitment Transaction durch den betreffenden Lightning Node-Betreiber selbst «ausgelöst».

Schliesslich verfolgen Inhaber von LNBTC in aller Regel keine für Derivatgeschäfte typische Strategien, wie etwa das Hedging, die Arbitrage oder die Spekulation bzw. Kapitalanlage.[55]

4. Kein Stablecoin

Es drängt sich in einem weiteren Schritt die Abgrenzung auf zwischen herkömmlichen Zahlungs-Token (siehe sogleich) und Token mit Zahlungsmittelcharakter, die Rückzahlungs- bzw. Einlösungs- oder Herausgabeansprüche der Inhaber verkörpern, namentlich in Form von «Stablecoins».[56] Nach der Auffassung der FINMA werden Stablecoins, indem sie in irgendeiner Form an einen möglichst preisstabilen Vermögenswert angebunden werden, mit dem Ziel der erhöhten Wertstabilität ausgegeben.[57]

LNBTC ist nach vorliegender Auffassung kein Stablecoin, für welchen ein «alternativer Stabilisierungsmechanismus»[58] besteht, denn die «Spiegelung» von LNBTC mit BTC bezweckt nicht die Wertstabilität des Token.

5. Vorliegen eines Zahlungs-Tokens

Bei den durch das Lightning Protokoll verfügbar gemachten LNBTC handelt es sich technisch gesehen um BTC.Die Funding und Closing Transactions sind letztlich gewöhnliche On-chain-Transaktionen mit BTC. Die Verwendung eines entsprechenden Skripts führt zur «Sperrung» der an die Multisig-Adresse übertragenen BTC bzw. der entsprechenden «Unspent Transaction Outputs» (UTXOs). Mit «gesperrt» ist gemeint, dass die an einem Zahlungskanal beteiligten Personen nicht anderweitig über die BTC on-chain oder off-chain (z.B. für die Eröffnung eines weiteren Kanals) verfügen können. Die gesperrten BTC sind lediglich im Rahmen des eröffneten Zahlungskanals verwendbar. Die Sperrung geht darum logischerweise auch nicht mit einer Ausweitung der BTC-Geldmenge einher (z.B. durch Teildeckung der gesperrten BTC).[59]

Der Kategorie der Kryptowährungen bzw. Zahlungs-Token werden gemäss FINMA-Praxis Token zugeordnet, die tatsächlich oder der Absicht des Organisators nach als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen akzeptiert werden oder der Geld- und Wertübertragung dienen sollen. Solche Token vermitteln keine Ansprüche (und somit Rechte) gegenüber einem Emittenten.[60]

Bei LNBTC handelt es sich letztlich um gesperrte BTC, die nach den Regeln des Lightning Protokolls zu übertragen sind. Sie sind vereinfacht gesagt ein «technisches Beweisstück» für die gesperrte Position, das seinerseits aber übertragbar ist. Wer protokollbedingt über die LNBTC verfügt, kann die entsprechenden BTC bei Bedarf wieder «freischalten». Ferner weisen sie denselben Zahlungscharakter wie BTC auf. LNBTC ermöglichen darum ebenfalls den Erwerb von Waren und Dienstleistungen und/oder die Geld- und Wertübertragung. Die im ersten Teil des Beitrages angeführten Anwendungsgebiete veranschaulichen dies.

### 6. Zwischenfazit

LNBTC entstehen durch die Sperrung von BTC in einem Smart Contract auf der Bitcoin Blockchain. LNBTC sind technisch betrachtet BTC, die in erster Linie den Regeln des Lightning Protokolls folgen. Es kann somit festgestellt werden, dass LNBTC ebenfalls als herkömmliche Zahlungs-Token qualifizieren.

## B. Teilnahme am Lightning Netzwerk

### 1. Einleitung

Der zweite Teil der rechtlichen Einordnung des Lightning Netzwerks befasst sich mit dem Betrieb einer Lightning Node und damit der direkten Teilnahme am Netzwerk. Es wird demgegenüber nachfolgend nicht auf den Anwendungsfall eingegangen, dass das Lightning Netzwerk für die Herausgabe und Übertragung von Finanzinstrumenten oder Effekten eingesetzt wird. Ebenfalls nicht Gegenstand dieses Beitrages ist die Qualifikation der Tätigkeiten von Wallet-Anbietern, die den Private Key von Nutzern aufbewahren und/oder Transaktionen technisch für Kunden auslösen.

### 2. Mögliche Anknüpfungskriterien

Die schweizerische Finanzmarktregulierung weist heute grundsätzlich eine Mischung aus Personen- und Aktivitätsbezogenheit auf: Die relevante Aktivität muss von einer Person oder Gruppe miteinander verbundener Personen ausgehen.[61] Technologie, Software und somit Smart Contracts als solche sind grundsätzlich nicht Gegenstand der Anknüpfung der Finanzmarktregulierung.[62] Ein (allzu) technologiespezifischer Ansatz würde ein Bruch mit überkommenen Regulierungsprinzipien darstellen. In praktischer Hinsicht liegt aber jedem Regulierungsentscheid eine implizite technologische Wertung zugrunde.[63]

Der Betrieb einer Lightning Node hat in finanzmarktrechtlicher Hinsicht insbesondere gewisse Ähnlichkeiten mit:

- der *Ausgabe eines Zahlungsmittels* (Verfügbarmachung von LNBTC durch die Sperrung von BTC in Smart Contracts);
- dem *Betrieb eines Zahlungssystems* (Teilnahme am Netzwerk als eine Node und Routing von Zahlungen);
- dem *Geld- oder Wertübertragungsgeschäft* (Routing von Zahlungen);
- der *Hilfe bei der Übertragung virtueller Währungen an Drittpersonen* (Routing von Zahlungen);
- der *Entgegennahme von Publikumseinlagen* (Eröffnung eines Zahlungskanals und Routing von Zahlungen).

3. Ausgabe eines Zahlungsmittels i.S.d. GwG

Die Sperrung von BTC in Smart Contracts zwecks Verfügbarmachung von LNBTC hat Ähnlichkeiten mit der geldwäschereirechtlich relevanten Ausgabe eines Zahlungsmittels.

Der Betrieb eines Zahlungssystems (siehe hierzu unten) ist grundsätzlich von der Ausgabe eines Zahlungsmittels i.S.v. Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. c GwV i.V.m. FINMA-RS 11/1, Rz. 63 ff. zu unterscheiden. Als nicht in Bargeld bestehende Zahlungsmittel gelten insbesondere Kreditkarten, Reisechecks und virtuelle Währungen, die tatsächlich oder nach der Absicht des Organisators oder Herausgebers als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen eingesetzt werden oder der Geld- und Wertübertragung dienen (Art. 4 Abs. $1^{bis}$ GwV).

Die mit der Eröffnung eines Zahlungskanals (Funding Transaction) verbundene Verfügbarmachung von LNBTC ist nach vorliegender Auffassung nicht als die Ausgabe von LNBTC aufzufassen. Die Ausgabe muss sachlogisch eine Erhöhung der Umlaufmenge des betreffenden Zahlungsmittels zur Folge haben.[64] LNBTC stellen jedoch lediglich in einer Multisig-Adresse gesperrte BTC dar, welche vom verteilten Bitcoin Netzwerk *bereits* ausgegeben worden sind. Augenscheinlich sind sodann die Betreiber einer Lightning Node nicht für die Ausgabe von BTC verantwortlich. BTC werden ausschliesslich im Rahmen des Konsensmechanismus («Mining») durch die Teilnehmer des Bitcoin Netzwerks geschöpft.[65] Das Bitcoin Netzwerk bzw. die einzelnen Netzwerkteilnehmer gelten nach überwiegender Auffassung in der Lehre indessen nicht als mit gemeinschaftlichem Rechtsbindungswillen agierender Emittent von BTC.[66]

Sollte man zur Auffassung gelangen, dass bei Eröffnung eines Zahlungskanals ein Zahlungsmittel ausgegeben wird, so könnte ein Node-Betreiber in Analogie zu Kreditkartensystemen als nichtunterstellter Acquirer (im Gegensatz zum unterstellten Issuer)

qualifiziert werden.[67] Das Bitcoin Netzwerk bzw. dessen Teilnehmer wären sodann als «Issuer» zu qualifizieren, was aber aus dem oben erwähnten Grund als nicht zielführend zu erachten ist.

### 4. Betreiben eines Zahlungssystems i.S.d. GwG

#### a) Vorbemerkungen

Die Teilnahme am Lightning Netzwerk durch den Betrieb einer Node inklusive Routing von Drittzahlungen könnte als geldwäschereirechtlich relevantes Betreiben eines Zahlungssystems qualifiziert werden.

Fehlt es an der Ausgabe eines Zahlungsmittels (siehe hierzu oben), stellt sich die Frage, ob damit überhaupt noch ein Zahlungssystem vorliegen kann. Die FINMA spricht davon, dass der Begriff des Zahlungsmittels «in Ergänzung zu den Zahlungssystemen verstanden werden» soll.[68] Ob damit kumulativ die Ausgabe eines Zahlungsmittels und der Betrieb eines Zahlungssystems vorauszusetzen sind, scheint nicht ganz klar zu sein. Aus der ICO-Wegleitung der FINMA ergibt sich jedoch, dass die Aufsichtsbehörde *bereits* die Ausgabe von Zahlungs-Token, die auf einer Blockchain-Infrastruktur übertragen werden können, als unterstellungspflichtige Tätigkeit auffasst.[69]In der Literatur wird hingegen geltend gemacht, dass die Ausgabe eines Zahlungsmittels für sich alleine noch nicht als finanzintermediäre Tätigkeit qualifiziert, sondern darüber hinaus auch eine gewisse Involvierung des Emittenten in den Zahlungsabwicklungsprozess zwischen Vertragspartei und Dritten notwendig ist.[70] Für Lightning ist der Schwerpunkt jedoch eher beim (blossen) Betrieb eines Zahlungssystems als der Ausgabe eines Zahlungsmittels zu verorten, weshalb die Abgrenzung vorliegend von untergeordneter Bedeutung zu sein scheint.

Das Betreiben eines Zahlungssystems i.S.v. Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. c GwV i.V.m. FINMA-RS 11/1, Rz. 63 ff. ist gemäss Praxis der FINMA dem GwG unterstellt, wenn es von einer Organisation betrieben wird, welche nicht mit den Benutzern des Zahlungssystems identisch ist (beispielsweise Käufer und Verkäufer einer Ware). Darunter fallen Systeme, die entweder das Zugreifen auf ein aufgrund einer Datenspeicherung verfügbares Guthaben (wiederaufladbarer E-Money-Datenträger, Debitkarten) oder das Speichern einer Schuld, welche anschliessend vom Betreiber des Zahlungssystems in Rechnung gestellt wird (Kreditkarten, Warenhauskarten in Dreiparteienverhältnissen usw.), ermöglichen (FINMA-RS 11/1, Rz. 65).

#### b) Organisation

Mit dem Begriff der Organisation ist die Erwartung einer zentralisierten Struktur verbunden. In Anlehnung an die «Einrichtung» gemäss Art. 81 FinfraG sollte auch für das GwG eine gewisse organisatorische und

strukturelle Zentralisierung des Zahlungssystems vorausgesetzt werden. [71]

Das Lightning Netzwerk wird in den Computerwissenschaften als dezentrales bzw. verteiltes Netzwerk bezeichnet: Je nach Blickwinkel weist das Netzwerk eine P2P-Topologie (im Bereich der Kommunikation) oder aber eine verteilte Topologie mit einigen grösseren Nodes (im Bereich der Zahlungskanäle) auf.[72] Wie bei öffentlichen Blockchains ist keine Einzelperson oder Gruppe von Personen, die miteinander rechtlich oder wirtschaftlich verbunden sind, für das Gesamtnetzwerk verantwortlich. Dies zeigt sich bereits daran, dass die Ausführung des Software Clients oder die Eröffnung eines Zahlungskanals nicht der Zustimmung eines zentralen «Betreibers» bedarf. Im Ergebnis führen Node-Betreiber zwar den Software Client des Lightning Protokolls aus, dies alleine führt aber offensichtlich noch nicht zum Betrieb des Gesamtsystems «Lightning», das über abertausende Nodes und Zahlungskanäle verfügt.

Ferner darf die betreibende Organisation nicht mit den Benutzern des Zahlungssystems identisch sein. Als Benutzer des Zahlungssystems gelten grundsätzlich der Verkäufer und der Käufer einer Ware. Die Rolle der betreibenden Organisation scheint demgegenüber nach Auffassung der FINMA rein intermediärer Natur zu sein, wobei die Benutzer typischerweise über Zahlungskonten bei der Betreiberin verfügen. Der Betrieb einer Lightning Node führt demgegenüber dazu, dass der Betreiber selbst zum Benutzer des Systems wird: Ein Händler etwa, der für den Empfang von LNBTC im Austausch für seine Waren und Dienstleistungen eine Lightning Wallet verwendet, betreibt je nach Applikation eine eigene Node innerhalb des Netzwerks. Eine solche Konstellation schliesst – zumindest ausserhalb des Routings von Drittzahlungen – begrifflich das Vorliegen eines geldwäschereirechtlich unterstellten Zahlungssystem aus.

c) Zahlungssystem

Als Zahlungssysteme qualifizieren gemäss Praxis der FINMA «Systeme, die entweder das Zugreifen auf ein aufgrund einer Datenspeicherung verfügbares Guthaben (wiederaufladbarer E-Money-Datenträger, Debitkarten) oder das Speichern einer Schuld, welche anschliessend vom Betreiber des Zahlungssystems in Rechnung gestellt wird (Kreditkarten, Warenhauskarten in Dreiparteienverhältnissen usw.), ermöglichen» (FINMA-RS 11/1, Rz. 65).

Neben dieser Umschreibung eines unterstellungspflichtigen Zahlungssystems kennt das Geldwäschereirecht keine Legaldefinition des Zahlungssystems selbst. Behelfsweise kann auch hier auf das FinfraG zurückgegriffen werden. Nach Art. 81 FinfraG gilt als Zahlungssystem eine

Einrichtung, die gestützt auf einheitliche Regeln und Verfahren Zahlungsverpflichtungen abrechnet und abwickelt.

Ob das Lightning Protokoll tatsächlich «einheitliche Regeln und Verfahren» für Abrechnung und Abwicklung von Zahlungsverpflichtungen aufstellt, ist fraglich.[73] Die jeweils *bilateral* unterhaltenen Zahlungskanäle können unterschiedliche Regeln für das Routing von LNBTC vorsehen, dies z.B. aufgrund unterschiedlicher Software Clients oder individueller Parametrisierung der Zahlungskanäle durch die Betreiberin. Während es zwar die standardisierten BOLT-Vorgaben gibt, existiert keine Referenzimplementierung des Lightning Protokolls. Generell besteht denn auch anders als in Bitcoin kein Bedürfnis nach Einhaltung gemeinsamer «Konsensregeln».[74] Typischerweise unterstellen sich die Teilnehmer eines Kanals auch nicht vertraglich vordefinierten Abrechnungs- und Abwicklungsregeln. Es fehlt diesbezüglich regelmässig bereits an einem Rechtsbindungswillen der Netzwerkteilnehmer. Von einem einheitlichen Regelwerk, das für alle oder wenigstens viele Teilnehmer gilt, kann darum eher nicht gesprochen werden.

Die FINMA verlangt sodann für das Vorliegen eines geldwäschereirechtlich relevanten Zahlungssystems, dass das System den Zugriff auf ein mittels Datenspeicherung verfügbares Guthaben oder das Speichern einer Schuld ermöglicht, welche anschliessend vom Betreiber des Zahlungssystems in Rechnung gestellt wird.[75]Guthaben und Schulden liegen in traditionellen Zahlungssystemen jeweils bei den Benutzern des Zahlungssystems vor; die Betreiberin des Zahlungssystems wird regelmässig als Gegenpartei der Forderung bzw. der Verbindlichkeit gestützt auf ein vertragliches Rechtsverhältnis auftreten.[76]

Im Lightning Netzwerk werden demgegenüber weder Guthaben (verstanden als Forderungen gegen eine Person) noch Schulden (verstanden als Verbindlichkeiten einer Person) «gespeichert».[77] Das Netzwerk weist ausserdem keine globale Sicht von «Guthaben» und «Schulden» auf, wie es für zentralisierte Zahlungssysteme typisch ist.[78] Mit anderen Worten verfügt ein einzelner Node-Betreiber immer nur über eine gesicherte Sicht des «Kontostandes» des eigenen Zahlungskanals, [79] wohingegen die «Kontostände» der übrigen Teilnehmer für ihn nicht direkt ersichtlich sind.[80]

Wenn ein Benutzer eine Invoice mit dem entsprechenden Payment Hash «begleicht», werden die «Kontostände» in den beanspruchten Zahlungskanälen automatisch aktualisiert. Technisch gesehen werden den Transaktionsdetails entsprechende HTLCs zwischen den an einem Routing einer Transaktion beteiligten Nodes auf- bzw. abgebaut. Die atomistische Natur der Transaktion führt zu einer automatischen

Reduktion im «Kontostand» des versendenden Benutzers und zu einer korrespondierenden automatischen Erhöhung des «Kontostandes» der empfangenden Benutzerin (abzüglich allfälliger Transaktionsgebühren). Hervorzuheben ist, dass ausschliesslich der Benutzer des Systems durch eine entsprechende Bestätigung die Übertragung auslösen kann. Die andere am Kanal beteiligte Person kann Zahlungen der Gegenseite weder selbst auslösen noch von dieser einmal ausgelöste Zahlungen verhindern.

Die Personen, welche über die Private Keys der in den Zahlungskanälen gesperrten BTC verfügen, sind ohnehin als Verfügungsberechtigte am jeweils einschlägigen «Kontostand» und nicht lediglich als Gläubiger von Forderungen gegenüber (anderen) Netzwerkteilnehmern zu betrachten. Darauf lässt auch der mangelnde Rechtsbindungswille von Personen schliessen, die an einem offenen Netzwerk teilnehmen. Keiner der Teilnehmer des Lightning Netzwerks hat sodann die Möglichkeit auf die in den Kanälen gesperrten BTC zuzugreifen, Zahlungsinformationen zu modifizieren oder sogar gänzlich Zahlungen zu blockieren.

Eine andere Sicht würde dazu führen, dass von einer rechtlich relevanten «Guthabenkette» zwischen den im Einzelfall involvierten Nodes auszugehen wäre – vergleichbar mit einer Anweisungskette im Interbanken- bzw. Korrespondenzbankenzahlungsverkehr. Dies wäre allerdings mit den tatsächlichen Gegebenheiten in Lightning nur schwer vereinbar: Ausführung und Abwicklung der Transaktionen erfolgen automatisch, atomistisch und zustimmungsfrei, d.h. gerade nicht sequenziell bzw. kettenartig und durch die involvierten Teilnehmer unterbrechbar. Eine partiell erfüllte Anweisungskette, womit Guthabenforderungen zwischen einzelnen Nodes offen bleiben würden, ist technisch ausgeschlossen.[81] Sichtbar wird die Atomizität der Transaktionen auch bei gescheiterten Routings, die nicht manuell oder stufenweise rückabgewickelt werden müssen, sondern sich grundsätzlich ohne Weiteres auf alle involvierten Nodes auswirken.[82]

### 5. Geld- oder Wertübertragungsgeschäft i.S.d. GwG

Der Betrieb einer Lightning Node ohne gleichzeitiges Routing von Drittübertragungen ist in den Software-Implementierungen nicht vorgesehen, technisch aber durchaus vorstellbar. Das Routing von Zahlungen von Drittpersonen hat auf ersten Blick Ähnlichkeiten mit dem geldwäschereirechtlich relevanten Geld- oder Wertübertragungsgeschäft. Demgegenüber ist die Übertragung eigener Vermögenswerte zum Vornherein nicht dem GwG unterstellt.

Als Geld- oder Wertübertragungsgeschäft i.S.v. Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. d GwV gilt der Transfer von Vermögenswerten durch Entgegennahme von Bargeld, Edelmetallen, virtuellen Währungen,

Schecks oder sonstigen Zahlungsmitteln und die (i) Auszahlung einer entsprechenden Summe in Bargeld, Edelmetallen oder virtuellen Währungen oder die (ii) bargeldlose Übertragung oder Überweisung über ein Zahlungs- oder Abrechnungssystem (Art. 4 Abs. 2 GwV). Bei der Geld- oder Wertübertragung handelt es sich um ein Dreiparteiengeschäft (dies etwa im Gegensatz zum bilateralen Geldwechsel).[83]

Der Begriff der Entgegennahme impliziert die Erlangung der *Verfügungsmacht* über fremde Vermögenswerte i.S.v. Art. 2 Abs. 3 Ingress GwG durch den Finanzintermediär.[84] Um ein Geld- oder Wertübertragungsgeschäft kann es sich beim Routing von Drittzahlungen nach vorliegender Ansicht mangels Verfügungsmacht über fremde Vermögenswerte grundsätzlich nicht handeln. Ein Teilnehmer am Lightning Netzwerk erlangt zu keinem Zeitpunkt die Verfügungsmacht über die gerouteten Vermögenswerte des Absenders bzw. Empfängers.[85] Demgegenüber wird beim Routing lediglich der «Kontostand» der an einem Kanal beteiligten Personen gemäss aktuellster Commitment Transaction in atomistischer Weise aktualisiert.

Im Betrieb einer Lightning Node ist darum viel eher der Betrieb *eines Teils* einer nicht dem GwG unterstellten Kommunikations- und Datenübertragungsinfrastruktur als die Vornahme einer Geld- oder Wertübertragung zu erkennen.[86] Dass der gesetzliche Rahmen ganz grundsätzlich an seine Grenzen stösst, ist auch daran ersichtlich, dass das Lightning Netzwerk jegliche Form der Vermögensübertragung ermöglichen kann (so etwa von tokenisierten Fiatwährungen in Form von Stablecoins oder von Effekten), *ohne* dass die im Einzelnen beteiligten Teilnehmer darum wissen müssen oder Übertragungen zu billigen hätten. Letztlich scheint sich darum der Vergleich mit herkömmlicher Informationsinfrastruktur, wie etwa Internetprotokolle, aufzudrängen.

### 6. Hilfe bei der Übertragung virtueller Währungen an Drittpersonen i.S.d. GwG

Schliesslich liegt auch eine Dienstleistung für den Zahlungsverkehr i.S.v. Art. 2 Abs. 3 lit. b GwG i.V.m. Art. 4 Abs. 1 lit. b GwV 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.

Mit der Revision von Art. 4 GwV wurde das Ziel verfolgt, gewisse Formen der Intermediation im Kryptobereich zu erfassen: *«Darunter fallen beispielsweise Handelsplattformen, die nicht im Besitz des privaten Schlüssels des Kunden sind, die Übertragung der virtuellen Währungen*

*jedoch mittels Smart Contract ermöglichen und dabei die Aufträge bestätigen, freigeben oder sperren können oder anderweitig Kontrolle über den Smart Contract haben […]».*[87] Art. 4 Abs. 1 lit. b GwV stellt einen Paradigmenwechsel im Geldwäschereirecht dar, indem das Kriterium der ausschliesslichen und unmittelbaren Verfügungsmacht über fremde Vermögenswerte (teilweise) aufgegeben wird. Anwendungsbedingung ist demgegenüber nach vorliegender Ansicht die effektive Möglichkeit des Finanzintermediärs, die Transaktionen seines Kunden in relevanter Weise zu beeinflussen (z.B. durch nicht bloss vorübergehende Blockierung oder aber Umleitung von Vermögenswerten), ohne dass diese Form der Kontrolle aber den Grad der Verfügungsmacht erreicht.[88] Ferner muss der Finanzintermediär eine dauernde Geschäftsbeziehung mit seinem Kunden unterhalten.

Die Teilnahme am Lightning Netzwerk verschafft dem Node-Betreiber keine faktische Kontrolle über die gerouteten Vermögenswerte, denn er hat solche Transaktionen weder zu bestätigen oder freizugeben noch kann er sie in relevanter Weise blockieren. Nodes können Drittzahlungen höchstens ignorieren. Die Möglichkeit, einen Zahlungskanal gegen den Willen der Gegenseite zu schliessen, kann nach vorliegender Auffassung ebenfalls nicht als ausreichende Zugriffsmöglichkeit betrachtet werden. Die Gegenseite kann solche erzwungenen Schliessungen jederzeit durch die Publikation des richtigen «Kontostands» auf der Blockchain verhindern.[89] Mit anderen Worten ist die Kontrolle über den Smart Contract protokollbedingt zweiseitig. Ausserdem verfügt ein Node-Betreiber auch nicht über eine vertragliche Rechtsbeziehung mit den übrigen Nutzern des Systems. Es scheitert in der Praxis regelmässig am Fehlen eines Rechtsbindungswillens zwischen den an einem Zahlungskanal beteiligten Personen.

### 7. Betrieb eines Zahlungssystems i.S.d. FinfraG

Gemäss Art. 4 Abs. 2 FinfraG benötigt ein Zahlungssystem nur dann eine Bewilligung der FINMA, wenn die Funktionsfähigkeit des Finanzmarkts oder der Schutz der Finanzmarktteilnehmer es erfordern und das Zahlungssystem nicht durch eine Bank betrieben wird. Entscheidend ist mit anderen Worten der Schutzzweck des Gesetze: «[Das FinfraG] bezweckt die Gewährleistung der Funktionsfähigkeit und der Transparenz der Effekten- und Derivatemärkte, der Stabilität des Finanzsystems, des Schutzes der Finanzmarktteilnehmerinnen und -teilnehmer sowie der Gleichbehandlung der Anlegerinnen und Anleger.» (Art. 1 Abs. 2 FinfraG). Derzeit werden diese Voraussetzungen nur von der SIX Interbank Clearing AG erfüllt. Das Zahlungssystem der PostFinance AG ist aufgrund des Bankstatus der Betreiberin freigestellt.[90] Dass Zahlungen in Kryptowährungen abgerechnet und abgewickelt werden (und nicht in heimischer oder ausländischer Fiatwährung), spielt nach wohl herrschender Ansicht grundsätzlich keine Rolle für die Anwendbarkeit

von Art. 81 FinfraG.[91]

Der Begriff der Einrichtung setzt, wie bereits ausgeführt, eine gewisse organisatorische und technische Zentralisierung voraus.[92] Eine solche fehlt beim Lightning Netzwerk, das von einer Mehrzahl von Personen betrieben wird. Dies gilt selbst für Zahlungskanäle, die in technischer Hinsicht auf jeden Fall zwei Nodes voraussetzen. Die Realität dezentraler Systeme wurde vom Bundesrat in Bezug auf Zahlungssysteme ausdrücklich anerkannt.[93] Die Bedeutung des *gesamten* Lightning Netzwerks wäre heute wohl ohnehin zu gering für die Bejahung der Bewilligungspflicht in Art. 4 Abs. 2 FinfraG.[94]

Wie oben ausgeführt, stellt das Routing von Zahlungen durch die eigene Node kein Geld- oder Wertübertragungsgeschäft im geldwäschereirechtlichen Sinne dar. Auch dieser Aspekt spricht grundsätzlich gegen das Vorliegen eines Zahlungssystems i.S.d. FinfraG.[95]

Eine Unterstellung aller Nodes unter das FinfraG wäre schliesslich aufgrund des grenzüberschreitenden Charakters des Netzwerks praktisch unmöglich. Die Unterstellung *einzelner* Node-Betreiber mit Sitz oder Wohnsitz in der Schweiz wäre demgegenüber wenig zielführend und müsste vor allem mit dem Schutzzweck des Gesetzes begründet werden können.

### 8. Entgegennahme von Publikumseinlagen oder kryptobasierten Vermögenswerten i.S.d. BankG

Die Eröffnung eines Zahlungskanals und das Routing von Zahlungen von Drittpersonen hat auf den ersten Blick gewisse Ähnlichkeiten mit der Entgegennahme von Publikumseinlagen oder kryptobasierten Vermögenswerten.

Gemäss Art. 1 Abs. 2 BankG i.V.m. Art. 5 Abs. 1 BankV i.V.m. FINMA-RS 08/3, Rz. 10 gelten grundsätzlich alle Verbindlichkeiten gegenüber Kunden vorbehaltlich der Anwendbarkeit einer Ausnahme als Publikumseinlagen. Das Bundesgericht fordert im Wesentlichen, dass der Empfänger fremder Gelder eine Verpflichtung zur Rückzahlung gegenüber dem Einleger oder einem Dritten eingeht und somit (selbst) zum Rückzahlungsschuldner der entsprechenden Leistung wird.[96] Für kryptobasierte Vermögenswerte in Form von Zahlungs-Token, falls sie i.S.v. Art. 16 Ziff. 1$^{bis}$ lit. b BankG sammelverwahrt werden, gilt heute ein ähnliches Regime wie für Publikumseinlagen (vgl. Art. 1b BankG i.V.m. Art. 5a Abs. 1 BankV). Werden die Zahlungs-Token hingegen für Eigengeschäfte des Empfängers verwendet und/oder werden derartige Guthaben verzinst, erfolgt eine aufsichtsrechtliche Gleichsetzung mit Publikumseinlagen (vgl. Art. 1a lit. b BankG).[97] Entsprechend könnte die Entgegennahme

von LNBTC, wenn sie als Publikumseinlagen oder sammelverwahrte Zahlungs-Token qualifizieren, die Bewilligungspflichten nach BankG auslösen.

Es ist demgegenüber festzuhalten, dass der reine Betrieb einer Lightning Node zu keinem Zeitpunkt mit dem Erhalt der Verfügungsmacht bzw. -befugnis über Vermögenswerte Dritter verbunden ist. Ein Betreiber erhält namentlich zu keinem Zeitpunkt Zugriff auf oder Kenntnis der Private Keys der durch seine Node gerouteten Vermögenswerte.[98] Bis zur gültigen Signierung und Auslösung einer Transaktion kann nur der Absender über die mittels Invoice angeforderte UTXO verfügen; danach fällt die alleinige Verfügungsmacht dem in der Invoice spezifizierten Empfänger zu. Es fehlt somit bereits an der Möglichkeit, dass der Node-Betreiber zum Vollrechtsinhaber hinsichtlich der gerouteten LNBTC und in der Folge zum Rückzahlungsschuldner wird. Zudem haben gewöhnliche Node-Betreiber regelmässig auch nicht den Rechtsbindungswillen, in einlagenrechtlich relevante Rechtsverhältnisse mit den übrigen Netzwerkteilnehmern oder Nutzern zu treten.

### 9. Zwischenfazit

Die Teilnahme am Lightning Netzwerk durch den Betrieb einer eigenen Node, was u.a. das Routing von Drittzahlungen beinhaltet, ist nach vorliegender Auffassung ohne finanzmarktrechtliche Unterstellung möglich.

# III. Schlussfolgerungen

Der Einsatz neuer Technologien ist regelmässig mit einem gewissen Mass an Rechtsunsicherheit behaftet. Dies gilt auch für das Lightning Netzwerk. Das Protokoll fordert in praktischer Hinsicht aufgrund seiner verteilten Struktur und der Teilnahmeoffenheit das vorherrschende Regulierungsparadigma der Intermediation heraus. Vor diesem Hintergrund scheint selbst eine vorwiegend wirtschaftliche Betrachtungsweise («substance over form») zu keiner eindeutigen rechtlichen Einordnung der Teilnahme am Lightning Netzwerk in das heutige finanzmarktrechtliche Gefüge zu führen. Die Risiken der Teilnahme am Lightning Netzwerk sind denn auch nicht vergleichbar mit den Risiken traditioneller Zahlungssystembetreiber («different risks, different rules»). So können etwa Netzwerkteilnehmer nicht auf die BTC der übrigen Node-Betreiber zugreifen, obschon sie grundsätzlich in die Übertragung der Vermögenswerte bis zu einem gewissen Grad involviert sind. Lightning sollte nach richtiger technologieneutraler Auffassung – analog zum Bitcoin Netzwerk – als quasiöffentliche Kommunikations- und Datenübertragungsinfrastruktur betrachtet werden, deren Betrieb durch eine Vielzahl von Personen keine Bewilligungspflichten oder dergleichen auslöst, auf welcher aber gegebenenfalls gewisse Formen regulierter

Tätigkeiten ausgeübt bzw. angeboten werden können.

---

[1] Vgl. etwa Mahdi H. Miraz/David C. Donald, LApps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications, ICISDM 2019, S. 185 ff.; ferner die Hinweise in Bundesrat, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz. Eine Auslegeordnung mit Fokus auf dem Finanzsektor, 14. Dezember 2018, S. 27.

[2] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 10. Oktober 1997, SR 955.0.

[3] Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 19. Juni 2015, SR 958.1.

[4] Bundesgesetz über die Banken und Sparkassen vom 8. November 1934, SR 952.0.

[5] Siehe Andreas M. Antonopoulos/Olaoluwa Osuntokun/René Pickhardt, Mastering the Lightning Network, Sebastopol 2022, S. 73.

[6] So etwa für die Ethereum Blockchain das «Raiden Network» (https://raiden.network/).

[7] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 71; ausführlich zu diesem Konzept Fabio Andreotti, Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht, Diss Zürich, erscheint 2023.

[8] Anders als die bedeutsamste Abspaltung (sog. *Hardfork*) von Bitcoin, «Bitcoin Cash», hat sich die Bitcoin Community nicht für grössere Blocks, die mehr Speicherplatz für Transaktionen bieten, ausgesprochen. Zur Kontroverse, die damit verbunden war, vgl. Jonathan Bier, The Blocksize War: The battle for control over Bitcoin's protocol rules, 2021, insbesondere Kapitel 6 und 19.

[9] Siehe für eine aktualisierte Version Joseph Poon/Thaddeus Dryja, The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 14. Januar 2016, DRAFT Version 0.5.9.2, https://lightning.network/lightning-network-paper.pdf.

[10] Zahlungskanäle können auch ohne öffentliche Ankündigung gegenüber dem Netzwerk betrieben werden, sog. *Unannounced Channels*; vgl. Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 50, 279.

[11] Siehe für aktuelle Statistiken https://1ml.com/statistics. Zur Begrifflichkeit des offenen dezentralen Systems vgl. Nicolas Jacquemart, Offene Blockchainsysteme und die Schutzziele des schweizerischen

Finanzmarktrechts, Zürich 2020, Rz. 161 ff.

[12] Vgl. Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 4 ff. sprechen von einem *Fairness Protocol*, das sie definieren als *«[…] a process that uses a system of incentives and/or disincentives to ensure fair outcomes for participants who don't trust each other […]".*

[13] Z.B. «lnd» (https://github.com/lightningnetwork/lnd/blob/master/docs/INSTALL.md) oder «Core Lightning» (https://github.com/ElementsProject/lightning#installation).

[14] Siehe die Übersicht bei Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 146.

[15] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 12. Die vorliegende Verwendung des Begriffs «LNBTC» dient lediglich der terminologischen Unterscheidung zu BTC.

[16] *State Channels* bilden die technische Grundlage für Zahlungskanäle, indem in ihnen ein gemeinsamer On-Chain-Zustand der an einem Kanal beteiligten Parteien abgebildet wird. Abgesichert werden die Vermögenswerte im Zahlungskanal durch eine spezielle *2-von-2-Multisig-Adresse*, welche den am Kanal beteiligten Parteien die Verfügung über die Vermögenswerte nur gemeinsam erlaubt. Damit die gegenseitige Abhängigkeit jedoch nicht dazu führt, dass Vermögenswerte gegen den Willen der einen Partei blockiert werden können, wird mit einem *HTLC* ein spezieller Smart Contract verwendet, der nach vorprogrammiertem Zeitablauf die Rücknahme der Vermögenswerte möglich macht. Zu diesen Primitiven im Einzelnen Andreas M. Antonopoulos, Mastering Bitcoin, 2. Aufl., Sebastopol 2017, S. 300 ff.

[17] Vgl. Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 44 ff.

[18] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 55.

[19] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 55.

[20] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 140 f.

[21] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 186.

[22] Vgl. hierzu ausführlich Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 186, 231 ff.

[23] Ausführlich hierzu Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 17 ff.

[24] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 131 ff.

[25] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 134 ff.

[26] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 134.

[27] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 128.

[28] Vgl. etwa Shinobi, Learning from the LND bug that could have robbed the Lightning Network, 24. Oktober 2022, https://bitcoinmagazine.com/technical/learning-from-the-lnd-bug-on-lightning.

[29] Siehe etwa Conner Fromknecht, Connecting Blockchains: Instant Cross-Chain Transactions On Lightning, 16. November 2017, https://blog.lightning.engineering/announcement/2017/11/16/ln-swap.html; ferner weiterführende Hinweise bei Andreotti, a.a.O.

[30] https://docs.lightning.engineering/the-lightning-network/taro/taro-on-lightning.

[31] Das Colored Coins Protokoll nutzt etwa das Metadatenfeld einer Bitcoin Transaktion, um arbiträre Daten auf der Blockchain zu speichern, welche typischerweise sodann auf extern gespeicherte Daten verweisen; vgl. hierzu Antonopoulos, a.a.O., S. 294 ff.

[32] Vgl. hierzu etwa Antonopoulos, a.a.O., S. 299 f.; Arvind Narayanan/Joseph Bonneau/Edward Felten/Andrew Miller/Steven Goldfeder, Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, Princeton 2016, S. 218 f.

[33] https://docs.lightning.engineering/the-lightning-network/taro/faq#taro-on-chain.

[34] https://docs.lightning.engineering/the-lightning-network/taro/faq#taro-on-the-lightning-network.

[35] Siehe Botschaft zu einem Bundesgesetz über die Börsen und den Effektenhandel vom 24. Februar 1993, BBl 1993 I, S. 1395 f.; FINMA, Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs), 16. Februar 2018, S. 4 («der für Effekten typische Kapitalmarktbezug»); Dieter Zobl, in: Hertig et al. (Hrsg.), Kommentar BEHG, Zürich 2000, Art. 2 lit. a N 3; ferner zum Bezug von Derivaten zum *Finanzmarkt* Stefan Kramer/Olivier Favre, in: Sethe et al. (Hrsg.), Schulthess Kommentar FinfraG, Zürich 2017, Art. 2 lit. c N 5, 7, 23 (nachfolgend «SK FinfraG-Autor/in»); bereits Daniel Daeniker/Stefan Waller, in: Watter/Vogt (Hrsg.), Basler Kommentar BEHG/FINMAG, 2. Aufl., Basel 2011, Art. 2 lit. a-c BEHG N 13 (nachfolgend «BSK BEHG/FINMAG-Autor/in»).

[36] Siehe FINMA, ICO-Wegleitung 2018, S. 4.

[37] Siehe FINMA, ICO-Wegleitung 2018, S. 4 f.

[38] Solche «tailormade» Derivate qualifizieren aber als Finanzinstrumente gemäss Art. 3 lit. a Ziff. 5 FIDLEG.

[39] So zumindest scheinbar die Aufsichtspraxis FINMA, ICO-Wegleitung 2018, S. 3.

[40] So auch Andri Abbühl, Effektenqualität von Blockchain-Token, iusNet BR-KR 23. Dezember 2021; bereits als fragwürdig bezeichnet Kevin MacCabe, Abbildung von Vermögenswerten durch Anlage-Tokens, Basel 2019, Rz. 124.

[41] Siehe FINMA, ICO-Wegleitung 2018, S. 2.

[42] Gl.M. wohl auch Yves Mauchle, Tokens als Effekten, GesKR 2022, S. 185, 193, der von der Erstellung, Ausgabe bzw. Buchung durch eine bestimmte Person als einem «Grundelement» einer Effekte spricht; ferner für das US-amerikanische Recht aufgrund einer umfassenden Rechtsprechungsanalyse Lewis Rinaudo Cohen/Gregory Strong/ Freeman Lewin/Sarah Chen, The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets Are not Securities, Discussion Draft, 10. November 2022, https://ssrn.com/abstract=4282385.

[43] Die FINMA spricht in Bezug auf Vorfinanzierungen und Vorverkäufen von Token davon, dass ein «*handelbarer* Anspruch auf Übertragung des [Ziel- bzw. End-]Token» vorzuliegen hat, vgl. FINMA, ICO-Wegleitung 2018, S. 7 (Hervorhebung hinzugefügt).

[44] Siehe hierzu Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 270 ff. (Vollzitat in Teil 1 dieses Beitrages).

[45] Siehe zum Begriff des Kapitalmarkts als volkswirtschaftliches Konzept Thomas Wiedmer, Kapitalmarkt, in: Boemle et al. (Hrsg.), Geld-, Bank- und Finanzmarkt-Lexikon der Schweiz, Zürich 2002, S. 637 f.; Dieter Zobl/Stefan Kramer, Schweizerisches Kapitalmarktrecht, Zürich 2004, N 1.

[46] Siehe bereits Botschaft zu einem Bundesgesetz über die Börsen und den Effektenhandel vom 24. Februar 1993, BBl 1993 I, S. 1395; Botschaft zum Finanzmarktinfrastrukturgesetz vom 3. September 2014, BBl 2014, S. 7513; ferner SK FinfraG-Kramer/Favre, Art. 2 lit. c N 33; BSK BEHG/FINMAG-Daeniker/Waller, Art. 2 lit. a-c BEHG N 12, wonach weiter auch eine *Swap-Komponente* zu unterscheiden ist (letztlich handelt es sich hierbei um ein Termingeschäft); ausführlich Franca Contratto, Konzeptionelle Ansätze zur Regulierung von Derivaten im schweizerischen Recht, Zürich 2006, S. 135.

[47] Siehe SK FinfraG-Kramer/Favre, Art. 2 lit. c N 21 ff. («Andere Instrumente mit einer derivativen oder derivatähnlichen Komponente»).

[48] *Gl. M.* Mauchle, GesKR 2022, S. 186.

[49] Siehe BSK BEHG/FINMAG-Daeniker/Waller, Art. 2 lit. a-c BEHG N 11; ferner Contratto, a.a.O., S. 138.

[50] Siehe Contratto, a.a.O., S. 141 f.

[51] So Botschaft zu einem Bundesgesetz über die Börsen und den Effektenhandel vom 24. Februar 1993, BBl 1993 I, S. 1395.

[52] Siehe etwa Eleonor Gyr, Smart Contracts and Contract Law, Jusletter IT vom 30. Juni 2022, Rz. 91.

[53] Vgl. hierzu SK FinfraG-Kramer/Favre, Art. 2 lit. c N 8.

[54] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 140 f.

[55] Siehe hierzu Contratto, a.a.O., S. 23 ff.

[56] Siehe den Vergleich zu *herkömmlichen* Zahlungs-Token, die keine Anbindung an einen unterliegenden Vermögenswert aufweisen, FINMA, Ergänzung der Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs), 11. September 2019, S. 1 f. *(«[…] aufgrund des üblichen Zahlungsmittelzwecks […]»)*.

[57] Siehe FINMA, Ergänzung ICO-Wegleitung 2019, S. 1.

[58] FINMA, Ergänzung ICO-Wegleitung 2019, S. 3.

[59] Eine Teildeckung wäre allenfalls mit dem Eingehen von bankrechtlich relevanten Verbindlichkeiten verbunden.

[60] Siehe FINMA, ICO-Wegleitung 2018, S. 3.

[61] Vgl. etwa Bundesrat, DLT-Bericht, S. 115 (Vollzitat in Teil 1 dieses Beitrages); ferner Claude Humbel, Decentralized Finance, GesKR 2022, S. 19 f. m.w.N.

[62] So offenbar auch FINMA, Jahresbericht 2021, S. 20; FATF, Virtual Assets and Virtual Asset Service Providers. Updated Guidance for a Risk-based Approach, Oktober 2021, Rz. 56, 67, 81; vgl. zu den fehlenden Anknüpfungspunkten Benedikt Maurenbrecher/Benjamin Leisinger, Decentralized Finance (Teil 2), SJZ 2022, S. 710 ff.

[63] Dies im Grundsatz anerkennend Bundesrat, DLT-Bericht, S. 14; ähnlich auch Hans Kuhn/Rolf H. Weber, I. Einleitung, in: Weber/Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, Rz. 20 f.

[64] Die FINMA spricht von «Emission»; vgl. FINMA-RS 11/1, Rz. 64.

[65] Siehe statt vieler Antonopoulos, a.a.O., S. 231 (Vollzitat in Teil 1 dieses Beitrages).

[66] Siehe die Nachweise bei Andreotti, a.a.O. (Vollzitat in Teil 1 dieses Beitrages).

[67] Siehe FINMA-RS 11/1, Rz. 67 f.

[68] Vgl. FINMA-RS 11/1, Rz. 64.

[69] Siehe FINMA, ICO-Wegleitung 2018, S. 6; ähnlich wohl auch SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 25.

[70] Siehe etwa My Chau Bachelard/Martin Hess, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar GwG, Basel 2021, Art. 2 Abs. 3 lit. b N 30 ff. m.w.N. (nachfolgend «BSK GwG-Autor/in»).

[71] Siehe SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 30; Rashid Bahar/Eric Stupp, in: Watter/Bahar (Hrsg.), Basler Kommentar FINMAG/FinfraG, 3. Aufl., Basel 2018, Art. 81 FinfraG N 2 (nachfolgend «BSK FINMAG/FinfraG-Autor/in»).

[72] Siehe etwa Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 81, 340 f.

[73] Vgl. etwa SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 31, wonach ein «für alle Teilnehmer gleichermassen geltendes einheitliches Regelwerk» existieren muss, wobei sowohl technische als auch administrative Regeln und Verfahren darunter fallen.

[74] Zum Ganzen ausführlich Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 89 (Implementations), 151 (Routing Fees), 162 ff. (Channel Parameters), 305 und 307 (Features).

[75] Vgl. FINMA-RS 11/1, Rz. 65. Im Falle der vom Bundesgericht beurteilten «Mobile Valued-Added Services» (MVAS) der Swisscom bestand das Speichern einer *Schuld* darin, dass die Swisscom die von ihren Kunden bezogenen Leistungen diesen erst bei Fälligkeit der nächsten Telefonrechnung in Rechnung stellt und somit bis dorthin *speichert* (Urteil des Bundesgerichts 2C_488/2018 vom 12. März 2020 E. 4.4.1 *in fine*).

[76] Vgl. BSK GwG-Bachelard/Hess, Art. 2 Abs. 3 lit. b N 44 («seine Vertragspartei»).

[77] Zwar stehen Absender und Empfänger einer LNBTC-Transaktion regelmässig in einem Rechtsverhältnis zueinander (z.B. aufgrund des Kaufs von Waren gegen LNBTC), doch sind solche vertraglichen Ansprüche vom Guthaben- bzw. Schuldbegriff des GwG abzugrenzen.

[78] Siehe Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 17, 69 *(«[…] the balance in a channel at a particular time is known only to the two channel partners […]»)*.

[79] Vgl. auch Bundesrat, DLT-Bericht, S. 27 *(«Zum Beispiel eröffnen beim Lightning-Netzwerk zwei Endpunkte einen Zahlungskanal über ein bestimmtes Guthaben. Dieses Guthaben kann danach beliebig häufig den Besitzer wechseln, und erst am Endes des Kanals werden die Guthaben den Endpunkten durch eine Blockchain Transaktion ausbezahlt.»)*.

[80] Vgl. hierzu Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 355 ff.

[81] Siehe Elizabeth Stark, Lightning Network, 15. September 2016, https://www.coincenter.org/education/key-concepts/lightning-network/ *(«[…] receiving a payment is dependent on having already forwarded it. Lightning payments are conditional upon disclosure of a cryptographic secret, and knowledge of that secret allows for redemption from prior nodes […].»)*.

[82] Denkbar ist, dass eine Node die «Rückabwicklung» verhindern möchte, indem ihr Betreiber in Bezug auf die Auflösung der etablierten HTLC unkooperativ agiert. In diesem Fall können die übrigen Nodes den richtigen «Kontostand» on-chain ausführen und somit unkooperative Teilnehmer umgehen (sowie bestrafen).

[83] Siehe Bundesrat, Bericht des Bundesrates zu virtuellen Währungen, 25. Juni 2014, S. 15; Simon Schären, in: Kunz/Jutzi/Schären (Hrsg.), Stämpflis Handkommentar GwG, Bern 2017, Art. 2 N 121 (nachfolgend «SHK GwG-Autor/in»).

[84] Siehe SHK GwG-Schären, Art. 2 N 81; Ralph Wyss, in: Thelesklaf et al. (Hrsg.), GwG Kommentar, Zürich 2019, Art. 2 N 27; ferner zum Begriff des Annehmens allgemein BSK GwG-Greter, Art. 2 Abs. 3 N 32.

[85] So wohl auch der Bundesrat, DLT-Bericht, S. 147 FN 802.

[86] So bereits Peter Van Valkenburgh, The Bank Secrecy Act, Cryptocurrencies and New Tokens: What is Known and What Remains Ambiguous, Coin Center Report May 2017, S. 15 ff.; ähnlich EFD, Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuterungen vom 18. Juni 2021, S. 23.

der Technik verteilter elektronischer Register. Erläuterungen, 18. Juni 2021, S. 23; ferner EFD/EFV, Praxis der Kontrollstelle für die Bekämpfung der Geldwäscherei zu Art. 2 Abs 3 GwG vom 29. Oktober 2008, Rz. 160, wonach *nicht jede Hilfeleistung* im Zusammenhang mit dem

Zahlungsverkehr dem GwG unterstellt ist.

[87] EFD, Erläuterungen DLT-Verordnung, S. 22.

[88] Die Rede ist von «Kontrolle über den Smart Contract» und «Zugriffsmöglichkeit»; vgl. EFD, Erläuterungen DLT-Verordnung, S. 22 f.; BSK GwG-Bachelard/Hess, Art. 2 Abs. 3 lit. b N 16, welche die «faktische Kontroll- und Eingriffsmöglichkeit des Dienstleisters betreffend die Transaktionen» voraussetzen; ebenso Andreotti, a.a.O., wo eine nicht bloss theoretische, sondern effektive Zugriffsmöglichkeit auf die Aufträge bzw. Transaktionen von Kunden verlangt wird.

[89] Sog. *Punishment Transaction*; vgl. hierzu Antonopoulos/Osuntokun/Pickhardt, a.a.O., S. 53 f.

[90] Siehe BSK FINMAG/FinfraG-Bahar/Stupp, Art. 81 FinfraG N 8 m.w.H.

[91] Siehe SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 22, 32, 34; BSK FINMAG/FinfraG-Bahar/Stupp, Art. 81 FinfraG N 4.

[92] Siehe SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 30; BSK FINMAG/FinfraG-Bahar/Stupp, Art. 81 FinfraG N 2.

[93] Siehe Bundesrat, DLT-Bericht, S. 111.

[94] Vgl. die in Teil 1 des vorliegenden Beitrags angeführten statistischen Werte des Netzwerks.

[95] Vgl. SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 27.

[96] Vgl. etwa BGE 136 II 43 E. 4.2 S. 48 f.; 132 II 382 E. 6.3.1 S. 391 f.

[97] Die Revision von Art. 1a lit. b BankG erscheint vor diesem Hintergrund als *nicht gelungen*: Bisher galten sammelverwahrte Zahlungs-Token i.S.v. Art. 16 Ziff. $1^{bis}$ lit. b BankG als die gemäss Art. 1b Abs. 1 lit. a BankG vom Bundesrat bezeichneten «kryptobasierten Vermögenswerte». Solche Token können definitionsgemäss («jederzeit bereitzuhalten») nicht auf eigene Rechnung des Intermediärs angelegt werden, sodass der Wortlaut von Art. 1a lit. b BankG in diesem Punkt wenig Sinn ergibt. Eine Verzinsung (ohne gleichzeitige Anlagemöglichkeit) wäre theoretisch denkbar, wenn auch betriebswirtschaftlich langfristig eher schwer zu rechtfertigen.

[98] Vgl. Van Valkenburgh, Coin Center Report, S. 15 f.

bitcoin BTC Finanzmarktregulierung lightning network LNBTC

← Stellungnahme zur Teilrevision des “Krypto-Geldwechsels” (Art. 51a GwV-FINMA)

Custodial Staking und FINMA-Aufsichtspraxis →

# Comments

## Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

MORE POSTS



# flock of ideas

the whole point of the dancing is the dance – A. W.

Designed with WordPress