SWISS BLOCKCHAIN FEDERATION

# Zirkular 2023/01

# Staking

**Aktualisierte Fassung des Zirkulars 2023/01 vom 05.09.2023**

Genehmigt von der Swiss Blockchain Federation[1] am 14.03.2024

Publikationsdatum: 03.04.2024

**Autoren**: Digital Assets Arbeitsgruppe (Sub-Gruppe Staking) unter der Leitung von Fabio Andreotti (Bitcoin Suisse AG) und der Mitarbeit von Diego Benz (Kaiser Odermatt & Partner), Sandro Brühlmann (PostFinance AG), Mauro Cappiello (Blockchain Innovation Group), Christoph Drexl (PrimeTax AG), Nina Gartmann (Crypto Helvetica AG), Hans Kuhn (Lawside), Dominic Nazareno (PrimeTax AG), Silke Nock Widmer (SDX), Ricardo Schlatter (Allegra LAW), Joshua R. Taucher (Sygnum Bank AG), Alexander Thoma (PostFinance AG), Rolf H. Weber (Bratschi AG) und Martina Wolf (PrimeTax AG).

**Kontakt**: Daniel Rutishauser, daniel.rutishauser@inacta.ch

[1] **Hinweis**: Die Swiss Blockchain Federation ist eine private Organisation. Die in diesem Dokument enthaltenen Empfehlungen widerspiegeln ökonomisch und rechtlich unser bestes Wissen und Gewissen, sind aber kein Ersatz für professionelle Beratung. Angesichts der fortlaufenden Entwicklung ist auch davon auszugehen, dass das vorliegende Zirkular zu gegebener Zeit durch eine überarbeitete Version ersetzt wird. Sodann enthält dieses Dokument ausschliesslich Informationen betreffend Schweizer Recht. Bei grenzüberschreitenden Sachverhalten kommen die entsprechenden Regeln der betroffenen Staaten zur Anwendung.

# Inhaltsverzeichnis

# 1. Einleitung

Der innovative Charakter öffentlicher Blockchains brachte eine Reihe von Neuerungen mit sich. Eine der Hauptinnovationen liegt dabei in der Konsensfähigkeit solcher dezentraler Systeme. Eine Vielzahl nicht miteinander verbundener Personen kommt dank der Vermittlung entsprechender Protokolle und Algorithmen zu einer für alle verbindlichen Sicht der Dinge. Mit diesen Neuerungen wurden auch neue Rechtsfragen aufgeworfen.

Dabei sind zwei Konsensmechanismen besonders bedeutend in der Praxis: *Mining (Proof-of-Work, PoW)*, d.h. der Einsatz von Rechenkapazitäten, und *Staking (Proof-of-Stake, PoS)*, d.h. die Bereitstellung eines geldwerten Einsatzes. Die beiden Konsensmechanismen führen jeweils zur fortlaufenden Ergänzung der Blockchain. In beiden Fällen koordinieren kryptoökonomische Anreize die korrekte Verarbeitung der Datenströme. Transaktionen werden in Blöcken gesammelt, deren Korrektheit unter Anwendung der Regeln eines Protokolls validiert wird. Die an der Validierung beteiligten Personen werden für ihre Leistungen zugunsten des Blockchainsystems vergütet; bei Regelverstössen können sie je nach Blockchain-Protokoll hingegen auch sanktioniert werden.

Das vorliegende Zirkular widmet sich dem Konsensmechanismus des *Stakings*. Die Innovation liegt dabei in der Blockierung bzw. Hinterlegung von kryptobasierten Vermögenswerten in einem *Proof-of-Stake*-Protokoll und damit auch der Unterstellung der Vermögenswerte unter die einschlägigen Regeln des Protokolls. Staking ist dabei nicht ohne Risiken für die Teilnehmer einer Blockchain. In der Praxis haben sich verschiedene Modelle des Stakings herausgebildet. Die Modelle tragen den unterschiedlichen Bedürfnissen der Marktteilnehmer Rechnung, die oftmals an einer arbeitsteiligen Erbringung von Staking-Dienstleistungen interessiert sind. Für Schweizer Krypto-Dienstleister stellt Staking eine attraktive Möglichkeit dar, mit ihrem Dienstleistungsangebot den erwähnten Bedürfnissen nachzukommen.

Die *erste* Fassung des Zirkulars wurde im September 2023 veröffentlicht und hatte zum Ziel, eine erste rechtliche Beurteilung von Staking vorzunehmen.[2] Neben einer zivilrechtlichen Einordnung stehen je nach Staking-Modell vor allem konkurs-, bank- und steuerrechtliche Fragestellungen im Vordergrund. Es zeigt sich dabei, dass das Custodial Staking die meisten neuen Rechtsfragen aufwirft. Der Schweizer Gesetzgeber hat allerdings bereits mit dem DLT-Mantelerlass vorausschauend einen Rechtsrahmen eingeführt, der auch auf damit zusammenhängende Fragen geeignete Antworten geben kann.[3] Eine *Aktualisierung* des Zirkulars drängte sich nunmehr auf, nachdem die Eidgenössische Finanzmarktaufsichtsbehörde am 20. Dezember 2023 die FINMA-Aufsichtsmitteilung 08/2023 «Staking» veröffentlicht hat.

[2] Die erste Fassung des Zirkulars ist verfügbar unter https://blockchainfederation.ch/downloads/.

[3] Siehe Medienmitteilung des Bundesrates, «Bundesrat will Rahmenbedingungen für DLT/Blockchain weiter verbessern», 27.11.2019, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-77252.html, zuletzt besucht am 29.02.2024.

# 2. Staking

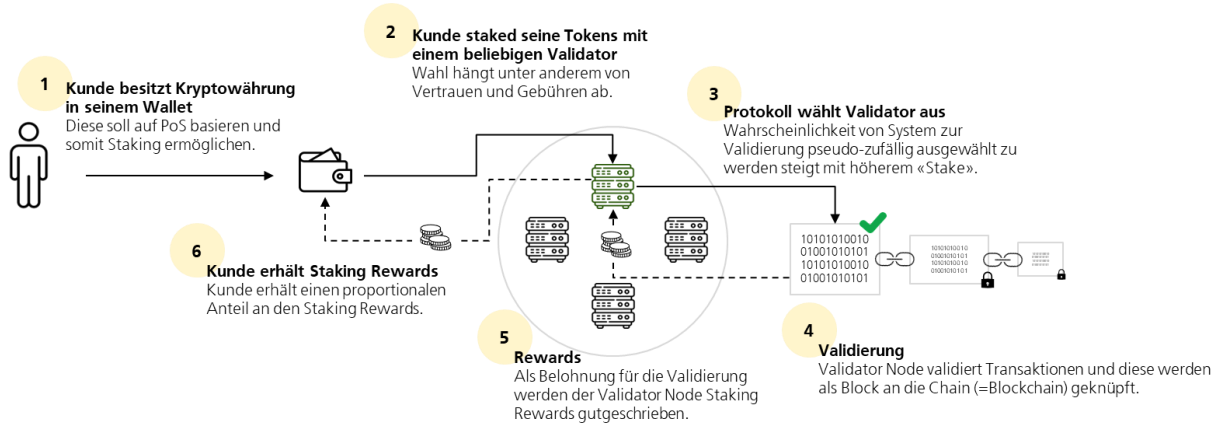
## 2.1 Funktionsweise

*Proof-of-Stake* bildet die Grundlage für einen Konsensmechanismus, der in Blockchain-Netzwerken verwendet wird, um Transaktionen zu bündeln, neue Blöcke zu erstellen und diese zu validieren.

Bei den meisten PoS müssen Validatoren eine bestimmte Menge an Kryptowährungen, die als sog. *Stake* bezeichnet werden, im Protokoll als Sicherheit hinterlegen, um am Netzwerk teilnehmen zu können. Die teilnehmenden Validatoren werden nach den Regeln des PoS-Protokolls ausgewählt, um die Validierungsleistungen zu erbringen. Abhängig vom PoS-Protokoll können die hinterlegten Kryptowährungen (auch *Coins* oder *Tokens*) während der gesamten Staking-Dauer blockiert sein (sog. *Lock-Up*). In diesem Fall können Validatoren die gestakten Token bis zur Beendigung des Stakings nicht frei übertragen. Als Entgelt bzw. Vergütung für protokollkonformes Verhalten verteilt das PoS-Protokoll den Validatoren in programmatischer Weise sog. *Staking Rewards* in der Regel in Form der Kryptowährung des jeweiligen Protokolls. Staking Rewards entspringen in der Regel den vom Protokoll neu geschöpften Token und je nach Protokoll auch den von Nutzern der Blockchain bezahlten Transaktionsgebühren.

Staking bildet die Grundlage dafür, dass die Validatoren eines Blockchain-Netzwerks protokollkonform handeln. Sie sind incentiviert, Transaktionen korrekt zu validieren, weil ihr Stake analog einem Pfand als Sicherheit dient. Validatoren können im Extremfall ihren Stake ganz oder teilweise verlieren, falls sie sich protokollwidrig verhalten, z.B. indem sie Transaktionen absichtlich falsch validieren oder ihren Stake doppelt hinterlegen (sog. *Slashing*). Ferner können Validatoren auch für kleinere Vergehen sanktioniert werden, so etwa, wenn sie im Validierungszeitpunkt nicht online sind. In diesem Fall sind je nach Protokoll nicht der Stake betroffen, sondern lediglich die absehbaren, aber noch nicht ausgeschütteten Staking Rewards (sog. *Penalties*). Insgesamt beruht Staking auf einem ökonomischen Anreizsystem, in dem Validatoren ein finanzielles Interesse am Erfolg des Netzwerks haben und motiviert sind, ehrlich zu handeln und den Regeln des Netzwerks zu folgen. Dies schafft ein sicheres und stabiles Netzwerk, das Transaktionen schnell und effizient verarbeiten kann. Es benötigt ausserdem deutlich weniger Energieressourcen als Konsensmechanismen, wie etwa das *Mining* bei *Proof-of-Work* (PoW).

Grafik 1: Übersicht des typischen Custodial Staking-Prozesses




Quelle: PostFinance

Es gilt anzumerken, dass sich der Prozess des Stakings von Protokoll zu Protokoll stark unterscheiden kann und die obige Abbildung somit lediglich als illustratives Beispiel verstanden werden soll. Nachfolgend soll der Staking-Vorgang vereinfacht am Beispiel der Ethereum Blockchain erklärt werden.

## 2.2 Beispiel von Ethereum

Um ein besseres Verständnis des Staking-Vorgangs auf der Ethereum Blockchain zu erhalten, ist vorab zwischen dem sog. *Consensus Layer* (ehemals Beacon Chain) und dem sog. *Execution Layer* zu unterscheiden. Der Consensus Layer beinhaltet im Wesentlichen die Logik des Konsensmechanismus inklusive Staking Rewards und Slashing bzw. Penalties[4], wohingegen der Execution Layer die Grundlage für Transaktionen und Interaktionen mit Smart Contracts bildet.

Der erste Schritt für Staker besteht darin, ihre Ether (ETH) vom Execution Layer auf den *Consensus Layer* zu transferieren. Nachdem die ETH erfolgreich transferiert worden sind, besteht die Möglichkeit, als Validator am PoS-Konsensmechanismus der Blockchain teilzunehmen. Dies erfordert die Blockierung eines Mindestbetrags von 32 ETH pro Validator Node (*Lock-Up*). Die Zeit auf dem Consensus Layer ist in sog. *Epochen* und *Slots* unterteilt. Eine Epoche ist ein Zeitraum von 6 Minuten 24 Sekunden, der aus 32 Slots von jeweils 12 Sekunden besteht. Validatoren müssen sich für Slots anmelden, um an der Blockproduktion teilzunehmen. Das Protokoll des Consensus Layer gibt schliesslich den Algorithmus vor, der den Teilnehmer als zuständigen Validator für den jeweils nächsten Block auswählt. Für ihre Beteiligung am Netzwerk und die erfolgreiche Validierung von Transaktionen erhalten Validatoren Staking Rewards in Form von ETH. Die ETH setzen sich einerseits aus neu geschöpften Tokens und andererseits aus Transaktionsgebühren der Nutzer der Ethereum Blockchain zusammen.

[4] Bei *Penalties* wird die Ethereum Validator Node mit dem Verlust der Staking Rewards bestraft, die sie erhalten hätte, wenn sie die Attestation korrekt abgegeben hätte. Beim *Slashing* wird die Validator Node mit dem Verlust der gestakten kryptobasierten Vermögenswerte bestraft. Darüber hinaus kann die Validator Node zwangsweise aus dem Netzwerk entfernt werden. Dies bedeutet, dass der Validator nicht nur seine gestakten Tokens, sondern auch die Möglichkeit verliert, Staking Rewards zu verdienen. Slashing stellt somit die härtere Sanktion dar.

Der Consensus Layer ist mit dem *Execution Layer* verbunden, welcher die Grundlage für die Ausführung von Transaktionen und Smart Contracts bildet. Consensus und Execution Layer kommunizieren miteinander über eine entsprechende Schnittstelle. Das Staking auf dem Consensus Layer ermöglicht es Validatoren, Blöcke zu erstellen und dadurch die auf dem Execution Layer stattfindenden Transaktionen und Smart-Contract-Interaktionen zu bestätigen.

Nach Beendigung des Staking-Prozesses kann der Stake in Ethereum aufgrund des einschlägigen Lock-Up-Mechanismus nicht unmittelbar zurückgezogen werden. Das Protokoll gibt den konkreten *Unstaking*-Prozess vor, wozu namentlich auch die Withdrawal bzw. Exit Queue gehört. Dieser Mechanismus sorgt dafür, dass die Anzahl der Validatoren nicht zu rasch abfällt, was den Konsensprozess und dadurch das Netzwerk destabilisieren könnte. Aus demselben Grund existiert umgekehrt eine Entry Queue in Ethereum: Erst nach Ablauf dieser Wartezeit nimmt der Validator an der Validierung teil. Die Dauer der jeweiligen Queue hängt von der sog. *Churn Limit* ab. Diese gibt vor, wie viele Validator Nodes pro Epoche gleichzeitig staken bzw. unstaken können. Wenn eine grössere Zahl an Validator Nodes im Netzwerk aktiv ist, können auch mehr neue Nodes pro Epoche ein- und austreten. Bei einer Churn Limit von 14 etwa bedeutet dies, dass alle 6 Minuten 24 Sekunden 14 Validator Nodes ihre ETH unstaken bzw. staken können (Stand 29.02.2024).

## 2.3 Marktentwicklungen

Der Markt für Staking ist in den letzten Jahren rapide gewachsen. Die meisten neueren Blockchainsysteme verwenden eine Version von Proof-of-Stake für die Konsensfindung. Gemäss der Webseite «Staking Rewards» (stakingrewards.com) erreichte die Gesamtmarktkapitalisierung der gestakten Vermögenswerte in PoS-Netzwerken Ende Februar 2024 über 300 Milliarden US-Dollar.

Einer der Haupttreiber dieses Wachstums ist die zunehmende Nachfrage im Krypto-Ökosystem nach Möglichkeiten, den bestehenden Kryptowährungsbestand zu bewirtschaften. Wie oben erwähnt, ermöglicht Staking, ein Entgelt für die Sicherung des Netzwerks zu erhalten. Ein weiterer Faktor, der das Wachstum des Stakings fördert, ist die Energieeffizienz von PoS- im Vergleich zu PoW-Konsensmechanismen. PoS-Netzwerke benötigen deutlich weniger Energie als PoW-Netzwerke wie Bitcoin. Für die Zukunft glauben viele Experten, dass Staking- und PoS-Protokolle weiterhin ein erhebliches Wachstum verzeichnen werden, da immer mehr Blockchain-Netzwerke diesen Mechanismus übernehmen werden. Zusätzlich erhöhen *Liquid Staking*-Lösungen, die es Personen ermöglichen, Staking Rewards zu erhalten und gleichzeitig ihre gestakten Vermögenswerte zu übertragen, bereits heute die Attraktivität des Stakings für Marktteilnehmer.

Es gibt jedoch auch potenzielle Herausforderungen und Risiken im Zusammenhang mit Staking, wie z.B. die Zentralisierung der Konsensmechanismen in den Händen weniger Staking-Anbieter. Für die Entwicklung der Staking-Protokolle dürfte es wichtig sein, diese Probleme anzugehen, um die langfristige Nachhaltigkeit und Sicherheit der Blockchain-Netzwerke zu gewährleisten.

Grafik 2: Übersicht der derzeit bedeutendsten PoS-Protokolle

| Name | Ticker | Reward Rate p.a. | Staking Ratio | Staking Market Cap in USD |
|---|---|---|---|---|
| **Ethereum** | ETH | 3.85% | 25.85% | 107.91 Mrd. |
| **Solana** | SOL | 7.15% | 67.91% | 47.70 Mrd. |
| **Cardano** | ADA | 3.06% | 64.31% | 15.76 Mrd. |
| **Sui** | SUI | 3.59% | 82.85% | 13.17 Mrd. |
| **Avalanche** | AVAX | 8.53% | 59.43% | 10.88 Mrd. |
| **Aptos** | APT | 7.00% | 81.57% | 10.67 Mrd. |
| **Celestia** | TIA | 14.50% | 52.70% | 9.15 Mrd. |
| **BNB Chain** | BNB | 2.24% | 14.19% | 9.07 Mrd. |
| **Polkadot** | DOT | 11.82% | 52.41% | 6.43 Mrd. |
| **Tron** | TRX | 4.15% | 50.66% | 6.38 Mrd. |

*Quelle: stakingrewards.com, per 29.02.2024

Quelle: stakingrewards.com, per 29. Februar 2024

## 2.4 Erscheinungsformen

Beim Staking lassen sich mehrere Erscheinungsformen unterscheiden. Im Folgenden wird eine praxisnahe Darstellung der Erscheinungsformen anhand der Bereiche (i) *Funktionsweise*, (ii) *Custody* und (iii) *Lock-Up Mechanismen* vorgenommen:

### 2.4.1 Funktionsweise

Je nach Protokoll und der damit zusammenhängenden Ausgestaltung des Konsensmechanismus gibt es unterschiedliche Varianten von PoS. Im Folgenden werden in Kurzform die wichtigsten Konsensmechanismen beschrieben und deren Vor- und Nachteile erläutert.

#### 2.4.1.1 Proof-of-Stake (PoS)

*PoS* ist der häufigste Staking-Mechanismus, der von vielen beliebten Kryptowährungen verwendet wird, wie etwa Ethereum, Polygon, Solana und Binance Coin. PoS ermöglicht es den Inhabern von Kryptowährungen, am Validierungsprozess des Netzwerks teilzunehmen, indem sie ihre Token staken. Validatoren werden auf der Grundlage der Anzahl der gestakten Token ausgewählt, wobei höhere Stakes die Chance proportional erhöhen, ausgewählt zu werden. PoS gilt im Allgemeinen als energieeffizienter als PoW und bietet in der Regel kürzere Transaktionsverarbeitungszeiten. PoS kann potentiell jedoch auch zu einer stärkeren Zentralisierung führen, da Personen mit grossen Stakes mehr Einfluss auf den Validierungsprozess des Netzwerks haben.

#### 2.4.1.2 Delegated Proof-of-Stake (DPoS)

*Delegated Proof-of-Stake* ist eine Abwandlung von PoS, die von Kryptowährungen wie Cardano, EOS und Tron verwendet wird. Bei DPoS können die Inhaber von Kryptowährungen für eine begrenzte Anzahl von Validatoren stimmen, die dann für die Validierung von Transaktionen des Netzwerks verantwortlich sind. DPoS ist im Allgemeinen schneller und energieeffizienter als PoW und PoS, erhöht jedoch auch das Risiko der Zentralisierung, da u.U. eine kleine Gruppe von Validatoren eine erhebliche Kontrolle über das Netzwerk ausüben kann.

#### 2.4.1.3 Proof-of-Authority (PoA)

*Proof-of-Authority* ist ein Staking-Mechanismus, der von einigen kleineren Kryptowährungen wie POA Network und GoChain verwendet wird. Bei PoA werden Validatoren basierend auf ihrer Identität, Reputation und Vertrauenswürdigkeit ausgewählt. Dies macht PoA weniger anfällig für unerkannte Zentralisierung und weniger ressourcenintensiv als andere Staking-Mechanismen. PoA kann jedoch insgesamt weniger dezentralisiert und anfälliger für Angriffe sein, da die Validatoren weniger zahlreich und darum einfacher anzugreifen sind.

#### 2.4.1.4 Proof-of-Burn (PoB)

*Proof-of-Burn* ist ein Staking-Mechanismus, der von einigen kleineren Kryptowährungen wie bspw. Counterparty verwendet wird. Bei PoB senden Inhaber von Kryptowährungen ihre Token an eine spezifische Adresse mit dem Ziel, sie unwiderruflich zu «vernichten» (sog. *Burning*). Diese Aktion beweist das Engagement des Inhabers für das Netzwerk und ermöglicht es ihm, am Validierungsprozess teilzunehmen. PoB gilt im Allgemeinen als energieeffizienter als andere Staking-Mechanismen, da keine signifikante Rechenleistung erforderlich ist. PoB kann jedoch auch zu deflationären Tendenzen und einen Mangel an Liquidität führen, da die Token aus dem Umlauf genommen werden.

#### 2.4.1.5 Liquid Proof-of-Stake (LPoS)

*Liquid Proof-of-Stake* ist ein Staking-Mechanismus, der von der Kryptowährung Tezos verwendet wird. Bei LPoS können Inhaber von Kryptowährungen ihren Stake an mehrere Validatoren delegieren anstatt auf einen einzigen Validator beschränkt zu sein. Dies ermöglicht mehr Flexibilität und verringert das Risiko der Zentralisierung, da kein einzelner Validator zu viel Einfluss auf das Netzwerk ausüben kann.

#### 2.4.1.6 Hybrid Proof-of-Stake (HPoS)

*Hybrid Proof-of-Stake* ist eine Kombination aus PoW und PoS und wird von Kryptowährungen wie Decred und Peercoin verwendet. Bei HPoS wird PoW verwendet, um neue Blöcke zu generieren; PoS wird hingegen angewendet, um diese Blöcke zu validieren. Dies ermöglicht mehr Sicherheit und Dezentralisierung, da sowohl PoW-Miner als auch PoS-Validatoren eine Rolle bei der Aufrechterhaltung des Netzwerks spielen. HPoS kann jedoch komplexer und ressourcenintensiver sein als andere Staking-Mechanismen.

#### 2.4.1.7 Masternodes

Der Einsatz von *Masternodes* beruht auf einem Staking-Mechanismus, der von einigen Kryptowährungen wie Dash und PIVX verwendet wird. Masternodes sind spezielle Knotenpunkte im Netzwerk, die eine erhebliche Menge an Kryptowährung benötigen, um eine Validator Node zu betreiben. Masternodes erfüllen verschiedene Funktionen, wie die Verarbeitung von Transaktionen, die Aufrechterhaltung der Netzwerkinfrastruktur und die Abstimmung über Vorschläge zur Verbesserung des Netzwerks. Masternode-Betreiber erhalten einen Teil der Staking Rewards als Entschädigung für ihre Dienste. Masternodes können erhöhte Sicherheit und Dezentralisierung bieten, erfordern jedoch auch eine erhebliche Menge an Startkapital.

### 2.4.2 Custody

#### 2.4.2.1 Non-Custodial

Non-Custodial Staking kann in der Praxis im Wesentlichen in zwei Formen betrieben werden: (i) *Self- bzw. Solo Staking* und (ii) *Staking-as-a-Service (SaaS)*.

Beim Self-Staking erbringt der Nutzer alle für das Staking notwendigen Elemente aus eigener Kraft. D.h., der Nutzer verwahrt nicht nur selbst den Private Key zu den gestakten Token, sondern er betreibt (auf eigene Rechnung) auch die Soft- und Hardware für die Teilnahme am Netzwerk. Beim SaaS verwahrt der Nutzer die Private Keys selbst, verlässt sich für die Ausführung des Stakings aber auf die technische Infrastruktur eines Dritten.

Formen des Non-Custodial Stakings ermöglichen es Nutzern, die volle Kontrolle über die Private Keys ihrer Token zu behalten. Non-Custodial Staking kann langfristig kostengünstiger als Custodial Staking sein, da keine Gebühren oder – bei SaaS – tiefere Gebühren anfallen. Allerdings gibt es auch Nachteile beim Non-Custodial Staking, vor allem in der Form des Self-Stakings. So sind beim Self-Staking ein höheres technisches Wissen und eine entsprechende Infrastruktur im Vergleich zum Custodial Staking notwendig, was für viele Personen eine zu hohe Einstiegshürde darstellen könnte. Entsprechend hat sich in der Praxis die Form des SaaS herausgebildet, welche es dem Nutzer erlaubt, die technische Infrastruktur einer Drittperson zu verwenden, ohne die Kontrolle über die gestakten Vermögenswerte aufgeben zu müssen. Mit diesem Modell ist allerdings immer noch ein erhöhtes Risiko verbunden, den Zugriff auf die Token aufgrund einer unsorgfältigen Selbstverwahrung zu verlieren.

#### 2.4.2.2 Custodial

In der Praxis können im Wesentlichen zwei Formen des Custodial Stakings unterschieden werden: (i) herkömmliches Custodial Staking und (ii) Sub-Custodial Staking.

*Custodial Staking* bezieht sich auf die Praxis, für die Aufbewahrung und das Staking der Kryptowährungen einen Staking-Anbieter (Custodian) zu beauftragen, der in der Regel auf Rechnung und Risiko des Kunden die Token hält und in dessen Auftrag stakt. In diesem Fall muss der Kunde die für das Staking erforderliche Hard- und Software nicht selbst betreiben und unterhalten. Eine besondere Art des Custodial Stakings ist das *Sub-Custodial Staking*: In diesem Fall zieht der Staking-Anbieter (Custodian/Hauptverwahrer) eine Drittperson (Sub-Custodian/Unterverwahrer) für die Aufbewahrung der Token und die Erbringung von Staking-Dienstleistungen bei.

Einer der Hauptvorteile von Custodial Staking besteht darin, dass es für den stakenden Kunden weniger technisches Wissen erfordert als beim Non-Custodial Staking. Der Custodial Staking-Dienstleister verpflichtet sich vertraglich sodann regelmässig dazu, die Token des Kunden sicher aufzubewahren. Darüber hinaus können Kunden von Custodial Staking-Anbietern oftmals am Konsensmechanismus eines PoS-Protokolls teilnehmen, ohne die von gewissen Protokollen verlangte Mindestzahl an Token bereitstellen zu müssen, was eine erhebliche Hürde des Non-Custodial Stakings sein kann.[5]

[5] Für Staking in Ethereum ist ein Minimum-Stake von 32 ETH notwendig, der bei den heutigen Marktpreisen rund 90’000 Fr. entspricht (Stand 29.02.2024).

Das Custodial Staking ist ebenfalls nicht frei von Risiken für die stakenden Kunden. Namentlich vertrauen stakende Kunden einer Drittperson, dass diese ihre Token sicher aufbewahren und das Staking in ihrem Einverständnis ausführen.

### 2.4.3 Lock-Up Mechanismen

#### 2.4.3.1 Native Staking

*Native Staking* bezieht sich auf die Praxis, eine Kryptowährung mit Hilfe des Blockchain-Protokolls zu staken, das die Kryptowährung herausgibt. Mit anderen Worten ist der Staking-Prozess in das PoS-Protokoll selbst integriert. Dabei ist regelmässig und ausschliesslich die Blockierung von Token zwecks Teilnahme am Konsensmechanismus und Generierung von Staking Rewards beabsichtigt.

Einer der Hauptvorteile von Native Staking ist, dass es eine höhere Sicherheit und Effizienz bieten kann, da der Staking-Prozess direkt in die der Kryptowährung zugrundeliegende Technologie integriert ist.

Native Staking bedeutet aber auch, dass die Protokollbedingungen eins zu eins auf das Staking zur Anwendung gelangen. Hierzu gehören namentlich auch Lock-Ups, soweit ein PoS-Protokoll solche vorsieht. Während eines Lock-Ups kann die stakende Person nicht frei über die gestakten Token verfügen. Soweit Lock-Ups vorliegen, dauern sie in der Regel von wenigen Minuten und Stunden bis zu einigen Tagen. Die Polkadot Blockchain etwa hat eine Lock-Up von rund 28 Tagen.

#### 2.4.3.2 Liquid Staking

*Liquid Staking* ist ein Protokoll, dass es Nutzern ermöglicht, trotz Lock-Up über den wirtschaftlichen Wert der Staking-Position frei zu verfügen.

Konkret ermöglicht Liquid Staking den Nutzern des Protokolls, ihre Staking-Positionen in liquiden Token abzubilden, die an ihre Wallets übertragen werden. Diese liquiden Token sind sodann frei übertragbar und können etwa in dezentralen Protokollen verwendet werden. Die liquiden Token können schliesslich wieder an das Protokoll zurückübertragen werden, um die bestehende Staking-Position aufzulösen.

## 2.5 Rollen

Die Hauptakteure in einem PoS-Netzwerk sind im Wesentlichen Validatoren, Staker und Entwickler.

### 2.5.1 Validator

Unter einem Validator versteht man einen Knotenpunkt (sog. *Node*) im Blockchain-Netzwerk, der für die Validierung von Transaktionen und deren Eintragung in das verteilte Register (d.h. die Blockchain) verantwortlich ist. Validatoren übernehmen eine existenzielle Rolle bei der Aufrechterhaltung der Integrität und Sicherheit des Blockchain-Netzwerks. Zu diesem Zweck betreiben Validatoren die für ihre Aktivitäten notwendige Hard- und Software.

Der Betrieb von Validator Nodes kann je nach Protokoll mit grösseren Anschaffungs- und Betriebskosten verbunden sein. Zudem setzen Betrieb und Wartung der Hard- und Software eine gewisse technische Expertise voraus.

### 2.5.2 Staker

Ein Staker ist eine Person oder Organisation, die am Staking-Prozess einer PoS-Blockchain teilnimmt. Beim Staking wird eine bestimmte Menge einer Kryptowährung als Sicherheit hinterlegt, um am Konsensmechanismus des Netzwerks teilzunehmen und Staking Rewards für die Validierung von Transaktionen zu erhalten. Durch das Staken ihrer Kryptowährung tragen Staker dazu bei, das Netzwerk abzusichern und ein ordnungsgemässes Funktionieren sicherzustellen, sowie potenzielle betrügerische Aktivitäten zu verhindern. Staker haben abhängig vom PoS-Protokoll auch die Möglichkeit, an der Governance der Blockchain, wie namentlich an der Abstimmung über Protokoll-Upgrades oder Änderungen der Netzwerkregeln, teilzunehmen.

Staker nutzen Validator Nodes, um am Staking-Prozess teilzunehmen. Entweder betreiben sie selbst solche Nodes oder aber sie verlassen sich auf die Dienstleistungen Dritter in diesem Bereich (so z.B. beim Custodial Staking). Die Vorteile einer Delegation an einen Staking-Anbieter liegen für den Staker in der einfachen Handhabung des Stakings und dem Wegfall der Anschaffungskosten.

### 2.5.3 Entwickler

Die Rolle von Entwicklern kann sehr vielfältig sein. Sie entwickeln und implementieren Staking-Protokolle, programmieren den Staking-Mechanismus, betreiben Nodes, um das Netzwerk zu unterstützen und/oder entwickeln notwendige Wallets und die dazugehörige Software. Zudem kümmern sie sich um die Sicherheit und Wartung der Infrastruktur und führen Protokoll-Upgrades durch. Ihre Arbeit trägt zur Stabilität, Sicherheit und Leistung des Netzwerks bei und gewährleistet einen reibungslosen Staking-Prozess für den Staker. Auch Sicherheitsaudits und Fehlerbehebungen können zu ihren Aufgaben gehören, wobei solche heutzutage oftmals an spezialisierte Firmen ausgelagert werden, nicht zuletzt um die Objektivität der Prüfungen zu wahren.

## 2.6 Chancen und Risiken

Staking ist ein innovatives Konzept, welches noch sehr neu ist, aber dennoch bereits sehr viel Anklang bei Krypto- und traditionellen Marktteilnehmern findet. Im Folgenden sollen einige der wichtigsten Chancen erläutert werden, wobei in einem zweiten Schritt die Risiken beschrieben werden.

### 2.6.1 Chancen

#### 2.6.1.1 Bewirtschaftung von Kryptowährungsbeständen

Staking ermöglicht es Einzelpersonen und Organisationen, mit ihren bestehenden Kryptowährungsbeständen durch Teilnahme am Netzwerk ein Entgelt in Form von Staking Rewards zu erzielen.

#### 2.6.1.2 Niedrige Einstiegshürden

Staking ist im Allgemeinen zugänglicher als andere Konsensmechanismen. Im Gegensatz zum Mining, das spezialisierte Hardware und technisches Wissen erfordert, kann Staking in vielen Fällen ohne spezielle Hardware durchgeführt werden.

#### 2.6.1.3 Netzwerk Teilnahme und Dezentralisierung

Durch das Staking ihrer Kryptowährung können Einzelpersonen und Unternehmen aktiv am Betrieb des Blockchain-Netzwerks teilnehmen. Staker haben ein persönliches Interesse am Erfolg des Netzwerks und sind motiviert, im besten Interesse des Netzwerks zu handeln. Diese Motivation hilft, die Dezentralisierung des Netzwerks zu fördern, welches ein Kernelement öffentlicher Blockchain-Protokolle ist.

#### 2.6.1.4 Sicherheit und Integrität

Staking trägt dazu bei, die Sicherheit und Integrität des Blockchain-Netzwerks zu gewährleisten. Staker tragen zur Validierung von Transaktionen und deren Hinzufügung zur Blockchain bei. Dieser Prozess hilft, Doppelausgaben («double spending») und andere Formen von betrügerischen Aktivitäten im Netzwerk zu verhindern.

#### 2.6.1.5 Beteiligung an der Governance

Staker haben u.U. die Möglichkeit, an der Governance eines Netzwerks teilzunehmen, wie z.B. an der Abstimmung über Protokoll-Upgrades und Änderungen der Netzwerkregeln. Diese Form der Beteiligung gibt Stakern eine Stimme in der Ausrichtung und Entwicklung des Netzwerks und trägt dazu bei, die Kontrolle über eine Blockchain zu «demokratisieren».

### 2.6.2 Risiken

Wie fast jede Tätigkeit weist auch das Staking von Kryptowährungen Risiken auf:

#### 2.6.2.1 Marktschwankungen

Die Höhe der Staking Rewards hängt von vielen Faktoren ab, die in der Regel weder der Staker noch die Betreiber von Validator Nodes bestimmen können. So wirkt sich etwa die Preisvolatilität der gestakten Token auf die Staking Rewards aus.

#### 2.6.2.2 Netzwerkprobleme

Netzwerkfehler, ein Unterbruch der Internetverbindung oder gar ein Cyberangriff auf eine Blockchain können dazu führen, dass Staker die in Aussicht stehenden Staking Rewards und im Extremfall die gestakten Token verlieren.

#### 2.6.2.3 Slashing-Risiko

Konzeptionell können unterschiedliche Formen von Slashing unterschieden werden, die je nach Ausprägung auch als «Penalties» bezeichnet werden. In Ethereum etwa besteht bei protokollwidrigem Verhalten eines Stakers das Risiko, absehbare Staking Rewards nicht zu erhalten (Penalties) oder einen Teil des Stake oder im Extremfall den gesamten Stake zu verlieren (Slashing).

Das Slashing-Risiko besteht unabhängig davon, ob Staking in Non-Custodial oder in Custodial Form betrieben wird. Wie weiter unten erwähnt (siehe Ziff. 5.3.2.2), können die Risiken des Slashings transparent gemacht und die Risikotragung vertraglich offengelegt und entsprechend zwischen dem Staking-Anbieter und dem Kunden aufgeteilt werden.

# 3. Zivilrecht

Um die Rechtsverhältnisse beim Staking zivilrechtlich einzuordnen, ist zwischen den verschiedenen Modellen von Staking zu differenzieren (siehe oben Ziff. 2.4.2).

## 3.1 Self-Staking

Self-Staking ist eine Art des Non-Custodial Stakings. Beim *Self-Staking* führt die stakende Person alle notwendigen technischen und operativen Schritte selbst aus: Sie betreibt eine Validator Node, um am Konsensmechanismus des Protokolls teilzunehmen, und ist für die Aufbewahrung der Private Keys der gestakten Token selbst verantwortlich. Diese Form der Teilnahme setzt je nach Protokoll und gewähltem Setup eine gewisse technische Expertise des Nutzers voraus. Abgesehen von allfälligen Software-Lizenzvereinbarungen zwischen Entwickler und Nutzer bestehen beim Self-Staking grundsätzlich keine vorliegend relevanten Rechtsverhältnisse. Namentlich möchte sich der Staker in aller Regel auch nicht gegenüber den anderen Validatoren des dezentralen Netzwerks in irgendeiner Weise verpflichten.

## 3.2 Staking-as-a-Service

Beim Non-Custodial Staking in Form des *Staking-as-a-Service (SaaS)* bewahrt der Kunde die Private Keys ebenfalls in seiner eigenen Wallet auf, greift aber für die Validierung von Transaktionen und Blöcken auf die Dienstleistungen eines Staking-Anbieters zurück. Die Dienstleistungen des Staking-Anbieters beschränken sich in der Regel auf die Zurverfügungstellung der notwendigen Hard- und Software.

Der Staking-Anbieter kann nur bis zu einem gewissen Grad beeinflussen, dass das Protokoll dem Kunden Staking Rewards ausbezahlt. Dies zeigt sich darin, dass nicht der Staking-Anbieter, sondern das Protokoll in algorithmischer Weise die zu vergütenden Validator Nodes auswählt, das Protokoll jedoch dem Kunden weder das Bestehen noch die Höhe von Staking Rewards zusichert. In aller Regel besteht keine im Voraus festgelegte, regelmässige Frequenz für die Ausschüttung von Staking Rewards und in den meisten Fällen kann auch die Höhe der Staking Rewards nicht vorab bestimmt werden. Darüber hinaus sind Fälle denkbar, in denen dem Kunden ein Slashing trotz des sorgfältigen Betriebs von Hard- und Software durch den Staking-Anbieter widerfährt (z.B. aufgrund eines generellen Programmierfehlers, der alle Validator Nodes gleichermassen trifft). Daraus folgt, dass der Staking-Anbieter seinem Kunden keinen Erfolg, sondern nur ein sorgfältiges Tätigwerden im auftragsrechtlichen Sinne schuldet.[6]

[6] Siehe Bruno Pasquier/André Lopes Vilar de Ouro, Le recours aux services de tiers lors du staking de Cryptomonnaies, AJP 2022, S. 1081.

Auch wenn durch die Bereitstellung, den Betrieb und die Wartung der Hard- und Software durch den Staking-Anbieter (z.B. die Durchführung notwendiger Softwareupdates) gewisse lizenzvertragliche und werksvertragsähnliche Elemente hinzutreten können, qualifiziert der Vertrag zwischen dem Kunden und dem Staking-Anbieter typischerweise als Innominatkontrakt mit vorwiegend auftragsrechtlichen Elementen.

## 3.3 Custodial Staking

Beim *Custodial Staking* führt der Staking-Anbieter nicht nur die Validierung der Transaktionen auf der Blockchain im Auftrag und auf Rechnung des Kunden durch, sondern bewahrt auch die kryptobasierten Vermögenswerte für den Kunden auf. Nach der von der FINMA in der Aufsichtsmitteilung 08/2023 verwendeten Terminologie handelt es sich um ein sog. *Direct Staking*.

Der Staking-Anbieter hält beim Custodial Staking in seinem Wallet die Private Keys der stakenden Kunden. Der Kunde hat grundsätzlich keine Möglichkeit, *direkt* auf seine Vermögenswerte zuzugreifen und diese selbst zu staken bzw. unzustaken. Im Unterschied zum vorstehend beschriebenen Non-Custodial Staking erfolgt somit jegliche Interaktion mit dem Staking-Protokoll durch den Staking-Anbieter. Zu diesem Zweck kann der Staking-Anbieter eigene Hard- und Software betreiben oder aber auf die Validator Node einer Drittperson zurückgreifen (wobei diese Drittperson keine Vermögenswerte aufbewahrt; siehe hingegen zum Sub-Custodial Staking sogleich).

Die reine Aufbewahrung von kryptobasierten Vermögenswerten für einen Kunden wird mangels hinterlegungsfähiger beweglicher Sache von der juristischen Lehre als Auftrag qualifiziert.[7] Der Auftrag weist allerdings einen ausgeprägten Hinterlegungscharakter auf. Wenn die hinterlegten Token *zusätzlich* gestakt werden, handelt es sich beim fraglichen Rechtsverhältnis weiterhin um ein Auftragsverhältnis,[8] das nunmehr Elemente der Aufbewahrung mit Elementen des Stakings kombiniert: Der Custodial Staking-Anbieter hat für den Kunden die Private Keys, welche den Zugriff auf die gestakten kryptobasierten Vermögenswerte vermitteln, weiterhin sicher aufzubewahren. Das vorbestehende auftragsrechtliche Rechtsverhältnis mit Hinterlegungscharakter wird somit durch den Staking-Auftrag nicht aufgehoben, sondern lediglich vom Staking-Auftragsverhältnis *überlagert*.[9]

Soweit der Staking-Anbieter selbst die Validator Nodes betreibt, können werkvertragsähnliche Elemente hinzutreten. Im Ergebnis ist der Vertrag in diesem Fall regelmässig (wiederum) als Innominatkontrakt mit vorwiegend auftragsrechtlichen Elementen zu qualifizieren.

## 3.4 Sub-Custodial Staking

Beim sog. *Sub-Custodial Staking* nutzt der Staking-Anbieter (Custodian) für die Aufbewahrung der Private Keys und ggf. weitere Dienstleistungen eine Drittperson (sog. Sub-Custodian), die zusätzlich die notwendige Hard- und Software für den Custodian betreibt (oder aber zu diesem

[7] Siehe Nicolas Jacquemart/Stephan D. Meyer, Der Bitcoin-/Bitcoin-Cash-Hardfork, S. 478 ff.; Benedikt Maurenbrecher/Urs Meier, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen, Jusletter 04.12.2017, Rz. 22.
[8] Siehe Bruno Pasquier/André Lopes Vilar de Ouro, Le recours aux services de tiers lors du staking de Cryptomonnaies, AJP 2022, S. 1081.
[9] *Gl.M.* Fabio Andreotti/Stephan Zimmermann/Florian Prantl, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, S. 338 f.

Zweck wiederum eine Drittperson bezieht), um im Auftrag der Kunden des Staking-Anbieters am Konsensmechanismus des Protokolls teilzunehmen.

Zivilrechtlich handelt es sich in diesem Fall um eine Kette von Auftragsverhältnissen (bzw. ähnlich gelagerten treuhänderischen Rechtsverhältnissen) zwischen dem Kunden und dem Staking-Anbieter bzw. Custodian, dem Staking-Anbieter bzw. Custodian und dem Sub-Custodian und ggf. zwischen dem Sub-Custodian und der Drittperson, welche die Validator Node betreibt.

Demgegenüber ist aufgrund der jeweiligen Verfolgung eigener Interessen mit unterschiedlichen Mitteln nicht von einer einfachen Gesellschaft zwischen den beiden Parteien auszugehen.

Um Sub-Custodial Staking-Setups vom Direct Staking abzugrenzen, verwendet die FINMA in der Aufsichtsmitteilung 08/2023 den Begriff der sog. *Staking-Ketten*. Nach der von der FINMA verwendeten Definition «[...] werden [bei Staking-Ketten] die zu stakenden kryptobasierten Vermögenswerte vom Dienstleister mit der Kundenbeziehung an ein oder mehrere Dritte weitergegeben, die den Validator Node betreiben [...]». Um Missverständnisse zu vermeiden, sei hier klargestellt, dass ausschliesslich die zu stakenden Token der Kunden an den Sub-Custodian weitergegeben werden, die Kundenbeziehung selbst verbleibt beim Custodian und Staking-Anbieter.

## 3.5 Fazit

Staking-Anbieter schulden ihren Kunden ein sorgfältiges Tätigwerden gemäss Auftragsrecht (Art. 398 Abs. 2 OR). Hinterlegungs-, lizenz- und/oder werkvertragsähnliche Pflichten können hinzutreten, soweit der Staking-Anbieter auch den Betrieb und Unterhalt von Hard- und Software schuldet.

Die zivilrechtliche Einordnung von Staking-Rechtsverhältnissen als Auftrag legt nahe, dass der Staking-Anbieter den Kunden über die mit Staking verbundenen Risiken *aufzuklären* hat. Das Vorgehen kann ähnlich zur Risikoaufklärung im Rahmen des Vertriebs von Finanzprodukten ausgestaltet sein (z.B. durch Hinweis auf die Verlustrisiken der gestakten Token aufgrund von Slashing). Details zur Risikoaufklärung und der entsprechenden Ausgestaltung sind unter Ziff. 5.3.2.2 ausgeführt.

Abschliessend sei erwähnt, dass die Qualifikation von Staking-Verträgen als Auftrag dazu führt, dass diese gemäss Art. 405 Abs. 1 OR mit der Konkurseröffnung über den Staking-Anbieter grundsätzlich erlöschen, sofern die Parteien nicht das Gegenteil vereinbart haben oder das Gegenteil aus der Natur des Geschäfts hervorgeht. Dies wäre bei einer Qualifikation als Werkvertrag anders, da dieser auch nach Konkurseröffnung fortdauern würde. Es kann u.E. deshalb empfehlenswert sein, in den Staking-Verträgen eine ausdrückliche Bestimmung vorzusehen, welche das Schicksal der Staking-Verträge nach Konkurseröffnung im Interesse der Parteien regelt.

# 4. Konkursrecht

## 4.1 Einleitung

Die 2021 in Kraft getretene DLT-Gesetzgebung hat u.a. zur Einführung von Tatbeständen im Zusammenhang mit der Herausgabe von kryptobasierten Vermögenswerten im Konkurs des Aufbe-

wahrers geführt. Davon erfasst ist nicht nur die bankenrechtliche Absonderbarkeit von Depotwerten bei Banken und Personen nach Art. 1b BankG (siehe hierzu unten Ziff. 5.3), sondern auch die konkursrechtliche Aussonderung von kryptobasierten Vermögenswerten im Konkurs eines Aufbewahrers.

Damit Vermögenswerte überhaupt in die Konkursmasse fallen, muss der Gemeinschuldner zum Zeitpunkt der Konkurseröffnung die *ausschliessliche tatsächliche Verfügungsmacht* über den Vermögenswert innehaben (vgl. Art. 242a Abs. 1 SchKG). Es fallen diejenigen Vermögenswerte in die Konkursmasse, auf welche die berechtigte Person keinen eigenen Zugriff hat und bei denen der Gemeinschuldner über sämtliche notwendigen Private Keys verfügt, um selber unmittelbar darüber verfügen zu können: Kann der Dritte selber über den Vermögenswert verfügen, so ist eine Herausgabe nicht erforderlich; kann die Konkursverwaltung nicht eigenständig darüber verfügen, so ist eine Herausgabe nicht möglich.[10] In letzterem Fall ist bei gegebenen Voraussetzungen dagegen zu prüfen, ob der Private Key gestützt auf Art. 242b SchKG («Zugang zu Daten und deren Herausgabe») herausverlangt werden kann.

Die Aussonderung im Konkurs ermöglicht die Herausgabe kryptobasierter Vermögenswerte: Gemäss Art. 242a Abs. 1 SchKG trifft die Konkursverwaltung eine Verfügung über die Herausgabe kryptobasierter Vermögenswerte, über die der Gemeinschuldner zum Zeitpunkt der Konkurseröffnung die Verfügungsmacht innehat und die von einem Dritten beansprucht werden. Nach Art. 242a Abs. 2 SchkG ist der Anspruch des Dritten dann begründet, wenn der Gemeinschuldner sich verpflichtet hat, die kryptobasierten Vermögenswerte für den Dritten jederzeit bereitzuhalten und diese (a) dem Dritten individuell zugeordnet sind oder (b) einer Gemeinschaft zugeordnet sind und ersichtlich ist, welcher Anteil am Gemeinschaftsvermögen dem Dritten zusteht.

Mit dem Begriff «kryptobasierte Vermögenswerte» sind alle Vermögenswerte gemeint, bei denen die Verfügungsmacht ausschliesslich über ein kryptobasiertes Zugangsverfahren vermittelt wird, womit andere unkörperliche oder digitale Vermögenswerte, etwa rein obligatorische Forderungsansprüche oder geldwerte Datensammlungen und Informationen, nicht Gegenstand der Regelung sind.[11]

Es ist darauf hinzuweisen, dass die Regelung in Art. 242a SchKG nur zur Anwendung kommt, wenn kein anderer konkursrechtlicher Herausgabetatbestand vorliegt, so insbesondere, wenn die kryptobasierten Vermögenswerte nicht im Rahmen der Bestimmungen über die Absonderung von Depotwerten gemäss BankG ausgehändigt werden können.[12] Namentlich ist Art. 16 Ziff. 1$^{bis}$ BankG für das Staking von kryptobasierten Vermögenswerten relevant (siehe hierzu unten Ziff. 5.3).

[10] Siehe BBl 2020, S. 292; ferner Kilian Schärli/Luzius Meisser/Reto Luthiger, Finanzmarktrechtliche Einordnung des Stakings von Kryptowährungen, Jusletter IT 30.09.2021, Rz. 16 ff.
[11] Siehe BBl 2020, S. 292.
[12] Siehe BBl 2020, S. 291.

## 4.2 Aussonderung im Konkurs

### 4.2.1 Vorbemerkungen

Das Aussonderungsregime von Art. 242a SchKG ist nicht nur für die reine Kryptoverwahrung relevant, sondern kann aufgrund der Überlagerung der Aufbewahrung durch das Staking-Rechtsverhältnis (siehe hierzu oben Ziff. 3.3) auch auf die Herausgabe von gestakten Token im Konkurs eines Custodial Staking-Anbieters Anwendung finden.

Im Zusammenhang mit der Verwahrung der gestakten Token ist festzuhalten, dass Staking protokollbedingt unterschiedlich ausgestaltet sein kann. In gewissen Fällen verbleiben die Token im ursprünglichen Wallet des Kunden beim Custodial Staking-Anbieter (so z.B. Tezos). In anderen Fällen werden sie an einen Smart Contract übertragen (so z.B. Polygon), wobei der ursprüngliche oder aber ein neuer (dedizierter) Private Key des Kunden typischerweise weiterhin die gestakte Position kontrolliert und entsprechend nur der Inhaber des Private Keys ein Unstaking veranlassen kann. In beiden Fällen bildet die fortlaufende Aufbewahrung der Private Keys der gestakten Token einen zentralen Aspekt der Beziehung zwischen Kunde und Staking-Anbieter.

Die Aussonderung gestakter kryptobasierter Vermögenswerte gemäss Art. 242a Abs. 1 i.V.m. Abs. 2 SchKG ist neben der ausschliesslichen tatsächlichen Verfügungsmacht grundsätzlich von *zwei Bedingungen* abhängig, nämlich der Pflicht zur jederzeitigen Bereithaltung der kryptobasierten Vermögenswerte (Ziff. 4.2.2) und der Pflicht zur Zuordnung der kryptobasierten Vermögenswerte zu den Kunden (Ziff. 4.2.3).

### 4.2.2 Pflicht zur jederzeitigen Bereithaltung

*Erstens* muss sich der Gemeinschuldner verpflichtet haben, die kryptobasierten Vermögenswerte jederzeit für den Dritten bereitzuhalten. «Jederzeit bereithalten» ist ein auslegungsbedürftiger Rechtsbegriff. Unklar ist insbesondere, ob es genügt, wenn die kryptobasierten Vermögenswerte (lediglich) ständig vorhanden sind, oder aber ob der Aufbewahrer sie auch jederzeit frei übertragen können muss.

Der Begriff der Pflicht zur jederzeitigen Bereithaltung wurde in der ersten Fassung dieses Zirkulars anhand der gängigen Methoden ausgelegt.[13] Im Ergebnis gelang das Zirkular zur klaren Auffassung, dass auch gestakte kryptobasierte Vermögenswerte als jederzeit bereitgehalten gelten können, und zwar selbst dann, wenn die betreffenden PoS-Protokolle Lock-Ups und/oder Slashing-Mechanismen aufweisen.[14]

Die zwischenzeitlich ergangene FINMA-Aufsichtsmitteilung 08/2023, welche die derzeitige Praxis der Eidgenössischen Finanzmarktaufsichtsbehörde festhält, bejaht die Aus- bzw. Absonderung gestakter Kundenvermögen bei Einhaltung gewisser Voraussetzungen.[15] Art. 242a SchKG ist primär für Staking-Anbieter *ohne* (relevante) finanzmarktrechtliche Bewilligung einschlägig. Für die Auslegung der Bestimmung sind in erster Linie die Praxis der Konkursbehörden und die Rechtsprechung der Zivilgerichte zu berücksichtigen.

[13] Die erste Fassung des Zirkulars ist verfügbar unter https://blockchainfederation.ch/downloads/.
[14] So etwa auch Fabio Andreotti/Stephan Zimmermann/Florian Prantl, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, S. 344 ff.
[15] Siehe hierzu unten Ziff. 5.3.1.

### 4.2.3 Pflicht zur Kundenzuordnung

#### 4.2.3.1 Vorbemerkung

Neben der Pflicht zur jederzeitigen Bereithaltung müssen *zweitens* die Vermögenswerte dem Dritten entweder individuell zugeordnet (Art. 242a Abs. 2 lit. a SchKG) oder aber einer Gemeinschaft zugeordnet sein, wobei in diesem Fall ersichtlich sein muss, welcher Anteil am Gemeinschaftsvermögen dem Dritten zusteht (Art. 242a Abs. 2 lit. b SchKG).

Erforderlich ist gemäss *lit. a*, dass jeder Token im Zeitpunkt der Konkurseröffnung individuell der berechtigten Person zugeordnet ist, was dadurch erreicht werden kann, dass die Token auf einem speziellen Konto bzw. in einer speziellen Wallet gehalten werden, die der berechtigten Person zugewiesen ist.[16] Es ist dabei ausreichend, wenn sich diese Zuordnung aus einem internen Register des Gemeinschuldners ergibt (z.B. eine Kundenverwaltungssoftware).[17] Soweit es technisch vorgesehen ist, dass die Token individualisiert werden können, indem bspw. jeder Token eine eigene «Seriennummer» hat, müssen sie nicht in einem Konto platziert werden, das jeweils der berechtigten Person zugeordnet ist, denn in diesem Fall ist die Voraussetzung der individualisierten Zuordnung auch erfüllt, wenn der einzelne, durch die Nummer spezifizierte Token mittels einer beim Gemeinschuldner verfügbaren Zuordnungstabelle der berechtigten Person zugeordnet werden kann.[18]

Sodann ist eine Aussonderung gemäss *lit. b* möglich, wenn die Vermögenswerte zwar nicht individuell, sie aber einer Gemeinschaft zugeordnet sind. Dabei muss gemäss Gesetz ersichtlich sein, welcher Anteil am Gemeinschaftsvermögen den einzelnen berechtigten Personen zusteht. Aussonderbar ist in diesem Fall der dem Dritten zustehende Anteil der vorhandenen Vermögenswerte. Auf diese Weise wird es möglich, die Token mehrerer Kunden auf einem Sammelkonto bzw. in einer Sammelwallet aufzubewahren.[19] Allerdings stellen sich in diesem Fall bankrechtliche Unterstellungsfragen (siehe unten Ziff. 5.2.2).

Die Frage der Zuordenbarkeit gestakter kryptobasierter Vermögenswerte löst eine Reihe von *Detailfragen* aus, die nachfolgend näher betrachtet werden:

#### 4.2.3.2 Zuordenbarkeit von Kundenadressen

Das Ziel der Zuordenbarkeit besteht in der systematischen Verknüpfung von konkreten Blockchain-Adressen, die für die eindeutige Zuweisung der Kunden-Token relevant sind, mit den Ansprüchen der Kunden gegenüber dem Custodian (wie insbesondere dem Anspruch auf Auslieferung der Tokens) in dessen internen Register. Da es sich bei der Frage der Zuordenbarkeit um ein eigenständiges Tatbestandsmerkmal handelt, ist es abhängig von den Umständen des Einzelfalls nicht zwingend erforderlich, jedoch regelmässig der Fall, dass die den Kunden zugewiesenen Blockchain-Adressen dem Custodian direkt die Verfügungsmacht über die kryptobasierten Vermögenswerte vermitteln.

[16] Siehe BBl 2020, S. 293.
[17] Siehe BBl 2020, S. 293.
[18] Siehe BBl 2020, S. 293.
[19] Siehe BBl 2020, S. 293.

Gemäss FINMA ist keine bankenrechtliche Bewilligungspflicht vorgesehen, wenn die gestakten kryptobasierten Vermögenswerte des Kunden «[...] weiterhin individuell verwahrt werden, d.h. pro Kunde eine separate und zuordenbare Blockchain-Adresse [...]» (S. 11) besteht.

Anders als bei der reinen Verwahrung können beim Staking je nach Protokoll *mehrere* Adressen für die Zuordnung infragekommen: Dies liegt im Wesentlichen daran, da beim Staking je nach Protokoll eine Verschiebung der Vermögenswerte in einen Smart Contract oder dergleichen zwecks Blockierung der Token für die Teilnahme am Konsensmechanismus vorgesehen sein kann.

Bei *Ethereum* handelt es sich etwa um die folgenden Adressen:

| **Adresse** | **Funktion** |
|---|---|
| Verwahrungsadresse (bzw. Deposit-Adresse) | Die zu stakenden Token gehen ab dieser Adresse des Staking-Anbieters in den Ethereum Staking Deposit Contract. |
| Staking-Adresse (bzw. Validator-Adresse) | Es handelt sich um die Adresse des Ethereum-Validators (bzw. der Validator Node), die mit den gestakten Token während des Stakings eindeutig verknüpft ist. |
| Withdrawal-Adresse | Token, die unstakt werden, gehen nach Beendigung des Stakings auf diese Adresse. In Ethereum ist diese Adresse auch als Empfängeradresse für die Staking Rewards des Consensus Layer relevant. |

Es ist nicht erforderlich, dass die ursprüngliche Verwahrungsadresse (d.h. die Deposit-Adresse), die Staking-Adresse (d.h. die Validator-Adresse) und die Withdrawal-Adresse zeitgleich jederzeit kundenspezifisch sind. Konkret haben die ursprüngliche Verwahrungsadresse und die Withdrawal-Adresse während des eigentlichen Staking-Vorgangs keine Relevanz für die Frage der Zuordnung der kryptobasierten Vermögenswerte zu einem Kunden. Es ist darum grundsätzlich davon auszugehen, dass *vor* der Ausführung des Staking-Auftrags des Kunden die ursprüngliche Verwahrungsadresse, *nach* der Ausführung des Staking-Auftrags des Kunden die Staking-Adresse und *nach* der Ausführung des Unstaking-Auftrags des Kunden die Withdrawal-Adresse jeweils dem Kunden zugeordnet ist. Der konkrete Zeitpunkt ist also massgebend für die Frage, welche der drei Adressen jeweils dem Staking-Kunden zuzuordnen ist.

Dies wird bei Ethereum-Staking etwa daran ersichtlich, dass die zu stakenden ETH an einen besonderen Smart Contract (sog. *Staking Deposit Contract*)[20] des Protokolls übertragen werden, weshalb die ursprüngliche Verwahrungsadresse grundsätzlich für die Frage der Zuordnung nicht mehr relevant sein kann. Demgegenüber ist ab diesem Zeitpunkt die Staking-Adresse (bzw. Validator-Adresse) für die jeweilige Staking-Position im Smart Contract hinterlegt, weshalb sich die Frage der Zuordenbarkeit in erster Linie nach der Staking-Adresse richtet. Aufgrund ihrer Bedeutung in Ethereum kommt für die Zuordnung während des Staking-Vorgangs alternativ auch die Withdrawal-Adresse infrage (wobei die Adresse in der Praxis auch deckungsgleich mit der Verwahrungsadresse sein kann).

[20] https://etherscan.io/address/0x00000000219ab540356cbb839cbe05303d7705fa.

Diese Einordnung scheint in Einklang mit der FINMA-Aufsichtsmitteilung 08/2023 zu stehen, wonach sicherzustellen ist, dass «[…] die auf einer bestimmten Validator-Adresse und *nach dem* Unstaking auf einer bestimmten Withdrawal-Adresse platzierten kryptobasierten Vermögenswerte jeweils eindeutig den berechtigten Kunden zugeordnet werden können» (S. 11, Hervorhebung hinzugefügt).

Dem Staking-Anbieter steht es natürlich frei, alle drei Adressen zeitgleich einem Kunden zuzuordnen. Kryptobasierte Vermögenswerte, die auf Adressen gehalten werden, die generell keinen Kunden (auch nicht i.S.v. Art. 242a Abs. 2 lit. b SchKG) oder die aber dem Staking-Anbieter selbst zugeordnet sind, qualifizieren grundsätzlich als Publikumseinlagen, soweit keine bankenrechtliche Ausnahme einschlägig ist. Dies könnte etwa dann der Fall sein, wenn die kryptobasierten Vermögenswerte des Kunden nach dem Unstaking (vorübergehend) auf eine nicht im internen System des Staking-Anbieters zugeordnete Withdrawal-Adresse verschoben werden, von wo aus sie auf die kundenspezifischen Adressen weitergeleitet werden.

#### 4.2.3.3 Withdrawal Keys (Verfügungsmacht)

Die FINMA führt in der Aufsichtsmitteilung 08/2023 ferner aus, dass der Staking-Anbieter über die *Withdrawal Keys* verfügen muss (S. 11). Diese Anforderung kann etwa im Rahmen der Auslagerung des Betriebs einer Validator Node an eine Drittperson relevant sein. Letztlich geht es um die Frage, ob und wie der Staking-Anbieter sicherstellen kann, dass er die Verfügungsmacht effektiv innehat.[21] In Bezug auf Ethereum-Staking kann die Verfügungsmacht etwa aufrechterhalten werden, indem der Betreiber der Validator Node vorab eine sog. *Voluntary Exit Message (VEM)* signiert und diese (off-chain) an den Staking-Anbieter übermittelt. Dieser kann die VEM bei Bedarf, wie etwa im Fall der Nichtverfügbarkeit der Validator Node, an die Ethereum Blockchain übermitteln, was automatisch, d.h. ohne weiteres Zutun des Validator-Betreibers, den Rückzug der gestakten ETH an die Withdrawal-Adresse auslöst.[22] Durch diese technische Lösung ist sichergestellt, dass die ausschliessliche tatsächliche Verfügungsmacht beim Staking-Anbieter verbleibt.

Bei Staking-Setups *ohne* Auslagerung ist diese Anforderung hingegen nicht weiter relevant, da der Staking-Anbieter alle technischen und administrativen Elemente der Dienstleistung selbst erbringt (siehe sogleich Ziff. 4.2.3.4).

Anders als in der Aufsichtsmitteilung erwähnt (S. 13), muss der Verlust der Withdrawal Keys nicht *per se* zum definitiven Verlust der gestakten kryptobasierten Vermögenswerte führen. Dies wäre nur dann der Fall, wenn, wie derzeit bei Ethereum, die Withdrawal-Adresse systembedingt lediglich einmalig festgelegt werden kann.

[21] Siehe SBF, Zirkular 2023/01, Staking, Fassung vom 05.09.2023 S. 21.
[22] Zum Ganzen Crypto Valley Association (CVA), Paper on Staking Services on Proof-of-Stake Protocols, 12. Dezember 2023, S. 4 f.

#### 4.2.3.4 Auslagerung oder Delegation der Verwahrung

Staking-Anbieter ohne finanzmarktrechtliche Bewilligung können ihren Kunden – in der Terminologie der FINMA – grundsätzlich lediglich das Direct Staking anbieten. Die Auslagerung oder Delegation der Verwahrung an einen Dritten (Unterverwahrung) ist ihnen nur gestattet, wenn ausnahmsweise ein einschlägiges Aussonderungsregime besteht.[23]

Elemente *ausserhalb* des Sub-Custody (d.h. der Verwahrung der Private Keys), wie etwa technische, operationelle und administrative Elemente des Staking-Vorgangs, können hingegen ohne Einschränkungen an Dritte ausgelagert bzw. delegiert werden. Für Ethereum beinhaltet dies auch den Betrieb der Validator Node durch einen Dritten, falls der Validator-Betreiber dem Staking-Anbieter vor Staking-Beginn eine vorsignierte Rückzugstransaktion (VEM) übermittelt, welche sicherstellt, dass der Staking-Anbieter jederzeit die Kontrolle über den Rückzug der gestakten kryptobasierten Vermögenswerte auf die Withdrawal Adresse des Kunden behält. Die ausschliessliche tatsächliche Verfügungsmacht des Staking-Anbieters über die gestakten kryptobasierten Vermögenswerte ist unter diesen Umständen gewährleistet.

#### 4.2.3.5 Sammelverwahrung

Staking-Anbieter ohne finanzmarktrechtliche Bewilligung führen das Staking im Auftrag und auf Rechnung ihrer Kunden von einer kundenspezifischen Adresse aus. Mit anderen Worten muss eine *Einzelverwahrung* der gestakten kryptobasierten Vermögenswerte des Kunden vorliegen.

Dies gilt grundsätzlich auch für die vom Protokoll ausgeschütteten Staking Rewards, sobald sie vom Staking-Anbieter an den Kunden weiterzuleiten sind.

Ausnahmen sind möglich, wenn sie sich auf den Ausnahmekatalog in Art. 5 Abs. 2 und 3 BankV bzw. Art. 5a Abs. 2 BankV stützen können. Namentlich könnte sich der Staking-Anbieter bei Vorliegen der entsprechenden Voraussetzungen auf die Abwicklungskontiausnahme für unverzinste Kundengelder berufen, um Staking Rewards, die vorübergehend auf einer Adresse gesammelt werden, die keinem einzelnen Kunden zugeordnet ist, bevor sie auf die kundenspezifischen Adressen *weitergeleitet* werden, vom Einlagenbegriff auszunehmen. In einem solchen Fall handelt es sich weder um (sammelverwahrte) kryptobasierte Vermögenswerte i.S.v. Art. 242a Abs. 2 SchKG bzw. Art. 16 Ziff. 1$^{bis}$ BankG noch um Zahlungs-Token i.S.v. Art. 5a Abs. 1 BankV oder um Publikumseinlagen i.S.v. Art. 5 Abs. 1 BankV.

## 4.3 Fazit

Die Aussonderung gestakter kryptobasierter Vermögenswerte im Konkurs eines Staking-Anbieters, der ohne finanzmarktrechtliche Bewilligung tätig ist, ist gestützt auf Art. 242a Abs. 2 lit. a SchKG grundsätzlich möglich. Für Ausführungen zur Pflicht zur jederzeitigen Bereithaltung sei auf die erste Fassung des vorliegenden Zirkulars verwiesen.[24]

[23] Prüfenswert wäre allf. eine Aussonderung der Forderungsrechte des Staking-Anbieters gegenüber dem Sub-Custodian durch die Kunden des Staking-Anbieters in dessen Konkurs gestützt auf Art. 401 Abs. 1 i.V.m. Abs. 2 OR. Bei grenzüberschreitenden Konstellationen wäre zudem die Möglichkeit der Aussonderung nach ausländischem Recht zu prüfen.
[24] Die erste Fassung des Zirkulars ist verfügbar unter https://blockchainfederation.ch/downloads/.

Massgeblich für die Aussonderbarkeit gestakter kryptobasierter Vermögenswerte ist einerseits die ausschliessliche tatsächliche Verfügungsmacht des Staking-Anbieters über die Token der Kunden. Zudem sind die gestakten Token grundsätzlich auf kundenspezifischen Adressen in Einzelverwahrung zu halten, um nicht bankenrechtliche Unterstellungsfragen auszulösen. Allerdings muss der Staking-Anbieter nicht alle für den Staking-Vorgang relevanten Adressen zeitgleich den einzelnen Staking-Kunden zuordnen können. Es genügt, wenn jeweils diejenige Adresse im internen Register des Staking-Anbieters dem Kunden zugeordnet ist, welche eine eindeutige Zuweisung der auf der Blockchain gestakten Position zum betreffenden Kunden erlaubt. Schliesslich sind Auslagerungs- und Delegationslösungen im technischen, operationellen und administrativen Bereich auf jeden Fall zulässig, solange sie keine Elemente der Unterverwahrung der Private Keys betreffend die Kunden-Token umfassen. Um den Betrieb einer Validator Node etwa bei Ethereum an eine Drittperson auslagern bzw. delegieren zu können, bedarf es der Vorsignierung einer Rückzugstransaktion (VEM). In diesem Fall behält der Staking-Anbieter weiterhin die ausschliessliche tatsächliche Verfügungsmacht über die gestakten kryptobasierten Vermögenswerte.

An dieser Stelle ist darauf hinzuweisen, dass Staking-Anbieter ihre Kunden gestützt auf ihre auftragsrechtliche Sorgfalts- und Treuepflicht vor dem Staking über die wesentlichen Risiken von Staking aufzuklären haben. Risiken aus der im Einzelnen geltenden Anwendbarkeit von Lock-Up-Mechanismen und Slashing werden somit auf der zivilrechtlichen Ebene adressiert, welche die Hinterlegungsstelle zu einem sorgfältigen Tätigwerden verpflichtet (siehe hierzu oben Ziff. 3.3). Dabei ist zu beachten, dass Staking-Anbieter in der Praxis nicht jegliche Fehler, die aus dem Staking resultieren, vertraglich auf den Kunden überwälzen können (vgl. Art. 100 Abs. 1 OR). Es steht dem Dienstleister selbstredend frei, die finanziellen Auswirkungen von Slashing-Ereignissen vollständig selbst zu tragen. Alternativ kann der Staking-Anbieter dem Kunden ggf. eine Versicherung gegen Slashing-Risiken anbieten.

Die Risikoaufklärung von Staking-Anbietern ohne finanzmarktrechtliche Bewilligung sollte sich an den Ausführungen zur Risikoaufklärung von regulierten Finanzinstituten orientieren (siehe hierzu unten Ziff. 5.3.2.2), jedoch mit dem Vorbehalt, dass Risiken im Zusammenhang mit dem Sub-Custody in der Regel keine Rolle spielen.

# 5. Bankenrecht

## 5.1 Einleitung

Gemäss Art. 1 Abs. 2 BankG ist die gewerbsmässige Entgegennahme von *Publikumseinlagen* Banken vorbehalten, wenn kein Ausnahmetatbestand gemäss Art. 5 Abs. 2 und Abs. 3 BankV vorliegt. Ferner kann es trotz Vorliegens von Publikumseinlagen an der Gewerbsmässigkeit der Tätigkeit fehlen, wenn eine Person etwa die Bedingungen der *Sandbox* erfüllt (vgl. Art. 6 BankV).

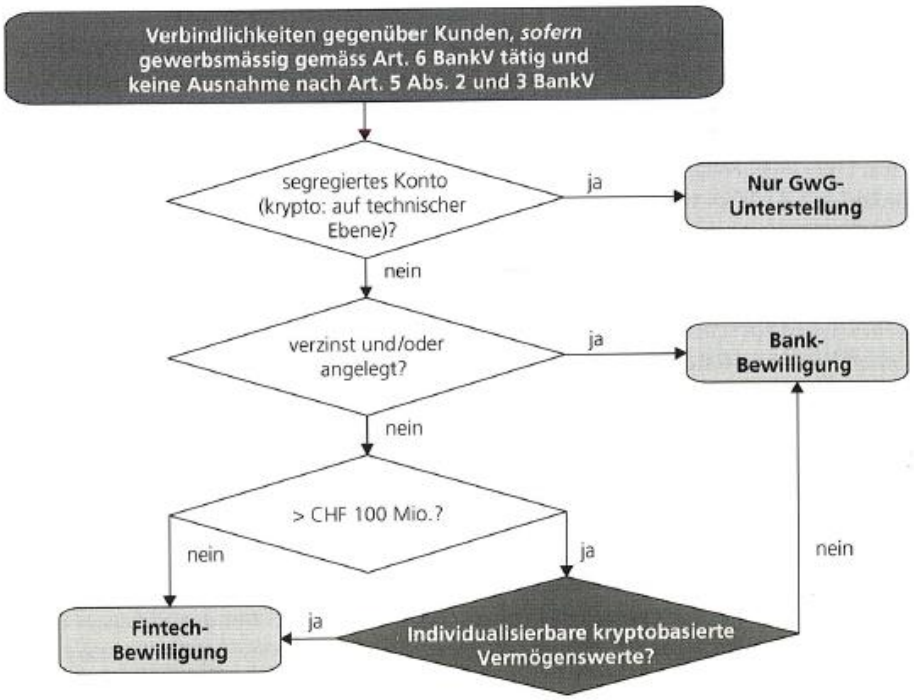
Um eine Publikumseinlage handelt es sich nach ständiger Rechtsprechung des Bundesgerichts, wenn eine Person Verpflichtungen gegenüber Dritten eingeht und dadurch zur Rückzahlungsschuldnerin der entsprechenden Leistung wird.[25]

[25] Siehe statt vieler Reto Luthiger/Hans Kuhn, in: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizerischen Blockchain-Recht, Basel 2021, Kapitel VIII., Rz. 22 m.w.N.

Nach Art. 1a BankG sind Banken grundsätzlich frei in der Entgegennahme von Publikumseinlagen; sie können mit diesen insbesondere das banktypische Zinsdifferenzgeschäft betreiben. Anderes gilt für Personen nach Art. 1b BankG (Fintech). Solche Unternehmen können zwar Publikumseinlagen bis 100 Mio. Fr. entgegennehmen, dürfen mit diesen Vermögenswerten allerdings weder Finanzanlagen auf eigene Rechnung und eigenes Risiko tätigen noch dürfen sie die Publikumseinlagen ihrer Kunden verzinsen. Andernfalls bedarf ihre Tätigkeit einer Bankbewilligung.

Dasselbe gilt für die Entgegennahme und Aufbewahrung *sammelverwahrter kryptobasierter Vermögenswerte* im Sinne von Art. 5a Abs. 1 BankV durch Personen nach Art. 1b BankG. In diesem Fall handelt es sich jedoch nicht um Publikumseinlagen, sondern um im Konkurs absonderbare Depotwerte. Doch hat der Gesetzgeber sammelverwahrte kryptobasierte Vermögenswerte, die tatsächlich oder nach der Absicht des Organisators oder Herausgebers in einem erheblichen Umfang als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen oder der Geld- oder Wertübertragung dienen (sog. Zahlungs-Token bzw. Kryptowährungen), aufsichtsrechtlich einem ähnlichen Regime wie Publikumseinlagen unterstellt.

Grafik 3: Überblick Bewilligungen beim Kryptoverwahrungsgeschäft




Quelle: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizerischen Blockchain-Recht, Basel 2021, S. 207

Demgegenüber sind die Tätigkeiten der Entgegennahme und Aufbewahrung von Zahlungs-Token bzw. Kryptowährungen i.S.v. Art. 1b Abs. 1 lit. a BankG i.V.m. Art. 5a Abs. 1 BankV, die in *Einzelverwahrung* gehalten werden, bewilligungsfrei möglich. In diesem Fall hat der Aufbewahrer die Kundenvermögen sowohl von den Beständen anderer Kunden als auch von seinen Eigenbeständen in aller Regel auf kundenspezifischen Blockchain-Adressen zu trennen. Ferner hat sich der Aufbewahrer für die Geldwäschereiaufsicht einer Selbstregulierungsorganisation (SRO) anzuschliessen (siehe hierzu unten Ziff. 9.2).

## 5.2 Publikumseinlagen und Depotwerte

### 5.2.1 Übersicht

Ausgangspunkt der Analyse von Staking in bankrechtlicher Hinsicht bildet die Frage, ob die entgegengenommenen kryptobasierten Vermögenswerte als Publikumseinlagen oder aber als Depotwerte gelten. Das Vorliegen von Depotwerten hängt damit davon ab, ob die von Kunden entgegengenommenen kryptobasierten Vermögenswerte die unter Art. 16 BankG aufgestellten Anforderungen erfüllen und somit im Konkurs der Bank absonderbar sind.

### 5.2.2 Einzel- und Sammelverwahrung

Eine Bank oder Person nach Art. 1b BankG kann ihr Staking-Angebot auf unterschiedliche Weise umsetzen:

Denkbar ist, dass eine Bank oder Person nach Art. 1b BankG das Staking-Produkt in Form von *Publikumseinlagen* ausgestaltet. Entsprechend wäre die Staking-Tätigkeit der Bank aufgrund der Risiken für die eigenen Bilanzwerte mit Eigenmitteln zu unterlegen.

Sodann kann eine Bank oder Person nach Art. 1b BankG Staking von kryptobasierten Vermögenswerten anbieten, deren Private Keys sich in der Einzel- oder Sammelverwahrung befinden. Staking aus der *Einzelverwahrung* heraus kann grundsätzlich selbst bewilligungsfrei angeboten werden (siehe oben Ziff. 5.1). Da jedoch gewisse Protokolle für den Betrieb einer Validator Node ein «Minimum Stake» vorsehen (so z.B. Ethereum im Umfang von 32 ETH), können Kunden u.U. lediglich über eine Pooling-Lösung am Staking teilnehmen. Vorbehaltlich der Anwendbarkeit bankrechtlicher Ausnahmen ist für das Staking aus der *Sammelverwahrung* heraus grundsätzlich die Bewilligung als Bank oder Person nach Art. 1b BankG erforderlich.

Die in einem Protokoll blockierten kryptobasierten Vermögenswerte bleiben beim Custodial Staking sodann unter ausschliesslicher Kontrolle der Staking-Anbieterin bzw. Verwahrerin. Auch im Rahmen eines Slashing erlangt in der Regel keine Drittperson die Verfügungsmacht über die gestakten Token.[26] Im Gegenteil sind solche Token Gegenstand eines sog. *Burning*, d.h., sie werden «vernichtet» und somit für jedermann unbrauchbar gemacht. Mit anderen Worten führt die Blockierung von kryptobasierten Vermögenswerten in einem Smart Contract in der Regel nicht zur Entgegennahme von Publikumseinlagen durch eine Drittperson, wie etwa den Betreiber einer Validator Node oder gar die Netzwerkteilnehmer einer Blockchain *in globo*.

## 5.3 Absonderung im Konkurs

### 5.3.1 Vorbemerkungen

Gemäss FINMA-Aufsichtsmitteilung 08/2023 kann Custodial Staking in Einklang mit der in der Literatur einhellig vertretenen Auffassung so betrieben werden, dass aus Kundensicht Depotwerte

[26] Siehe Kilian Schärli/Luzius Meisser/Reto Luthiger, Finanzmarktrechtliche Einordnung des Stakings von Kryptowährungen, Jusletter IT 30.09.2021, Rz. 7.

und nicht lediglich Publikumseinlagen vorliegen. Dabei ist in der Terminologie der FINMA zwischen Direct Staking (reguläres Custodial Staking) und Staking-Ketten (Sub-Custodial Staking) zu unterscheiden:

Sofern Banken beim *Direct Staking* die in der Aufsichtsmitteilung gestellten Anforderungen einhalten (S. 10), sind die gestakten kryptobasierten Vermögenswerte im Konkurs der Bank oder des Instituts nach Art. 1b BankG gestützt auf Art. 16 Ziff. 1$^{bis}$ BankG absonderbar.

Ausserdem erachtet die FINMA Formen des Sub-Custodial Stakings, die sie als *Staking-Ketten* bezeichnet, als zulässig, sofern der Custodian die SBVg-Richtlinien zu Treuhandanlagen 2016 «in angepasster, analoger» Weise auf die Staking-Dienstleistungen so anwendet, dass die spezifischen Risiken der «Staking-Treuhand» berücksichtigt werden (S. 9). In diesem Fall erfolgt mangels Zugriffsmöglichkeit auf die Private Keys keine (direkte) Absonderung der gestakten kryptobasierten Vermögenswerte, sondern es werden die von der Bank oder der Person nach Art. 1b BankG treuhänderisch für den Kunden gehaltenen Forderungen in deren Konkurs gestützt auf Art. 16 Ziff. 2 BankG abgesondert.

Mit der Aufsichtsmitteilung klärt die FINMA als die für die Konkursliquidation von Banken zuständige Behörde (vgl. Art. 25 Abs. 1 i.V.m. 33 BankG) die in der Praxis auftretenden Fragen aus ihrer Warte und schafft dadurch eine für die Marktteilnehmer nachvollziehbare Praxis, womit die gemäss FINMA bestehende «unklare Rechtslage» zumindest diesbezüglich geklärt wird.[27]

### 5.3.2 Generelle Anforderungen

Die folgenden Anforderungen kommen sowohl beim regulären Custodial Staking als auch beim Sub-Custodial Staking zur Anwendung, wobei auf allfällige Unterschiede jeweils hingewiesen wird.

#### 5.3.2.1 Kundeninstruktion

Die FINMA verlangt von bewilligten Instituten, dass ein spezifischer Auftrag des Kunden über die Art und Anzahl der zu stakenden kryptobasierten Vermögenswerte vorliegt (S. 9 und 10), welche sich u.a. gestützt auf die vertragliche Beziehung zwischen Institut und Kunde ergibt. Voraussetzung beim *Sub-Custody-Verhältnis* ist gemäss FINMA, dass die Bank mit dem Kunden eine «Treuhandvereinbarung» (S. 9) abschliesst; insoweit muss aber weder ein Vertragsdokument mit dieser Bezeichnung vorliegen noch ist bei jeder einzelnen Staking-Instruktion darauf hinzuweisen. Vielmehr kann die Treuhandklausel, soweit sie überhaupt als notwendig erachtet wird (siehe hierzu Ziff. 5.3.3.1), etwa in den Allgemeinen Geschäftsbedingungen oder einem besonderen Staking-Vertrag mit dem Kunden vereinbart werden.

Ferner können Kunden das Institut bereits im Voraus zum «Restaking» von gutgeschriebenen Staking Rewards instruieren, soweit die Instruktion unter Berücksichtigung des konkreten Vorgangs genügend spezifisch ist.

[27] Gemäss der Webseite der FINMA enthalten Aufsichtsmitteilungen wichtige und dringende Informationen oder Erläuterungen zu relevanten Fragen für die Beaufsichtigten sowie Hinweise auf aktuelle Risiken. Zwar sind sie im Unterschied zu Verordnungen und Rundschreiben der FINMA kein Regulierungsinstrument, jedoch dienen sie der reibungslosen Anwendung von Vorschriften in der Praxis; vgl. https://www.finma.ch/de/dokumentation/finma-aufsichtsmitteilungen/, zuletzt besucht am 29.02.2024.

Es besteht kein allgemeines Schriftlichkeitserfordernis für die Kundeninstruktion. Jedoch wird es in der Regel im Interesse des Staking-Anbieters sein, die Instruktion in nachvollziehbarer Weise zu *dokumentieren*.

Andere vertragliche Regelungen, die ein Einlagengeschäft der Bank ausschliessen würden, vorbehalten, stellt die Verwendung von Tokens zwecks Staking ohne die Zustimmung des Kunden ein für Banken zwar zulässiges Aktiv- bzw. Eigengeschäft dar, das jedoch zur Anwendbarkeit der im Bereich der kryptobasierten Vermögenswerte ungemein einschneidenden Eigenmittelanforderungen führen würde.

#### 5.3.2.2 Risikoaufklärung

Wie in Ziff. 3.5 dieses Zirkulars erwähnt, schulden Staking-Anbieter ihren Kunden grundsätzlich ein sorgfältiges Tätigwerden gemäss Auftragsrecht (Art. 398 Abs. 2 OR). Dazu gehört auch eine angemessene Risikoaufklärung des Kunden, soweit der Kunde aufklärungsbedürftig ist.

Die Risikoaufklärung sollte *vor* der Erbringung von Staking-Dienstleistungen separat oder als Teil einer allgemeinen Risikoaufklärung etwa betreffend kryptobasierte Vermögenswerte erfolgen. Eine solche Aufklärung gilt unabhängig vom finanzmarktrechtlichen Bewilligungsstatus des Staking-Anbieters, d.h. auch nichtbewilligte Anbieter sollten eine entsprechende Risikoaufklärung vornehmen (siehe hierzu Ziff. 4.3).

Die Risikoaufklärung der Kunden kann sich etwa an der durch Finanzinstitute vorgenommenen Risikoaufklärung für Finanzinstrumente orientieren, deren Motivation im Anlegerschutz zu finden ist (FIDLEG, MiFID II usw.). Denkbar ist, dass sich künftig standardisierte Dokumente analog der Broschüre der Schweizerischen Bankiervereinigung über die Risiken im Handel mit Finanzinstrumenten[28] entwickeln werden.

Der Inhalt einer Risikoaufklärung könnte etwa folgende Punkte umfassen:

- generelle Erläuterungen zum Zweck und zur Funktionsweise von Staking (inklusive Staking Rewards);
- Beschreibung der konkret erbrachten Staking-Dienstleistungen des betreffenden Staking-Anbieters (Verwahrung, Betrieb einer Validator Node, Auslagerungen/Delegationen usw.);
- allfällige Lock-Ups (Dauer, Bedingungen usw.) und die damit verbundenen Einschränkungen für den Kunden;[29]
- allfällige Slashing-Risiken und weitere Sanktionen (möglicher Umfang, potenziell betroffene Vermögenswerte des Kunden usw.);[30]
- allfällige Gegenparteirisiken beim Sub-Custodial Staking und bei anderweitigen Auslagerungen und Delegationen der Staking-Dienstleistungen;[31]
- eine allfällige Haftungsbeschränkung des Staking-Anbieters für den Fall der Realisierung der erwähnten und allfälliger weiterer Risiken.

[28] Vgl. SBVg, Risiken im Handel mit Finanzinstrumenten, Juni 2023.
[29] Siehe Ausführungen zu «Marktrisiken» in der FINMA-Aufsichtsmitteilung 08/2023, Ziff. 2.3.
[30] Siehe Ausführungen zu «technischen Risiken» in der FINMA-Aufsichtsmitteilung 08/2023, Ziff. 2.3, sowie Ziff. 2.6.2.3 dieses Zirkulars.
[31] Siehe Ausführungen zu «Gegenparteirisiken» in der FINMA-Aufsichtsmitteilung 08/2023, Ziff. 2.3, sowie Ziff. 5.3.3.1 dieses Zirkulars.

#### 5.3.2.3 Zuordenbarkeit von Kundenadressen

Im Wesentlichen gelten die Ausführungen in Ziff. 4.2.3.2 auch für bewilligte Institute.

#### 5.3.2.4 Withdrawal Keys (Verfügungsmacht)

Im Wesentlichen gelten die Ausführungen in Ziff. 4.2.3.3 auch für bewilligte Institute.

#### 5.3.2.5 Business Continuity Management (BCM)

Die FINMA sieht als weitere Voraussetzung für bewilligte Institute vor, dass geeignete Massnahmen zur Minderung der operationellen Risiken infolge des Betriebs einer Validator Node, inklusive eines Business Continuity Management (BCM), getroffen werden. Hierbei geht es darum, dass die sich im Einflussbereich des Instituts befindenden operationellen Risiken, auf die der Kunde im Rahmen der Risikoaufklärung aufmerksam gemacht wird (siehe oben Ziff. 5.3.2.2), identifiziert, adressiert und überwacht werden. Namentlich soll die Realisierung des Slashing-Risikos und allfälliger weiterer Sanktionen, die sich aus einem nicht planmässigen Betrieb der Validator Node ergeben können, verhindert bzw. deren Auswirkungen minimiert werden.

Im *Sub-Custody-Verhältnis* hat nicht nur der Custodian die Geschäftskontinuität sicherzustellen, sondern auch der Sub-Custodian, der die Validator Nodes selbst betreibt oder sie durch eine Drittperson betreiben lässt. In der Praxis wird der Sub-Custodian oftmals dem Custodian seinen Business Continuity Plan (BCP) oder diesbezügliche Informationen und allenfalls weitere Informationen zu den Prozessen, welche die kontinuierliche Erbringung der Staking-Tätigkeit intern regeln, auf Anfrage darlegen müssen.

#### 5.3.2.6 Digital Asset Resolution Package (DARP+)

Im Rahmen ihrer Aufsichtspraxis verlangt die FINMA seit 2022 von bewilligten Instituten, dass diese im Rahmen der Verwahrung von kryptobasierten Vermögenswerten ein sog. *Digital Asset Resolution Package (DARP)* erstellen und unterhalten.[32] Dies erfolgt vor dem Hintergrund eines angemessenen Risikomanagements von Kryptoverwahrern. In ihrer Aufsichtsmitteilung (S. 10 und 11) statuiert die FINMA diese Praxis nun erstmals öffentlich und dehnt sie zudem auf gestakte kryptobasierte Vermögenswerte aus (DARP+). Sie gibt dadurch der Industrie wichtige Leitplanken, welche generellen Erwartungen die Aufsichtsbehörde an ein DARP hat. Gleichzeitig sollte den Instituten aber genügend Raum verbleiben, ein auf ihre Bedürfnisse zugeschnittenes DARP zu erstellen.

Das *Ziel* eines DARP ist es, sicherzustellen, dass ein externer Liquidator im Konkursfall die kryptobasierten Vermögenswerte effizient an die Kunden ausbezahlen kann, so dass sich der Aufwand und die Kosten für eine ordnungsgemässe Rückgabe «auf ein Minimum» beschränken las-

[32] Vgl. Ronald Kogens/Patrick Niklaus, Digital Asset Resolution Package (DARP), 12.07.2023, https://www.mme.ch/de-ch/magazin/artikel/digital-asset-resolution-package-darp, zuletzt besucht am 29.02.2024.

sen. So definiert die FINMA das DARP denn auch als interne Handlungsanweisung zur Information eines Liquidators über Verantwortlichkeiten und Zugriffsmöglichkeiten im Fall des Konkurses einer Bank, die kryptobasierte Vermögenswerte verwahrt.

Zeitlich regelt das DARP vorwiegend die Periode ab dem Zeitpunkt der Konkurseröffnung, wobei je nach Geschäftsmodell auch bestimmte Massnahmen bei einem sich erst abzeichnenden Konkurs denkbar sind. Da ab Konkurseröffnung ein von der FINMA eingesetzter Konkursliquidator für Handlungen betreffend die Vermögenswerte der Kunden zuständig ist, handelt es sich bei den Handlungsanweisungen im DARP meist nicht um zwingende Vorgaben des Instituts, sondern eher um eine Hilfestellung für den Konkursliquidator, wie dieser im Falle eines Konkurses möglichst rasch über die den Kunden gehörenden Vermögenswerte verfügen kann.

Das DARP hat somit einerseits Informationscharakter für den Konkursverwalter, enthält aber gleichzeitig auch zwingende Anweisungen an die Arbeitnehmer des bewilligten Instituts und stellt somit einen Bestandteil des Weisungswesens dar, welches abhängig von der konkreten internen Organisation auf angemessener Stufe genehmigt werden muss.

*Inhaltlich* sollen im DARP die wichtigsten Informationen zur Identifikation und zeitnahen Sicherstellung der Forderungen an kryptobasierten Vermögenswerte zusammengefasst und laufend aktualisiert werden. Dazu gehören die wichtigsten Informationen für die Identifizierung und unverzügliche Sicherstellung der kryptobasierten Vermögenswerte, eine Beschreibung der Verwahrungsart und der Zugriffsmöglichkeiten (d.h. insbesondere der damit zusammenhängenden Zugriffsrechte), Angaben zum Zugang zu einer aktuellen Kopie der internen Bestandesaufstellungen, Ausführungen zu den mit dem Staking potenziell verbundenen operationellen Risiken und adäquate Massnahmen zu deren Minderung (im Falle einer ausserordentlichen Abwicklung), Informationen zu den für die Verwahrung und die Auslösung von Transaktionen zuständigen Funktionsträgern und deren Aufgaben. Betreffend die für die jeweiligen Abläufe zuständigen Funktionsträger (z.B. Head Custody oder Head Banking Operations) erscheint eine klare Regelung der Verantwortlichkeiten als empfehlenswert. Es muss jederzeit – d.h. nicht erst im Konkursfall – klar sein, welche Funktionen bzw. Funktionsträger für welche Schritte verantwortlich sind. Diese Verantwortlichkeiten ergeben sich in der Praxis bereits aus den institutsinternen Weisungen und Richtlinien und nicht erst aus dem DARP. Vor diesem Hintergrund kann es auch als sinnvoll erscheinen, dass das DARP sich auf «die wichtigsten Informationen» beschränkt und für weitergehende Informationen auf die relevanten Weisungen und Richtlinien des Instituts verweist.

Im *Sub-Custody-Verhältnis* sind zusätzliche Angaben zu den Sub-Custodians und deren Aufbewahrungsmodalitäten im DARP des Staking-Anbieters zu erfassen. Dies kann wohl nur angemessen dokumentiert werden, wenn der eigentliche Staking-Anbieter in der Kette (d.h. derjenige mit der Endkundenbeziehung) die notwendigen Information von den nachfolgenden Dienstleistern erhält, wie bspw. die Kontaktangaben der zuständigen Person beim Sub-Custodian. Diese Informationen werden vom Staking-Anbieter im Rahmen der oben beschriebenen Due Diligence von den (potentiellen) Sub-Custodians soweit nötig verlangt und überprüft werden müssen. Typischerweise wird in der Praxis denn auch auf das DARP der Sub-Custodians verwiesen. Bei ausländischen Dienstleistern stellt sich derzeit in der Praxis aber die Frage, ob alle Dienstleister ein DARP erstellen und bereit sind, alle notwendigen Informationen mit dem Custodian und Staking-Anbieter zu teilen.

### 5.3.3 Besondere Anforderungen beim Sub-Custodial Staking

#### 5.3.3.1 Due Diligence bezüglich Sub-Custodian

Damit die Forderung des Custodians und Staking-Anbieters gegenüber dem Sub-Custodian aus der Delegation des Betriebs der Validator Node als treuhänderisch «verwahrte» Forderung i.S.v. Art. 16 Ziff. 2 BankG qualifiziert und damit als Depotwert behandelt werden kann, verlangt die FINMA eine an die Risiken (gestakter) kryptobasierter Vermögenswerte angepasste, analoge Anwendung der SBVg-Richtlinien betreffend Treuhandanlagen 2016.

Die SBVg-Richtlinien betreffend Treuhandanlagen passen auf die Rechtsverhältnisse beim Staking allerdings mehr schlecht als recht: Bei Treuhandanlagen erwirbt die Bank eine Forderung gegen die Drittbank, wobei der Kunde der Bank das Ausfallrisiko der Drittbank trägt (*Delcredererisiko* gemäss den Treuhand-Richtlinien). Demgegenüber geht es im vorliegenden Zusammenhang gerade darum, dass der Custodian bzw. Staking-Anbieter gestakte kryptobasierte Vermögenswerte im Konkurs des Sub-Custodians aussondern kann (unter Schweizer Recht im Regelfall gestützt auf Art. 16 Ziff. 1$^{bis}$ BankG). Mit der analogen Anwendung der Treuhand-Richtlinien will die FINMA – wie sich der Aufsichtsmitteilung entnehmen lässt – Gegenparteirisiken eliminieren. Diese werden aber bereits wirksam gemindert, wenn die gestakten kryptobasierten Vermögenswerte im Konkurs des Sub-Custodians aussonderbar sind.

Aus der sinngemässen Anwendung der Treuhand-Richtlinien ergeben sich die folgenden Anforderungen für die Auswahl des Sub-Custodians:

- Der Sub-Custodian ist ein prudenziell beaufsichtigtes Institut oder eine Tochtergesellschaft einer konsolidiert beaufsichtigten Finanzgruppe. Gemäss Treuhand-Richtlinien müssen diese über eine gute Bonität verfügen. Die *prudenzielle Aufsicht* dient dem Gläubiger-, Anleger- und Funktions- bzw. Systemschutz. Einer prudenziellen Aufsicht unterstehen namentlich ausländische Kreditinstitute, Wertpapierfirmen und künftig auch Anbieter von Kryptowerte-Dienstleistungen nach MiCAR, nicht jedoch Dienstleister, welche einer reinen Geldwäschereiaufsicht unterliegen (VASPs). Da der Schutz der Rechtsposition des Kunden beim Staking primär durch die Aus- bzw. Absonderbarkeit der gestakten kryptobasierten Vermögenswerte gewährleistet wird, kommt dieser Anforderung beim Staking jedoch nur geringere Bedeutung zu.
- Die Festlegung von *Limiten* (SBVg-Treuhand-Richtlinien, Ziff. III 1. b)) erscheint im vorliegenden Zusammenhang nicht angezeigt. Limiten sollen Gegenparteirisiken begrenzen, die im vorliegenden Zusammenhang aufgrund der Aussonderungsfähigkeit der gestakten kryptobasierten Vermögenswerte gemindert werden.
- Auch ein *Verrechnungsverzicht* (SBVg-Treuhand-Richtlinien, Ziff. III 1. c)) ist in der Regel nicht erforderlich, da eine Verrechnungslage im Staking-Kontext mangels Gleichartigkeit der Forderungen ausscheidet.
- Rechtlich betrachtet erscheint der Abschluss einer *Treuhandvereinbarung* zwischen Kunde und Custodian bzw. Staking-Anbieter als nicht zwingend. Eine Klarstellung der treuhandähnlichen Ausgestaltung der Unterverwahrung im Verhältnis zwischen Kunde und Custodian drängt sich anders als bei der klassischen Treuhandanlage mit Einlagencharakter nicht auf; die Treuhandabrede ergibt sich vielmehr regelmässig aus dem Verwahrungsvertrag zwischen Custodian und Sub-Custodian. Eine Klausel, wonach die Verwah-

rung auf Rechnung der Kunden des Custodians (d.h. der Endkunden) erfolgt, ist u.E. ausreichend, denn in diesem Fall ist klar, dass der Sub-Custodian die Vermögenswerte für Rechnung eines Dritten verwahrt.

Demgegenüber sind die weiteren in der FINMA-Aufsichtsmitteilung 08/2023 genannten Anforderungen an das Sub-Custody-Verhältnis sinnvoll:

- Der Sub-Custodian muss die relevanten *Withdrawal Keys* selbst halten, was nach Ansicht der FINMA längere Staking-Ketten ausschliesst. Nicht ausgeschlossen ist hingegen, dass der Sub-Custodian Drittpersonen zum technischen Betrieb von Validator Nodes beizieht oder sonstige operationelle Delegationen vornimmt. Soweit notwendig, hat der Sub-Custodian in diesem Fall allerdings Massnahmen zu treffen, damit die ausschliessliche tatsächliche Verfügungsmacht weiterhin bei ihm verbleibt (wie bspw. durch die Ausstellung einer VEM durch den Betreiber der Validator Nodes).
- Der Sub-Custodian bezeichnet die *Adressen der Validator Nodes*, auf der er die kryptobasierten Vermögenswerte des Custodians bzw. Staking-Anbieters hält. Er teilt dem Staking-Anbieter sodann auf Nachfrage die im Einzelfall einschlägigen Validator Node-Adressen mit. Dies gibt dem Staking-Anbieter die Möglichkeit, die korrekte Ausführung des Staking-Auftrags bei Bedarf auf der Blockchain nachzuprüfen.
- Der Sub-Custodian muss notwendige Massnahmen treffen, um die *operationellen Risiken* aus dem Betrieb der Validator Node (Validierungsfehler oder Offline-Status) zu beschränken, weitere Sanktionen gegen die Validator Node auszuschliessen und die Geschäftskontinuität sicherzustellen.

Nach Auffassung der FINMA ist die analoge Anwendung der Treuhandrichtlinien Voraussetzung, «[...] um *grobe Fahrlässigkeit* der Verwahrer gegenüber ihren Kunden auszuschliessen» (Hervorhebung hinzugefügt). Bei grober Fahrlässigkeit ist eine Freizeichnung unwirksam (Art. 100 Abs. 1 OR). Das ist in dieser Absolutheit unzutreffend. War der Custodian zum Beizug eines Sub-Custodians befugt, so haftet sie dem Kunden gegenüber nur für gehörige Sorgfalt bei der Auswahl und Instruktion des Sub-Custodians (Art. 399 Abs. 2 OR). Sorgfältige Auswahl heisst in erster Linie, dass der Sub-Custodian über die technischen und operationellen Fähigkeiten verfügt, um die kryptobasierten Vermögenswerte der Kunden sicher verwahren zu können. Darüber hinaus muss das anwendbare Recht für einen angemessenen Schutz in der Insolvenz des Sub-Custodians sorgen.

#### 5.3.3.2 Ausländische und nichtbewilligte Sub-Custodians

Die vorgenannten Anforderungen an das Sub-Custodial Staking könnten sich vor allem auf das Staking-Angebot von ausländischen Anbietern sowie Schweizer Anbietern ohne finanzmarktrechtliche Bewilligung auswirken.

Für den Beizug von Sub-Custodians mit Sitz im Ausland verlangt die FINMA zusätzlich zu den vorgenannten Voraussetzungen, dass diese aus einer *(konkursrechtlich) gleichwertig regulierten Jurisdiktion* stammen. Es geht hierbei in erster Linie darum, dass in einem Konkurs des Sub-Custodians die Aussonderbarkeit von kryptobasierten Vermögenswerten gewährleistet ist. Soweit die Aussonderbarkeit nicht (wie in der Schweiz) durch eine ausdrückliche und eindeutige Gesetzesbestimmung gewährleistet ist, wird man dazu ein Rechtsgutachten (*legal opinion*) einer qualifizierten Kanzlei einholen müssen. In vielen Rechtsordnungen dürfte dieser Nachweis mangels

verwertbarer Rechtsprechung heute noch schwierig sein. Das gilt auch für die Mitgliedstaaten der EU, wird die konkursrechtliche Behandlung von Kryptowerten doch durch MiCAR nicht berührt.

Die FINMA verlangt ferner, dass ein Anbieter von Sub-Custodial Staking selbst oder als Teil einer Gruppe der *prudenziellen Aufsicht in der Schweiz oder im Ausland* untersteht. Die FINMA setzt ausserdem voraus, dass die Due Diligence-Prüfung auch die Einhaltung einer allfälligen *Bewilligungspflicht* umfasst. Der Sub-Custodian muss nach dem Gesagten nicht selbst bewilligt sein, wenn er nach den auf ihn anwendbaren Rechtsnormen die Verwahrungs- und Staking-Tätigkeiten bewilligungsfrei ausüben darf. In diesem Fall muss er aber Teil einer prudenziell beaufsichtigten Finanzgruppe sein.

Obschon die Absicht hinter diesen Ausführungen nachvollziehbar ist, sind die Anforderungen zu weitgehend: Banken und Personen nach Art. 1b BankG sollten den aus ihrer Sicht *besten* Anbieter auswählen können. Der Umstand der prudenziellen Beaufsichtigung des Anbieters (wie auch dessen gute Bonität) sind dabei weniger entscheidend als die konkursrechtliche Behandlung der gestakten kryptobasierten Vermögenswerte im Konkurs des Anbieters. Denn die Konkursfestigkeit von Vermögenswerten ist gerade der relevante Unterschied zu einer treuhänderisch für den Kunden gehaltenen Anlage im Devisenbereich, welche typischerweise dem Ausfallrisiko der Drittbank ausgesetzt ist (siehe auch oben Ziff. 5.3.3.1).

Auch unter Berücksichtigung der Richtlinien der SBVg betreffend Treuhandanlagen lässt sich die Auffassung der FINMA nicht aufrechterhalten: Banken treten im Verkehr regelmässig als Treuhänderinnen ihrer Kunden auf. Dies kann im Interesse der Bank oder aber des Kunden geschehen. Typisch ist die treuhänderische Anlage etwa bei der Festgeldanlage in Fremdwährungen bei ausländischen Drittbanken. Dem Treuhandgeschäft liegt typischerweise ein Auftragsverhältnis zugrunde. Die Bank hat mit anderen Worten die Weisungen des Kunden zu befolgen. Auf Risiken und Besonderheiten des Treuhandgeschäfts wird sie den Kunden, zumindest wenn es sich um keinen professionellen Kunden handelt, regelmässig hinzuweisen haben. Für Schäden aus dem Konkurs des Dritten, bei dem die Anlage vorgenommen wurde, haftet die Bank ihrem Treuhandkunden nur, wenn sie selber die Auswahl des Dritten vorgenommen hat und dabei unsorgfältig vorgegangen ist. Damit bleibt es aber möglich, dass ein Kunde seiner Bank den Auftrag erteilt, das Staking über einen *bestimmten* ausländischen oder schweizerischen Sub-Custodian auszuführen, selbst wenn dieser nicht selbst oder als Teil einer Gruppe prudenziell beaufsichtigt bzw. bewilligt sein sollte. Hier bezeichnet der Bankkunde die Gegenpartei der «Anlage» unter Inkaufnahme der Risiken selbst.[33]

## 5.4 Fazit

Die FINMA schafft mit der FINMA-Aufsichtsmitteilung 08/2023 Klarheit für die Praxis der Marktteilnehmer in der zentralen (und bislang umstrittenen) Frage, ob gestakte kryptobasierte Vermögenswerte trotz Lock-Ups und Slashing-Risiken im Einzelfall als jederzeit bereitgehalten i.S.v. Art. 16 Ziff. 1$^{bis}$ BankG gelten.

Unter Beachtung der in der Aufsichtsmitteilung aufgestellten Anforderungen ist es für Banken und Personen nach Art. 1b BankG somit möglich, Custodial Staking-Dienstleistungen anzubieten und zu diesem Zweck unter gewissen Bedingungen auch Drittanbieter für die Verwahrung und technisch-administrative Dienstleistungen beizuziehen. In diesem Fall entfallen für Banken die in der

[33] Vgl. SBVg, Richtlinien betreffend Treuhandanlagen 2016, Ziff. III 1. f).

ersten Fassung dieses Zirkulars als prohibitiv bezeichneten Eigenmittelvorgaben beim Custodial Staking.

In einem Sub-Custody-Setup sind die gestakten kryptobasierten Vermögenswerte sodann über Art. 16 Ziff. 2 BankG absonderbar, weil es sich bei dieser Form um eine fiduziarische Strukturierung der Staking-Dienstleistungen für den Bankkunden handelt.

In vielen Punkten vollzieht die Aufsichtsmitteilung die in der Industrie bereits gelebte Praxis nach. In einigen Punkten löst sie aber auch neue Fragen aus: Gerade in Bezug auf das Sub-Custodial Staking stellen sich insbesondere Fragen zum Umfang und Inhalt der Due Diligence-Pflicht des Custodians und Staking-Anbieters sowie zur Länge der Staking-Kette und der möglichen Glieder in der Kette.

# 6. Kollektivanlagenrecht

Weiter stellt sich die Frage, ob *Custodial* Staking als kollektive Kapitalanlage qualifiziert werden könnte.

## 6.1 Einleitung

Gemäss Art. 2 Abs. 1 sind dem KAG unabhängig von der Rechtsform (i) kollektive Kapitalanlagen und Personen, die diese aufbewahren, (ii) ausländische kollektive Kapitalanlagen, die in der Schweiz angeboten werden, sowie (iii) Personen, die in der Schweiz ausländische kollektive Kapitalanlagen vertreten, unterstellt. Nicht unterstellt sind u.a. operative Gesellschaften, die eine unternehmerische Tätigkeit ausüben.

Nach Art. 7 Abs. 1 KAG sind kollektive Kapitalanlagen Vermögen, die von Anlegern zur gemeinschaftlichen Kapitalanlage aufgebracht und für deren Rechnung verwaltet werden, wobei die Anlagebedürfnisse der Anleger in gleichmässiger Weise befriedigt werden.

## 6.2 Kollektive Kapitalanlage

Custodial Staking kann je nach operationeller Ausgestaltung zum «Pooling» von gestakten Token in einem Smart Contract oder dergleichen führen. Damit liegt allerdings nicht *Gemeinschaftlichkeit* der Kapitalanlage in Form eines «pot commun» i.S.d. KAG vor, sondern lediglich die technisch notwendige Zusammenführung von kryptobasierten Vermögenswerten zum Zweck des Stakings. Jede Kundin des Staking-Anbieters kann weiterhin frei über ihre Staking-Position verfügen und somit jederzeit ein Unstaking ihrer Token verlangen. Etwas Anderes kann dort gelten, wo der Betrieb einer Validator Node ein Minimum-Stake voraussetzt, wobei die kryptobasierten Vermögenswerte mehrerer Kunden eines Dienstleisters für den Betrieb der Node zusammengelegt werden (so z.B. im Fall von Ethereum, deren Validatoren jeweils 32 ETH erfordern).

Ferner ist für eine kollektive Kapitalanlagetätigkeit *Fremdverwaltung* vorauszusetzen. Staking ist jedoch eine weitgehend ermessensfreie Tätigkeit im Auftrag des Kunden (*Execution-Only*). Es besteht keine Anlagepolitik, sondern jede Veränderung des Stakings-Auftrags erfolgt gemäss Instruktion des Kunden. Ebenso wenig stellt die Vermeidung von operationellen Risiken in Form von Slashing oder die technisch-administrative Optimierung der Staking-Dienstleistung durch den Staking-Anbieter eine Form der Anlagepolitik i.S.d. KAG dar.

Staking hat nach dem Gesagten vom Risikoprofil her eine grössere Ähnlichkeit mit einer unternehmerischen Tätigkeit oder ggf. einer selbstverwalteten «Anlagetätigkeit» als mit einer kollektiven Kapitalanlage.

# 7. Finanzdienstleistungsrecht

## 7.1 Einleitung

Art. 3 lit. d FIDLEG definiert den Begriff der Finanzdienstleistung. Dabei handelt es sich um für den Kunden erbrachte Tätigkeiten, die jeweils im Zusammenhang mit einem Finanzinstrument stehen, wie etwa den Erwerb und die Veräusserung, die Annahme und Übermittlung von Aufträgen, die Anlageberatung und die Vermögensverwaltung.

Die reine Verwahrung von Token ist keine Finanzdienstleistung, selbst wenn die Token als Finanzinstrumente qualifiziert werden sollten.

## 7.2 Finanzdienstleistung

In aller Regel sind die gestakten Token *keine* Finanzinstrumente.[34] Bei den Token, die üblicherweise zur Konsensbildung eines Staking-Protokolls verwendet werden, handelt es sich um Zahlungs- und/oder Nutzungs-Token nach der Auslegungshilfe in der ICO-Wegleitung der FINMA. Ein einmal gestakter Token kann bei Anwendbarkeit eines Lock-Ups zwar nicht mehr frei übertragen werden. Infolgedessen ändern sich allerdings die (technischen) Eigenschaften des Tokens nicht. Der Token verkörpert mit anderen Worten aufgrund seiner Blockierung in einem Staking-Protokoll in der Regel keine Rechtsansprüche. Somit ändert auch der Staking-Vorgang als solcher nichts an der fehlenden Qualität von Staking (bzw. des zugrundeliegenden Rechtsverhältnisses) als Finanzinstrument und Effekte.

Staking weist sodann in keiner der Ausprägungen Elemente einer Finanzdienstleistung i.S.d. FIDLEG auf. Namentlich zielt ein Staking-Auftrag des Kunden nicht *direkt* auf den Erwerb und die Veräusserung von konkreten Finanzinstrumenten ab (vgl. Art. 3 Abs. 2 FIDLEV); demgegenüber werden Staking Rewards im Zusammenhang mit der Validierung als Entgelt für die Tätigkeit «beiläufig» ausgeschüttet. Ferner fehlt es auch an der Annahme und Übermittlung von Aufträgen, die Finanzinstrumente zum Gegenstand haben. In diesem Fall werden Aufträge des Kunden im Hinblick auf den Geschäfts- und Transaktionsabschluss angenommen und üblicherweise an Dritte übermittelt.[35] Beim Ausführen eines Staking-Auftrags des Kunden, der in die Blockierung der kryptobasierten Vermögenswerte im PoS-Protokoll resultiert, kommt demgegenüber kein solcher Abschluss zustande.

[34] Vgl. hierzu Fabio Andreotti/Stephan Zimmermann/Florian Prantl, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, S. 349; ferner Yannick Fuchs, Staking auf der Ethereum-Blockchain – Ausgewählte zivil- und aufsichtsrechtliche Aspekte, in: Magister, Editions Weblaw, Bern 2023, Rz. 125 ff.

[35] Siehe etwa SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. c N 91 ff., 101, Zürich 2021; BSK FIDLEG/FINIG-Rayroux, Art. 3 lit. c FIDLEG N 41 ff., Basel 2023.

# 8. Finanzmarktinfrastruktur- und Marktverhaltensrecht

## 8.1 Einleitung

Der Begriff der Finanzmarktinfrastruktur ist abschliessend in Art. 2 lit. a FinfraG definiert. Darunter fallen u.a. Börsen, Zentralverwahrer, DLT-Handelssysteme und Zahlungssysteme.

Unter Marktverhaltensregeln werden u.a. Bestimmungen zum Insiderhandel und zur Marktmanipulation verstanden (Art. 142 ff. FinfraG).

## 8.2 Finanzmarktinfrastruktur und Marktverhalten

Der Betrieb von Custodial Staking stellt keine Finanzmarktinfrastruktur dar. Namentlich beinhaltet Custodial Staking weder den multilateralen oder bilateralen Handel von Effekten und Finanzinstrumenten noch die Abrechnung und Abwicklung solcher Geschäfte.

Da die stakbaren Token in der Regel keine Anlage-Token darstellen, ist der Effektenbegriff zum Vornherein nicht erfüllt. Mangels Vorliegens einer Effektenhandelstätigkeit sind die Marktverhaltensregeln gemäss FinfraG grundsätzlich nicht anwendbar. Banken haben jedoch die in diesem Zusammenhang anwendbaren Gewährsvorschriften (z.B. mit Blick auf Marktverhaltensregeln) zu beachten.

# 9. Geldwäschereirecht

## 9.1 Einleitung

Banken und Personen nach Art. 1b BankG gelten von Gesetzes wegen als Finanzintermediäre (Art. 2 Abs. 2 lit. a GwG). Als Finanzintermediäre gelten ferner Personen, die berufsmässig fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen (Art. 2 Abs. 3 GwG).

## 9.2 Unterstellung und GwG-Pflichten

Unabhängig von der Notwendigkeit einer Bewilligung als Bank oder Person nach Art. 1b BankG sind Staking-Anbieter im Bereich des *Custodial* Staking in der Regel dem GwG unterstellt, da bei der Aufbewahrung der kryptobasierten Vermögenswerte Verfügungsmacht über die *fremden* Vermögenswerte erlangt wird.

Eine GwG-Unterstellungspflicht hat somit für Nicht-Banken u.a. eine Anschlusspflicht an eine Selbstregulierungsorganisation (SRO) zur Folge und verpflichtet alle Finanzintermediäre zur Einhaltung der anwendbaren Sorgfalts- und Meldepflichten.

Auch für das *Non-Custodial* Staking in Form des SaaS kann sich die Unterstellungsfrage stellen: Art. 4 Abs. 1 lit. b GwV knüpft nicht mehr ausschliesslich an den Begriff der Verfügungsmacht

über fremde Vermögenswerte an. Deshalb ist abzuklären, ob der Staking-Anbieter über eine vergleichbar gesteigerte Form der Kontrolle der Vermögenswerte des stakenden Kunden verfügt.[36] Der Anbieter des Non-Custodial Stakings hat regelmässig keinen Zugriff auf die gestakten Vermögenswerte des Kunden, vergleichbar mit der dem GwG nicht unterstellten Abwicklung von Transaktionen ohne Zugriffsmöglichkeit des Betreibers einer Handelsplattform.[37] Dass keine Verfügungsmacht beim Non-Custodial-Drittanbieter vorliegt, kann etwa im Rahmen von Ethereum-Staking mit der Vorsignierung und Übermittlung einer VEM an den Solo-Staker bzw. Staking-Anbieter sichergestellt werden. Ferner fehlt es beim Staking an der für Dienstleistungen für den Zahlungsverkehr typischen Übertragung von fremden Vermögenswerten an eine Drittperson.

Die Anwendbarkeit des GwG kann in gewissen Fällen verneint werden, bspw. wenn Staking-Dienstleistungen ausschliesslich gegenüber inländischen und ausländischen prudenziell beaufsichtigten Finanzintermediären erbracht werden (Art. 2 Abs. 4 lit. d GwG).

Es wird empfohlen, die relevanten Sorgfaltspflichten im Zusammenhang mit der Erbringung von Staking-Dienstleistungen unter Einbezug des konkreten Setups genau zu prüfen.

## 9.3 Travel Rule

Die FINMA-Aufsichtsmitteilung 02/2019 «Zahlungsverkehr auf der Blockchain» hält fest, dass beim Zahlungsverkehr im Blockchain-Bereich die Voraussetzungen von Art. 10 GwV-FINMA bzw. der einschlägigen Bestimmungen einer SRO zur Anwendung gelangen.

Da Staking-Dienstleistungen keine «Zahlungsfunktion» aufweisen, sollte die Travel Rule gemäss FINMA-Aufsichtsmitteilung nicht anwendbar sein.

Die der Travel Rule zugrundeliegenden Themen (Verhinderung Terrorismusfinanzierung, Umgehung Sanktionen etc.) sind insofern bei Staking weniger relevant, als dass die eingesetzten Vermögenswerte grundsätzlich nicht an Dritte übertragen werden und die Kontrolle beim Staking-Anbieter verbleibt.

Staking Rewards werden sodann direkt vom Protokoll neu geschöpft oder, soweit aus Transaktionsgebühren der Nutzer der Blockchain stammend, durch das Protokoll vermittelt und in der Folge vom Staking-Anbieter an die Kunden weitergeleitet. Da es sich bei Staking Rewards um ein Entgelt für Validierungsleistungen handelt, liegt in der Regel ebenfalls keine Zahlungsfunktion vor.

# 10. Steuerrecht

## 10.1 Verrechnungssteuer

Gegenstand der Verrechnungssteuer sind u.a. Erträge aus beweglichem, bei Inländern angelegtem Kapitalvermögen, Gewinne aus Geldspielen sowie aus Lotterien und Geschicklichkeitsspie-

[36] Siehe EFD, Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Erläuterungen, 18.06.2021, S. 11, 22.
[37] *Gl.M.* Fabio Andreotti/Stephan Zimmermann/Florian Prantl, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, S. 336 FN 19.

len zur Verkaufsförderung sowie gewisse Versicherungsleistungen. Erträge aus beweglichem Kapitalvermögen sind namentlich Zinsen aus Obligationen und Kundenguthaben, Dividenden und sonstige Erträge aus Beteiligungsrechten und Anteilen an kollektiven Kapitalanlagen.

Beim Custodian handelt es sich um ein Institut (Depotbank), das Wertpapiere bzw. andere Vermögenswerte im Auftrag von Kunden verwahrt. Im Falle von kryptographischen Vermögenswerten «speichert» der Custodian Bestände an digitalen Vermögenswerten im Auftrag der Anleger. Sie verwalten diese grundsätzlich nicht im eigenen Namen und auf eigene Rechnung. Da es in der Regel beim Staking am Steuerobjekt im verrechnungssteuerlichen Sinne fehlt, unterliegen die Staking Rewards, welche einem Anleger gutgeschrieben werden, zumindest auf Ebene des verwahrenden Instituts nicht der Verrechnungssteuer.

Eine hiervon abweichende Beurteilung ergibt sich bei Anlage-Token, welche Beteiligungsrechte abbilden (Aktien oder andere Beteiligungsrechte). Zahlungen im Zusammenhang mit auf Anlage-Token mit Beteiligungsrechten basierenden Verpflichtungen sind als Erträge von Aktien oder anderen Beteiligungspapieren einzustufen und somit verrechnungssteuerpflichtig. Hier wäre jedoch der Emittent und nicht die Verwahrstelle in der Pflicht, die Verrechnungssteuer abzuliefern und auf die Investoren zu überwälzen. Von den Anlage-Token mit Beteiligungsrechten sind Anlage-Token mit vertraglicher Grundlage zu unterscheiden. Letztere lösen keine Verrechnungssteuerpflicht aus.

## 10.2 Gewinnsteuer

Da der Custodian die Bestände an digitalen Vermögenswerten lediglich im Auftrag der Anleger verwahrt, fliessen dem Custodian hieraus keine steuerpflichtigen Erträge zu.

Für die abgesicherte Verwahrung der Bestände an digitalen Vermögenswerten behält sich der Custodian in aller Regel eine Gebühr ein, die sog. *Staking Fee*. Dieses umfasst in der Praxis in der Regel einen Prozentsatz der Staking Rewards. Hierbei handelt es sich um einen Dienstleistungsertrag, der als solcher den Reingewinn des Custodians erhöht und damit der Gewinnsteuer unterliegt.

## 10.3 Emissionsabgabe

Gegenstand der Emissionsabgabe sind die entgeltliche oder unentgeltliche Begründung und Erhöhung des Nennwertes von Beteiligungsrechten u.a. in Form von Aktien, Stammanteilen und Partizipationsscheinen inländischer Gesellschaften.

Da der Custodian die Bestände an digitalen Vermögenswerten nur verwahrt und hierdurch nicht direkt Nennwert begründet oder ein solcher Nennwert erhöht wird, fällt auf dieser Stufe keine Emissionsabgabe an. Werden hingegen Anlage-Token mit Beteiligungsrechten ausgegeben, unterliegt die Emission solcher Token beim Emittenten der Emissionsabgabe.

## 10.4 Umsatzabgabe

Die Umsatzabgabe wird auf den Käufen und Verkäufen von in- und ausländischen Wertpapieren erhoben, sofern eine der Vertragsparteien oder einer der Vermittler Effektenhändler (im steuerrechtlichen Sinne) ist.

Das Staking selbst stellt keinen Tatbestand dar, der von der Umsatzabgabe zu erfassen ist. Sofern der Custodian als Vermittler auftritt und den Handel mit den ihm überlassenen Beständen an digitalen Vermögenswerten mit Wertpapiercharakter (d.h. Anlage-Token, die Aktien oder andere Beteiligungsrechte abbilden) betreibt, handelt es sich um einen der Umsatzabgabe unterliegenden Tatbestand, auf den eine halbe Abgabe zu leisten ist, sofern es sich beim Custodian um einen Effektenhändler (im steuerrechtliche Sinne) handelt.

## 10.5 Mehrwertsteuer

### 10.5.1 Blockierung von kryptobasierten Vermögenswerten in einem Protokoll

Durch die Blockierung des Stakes selbst führt der Staker dem Protokoll keinen verbrauchsfähigen Vermögenswert definitiv zu. Funktionsweise und Ausgestaltung des Stake entsprechen eher einem Pfand, das der Staker zurückerhält, sofern er sich regelkonform verhält. Mangels Leistung gelten solche Mittelflüsse aus Sicht der Mehrwertsteuer nicht als Entgelt (Art. 18 Abs. 2 lit. h MWSTG). Im Umkehrschluss muss auch für die Hinterlegung des Pfands gelten, dass dieses keine Leistung in Erwartung eines Entgelts darstellt.

### 10.5.2 Validierung

Die ESTV unterschied bis anhin danach, ob der Staking Reward die Form vom Protokoll neu geschaffener Vermögenswerte hat (sog. *Block Reward* – ein Nicht-Entgelt mangels bestimmbarer Gegenpartei) oder ob der Staking Reward dem Validator vom Versender zugesprochen wird (ein Entgelt für eine steuerbare Leistung).[38]

Im ersten Urteil[39] im Bereich der Mehrwertsteuer zum Themenkomplex der Validierungsleistungen in PoS-Netzwerken stellte das Bundesverwaltungsgericht fest, dass Validatoren in Netzwerken, die theoretisch auch die Bildung «leerer» Blöcke vorsehen, grundsätzlich zwei Leistungen erbringen: (i) das Hinzufügen neuer Blöcke zur Blockchain als Leistung gegenüber dem Netzwerk und (ii) die Transaktionsverarbeitung als Leistung gegenüber den Versendern von Transaktionen. Sofern die Tätigkeiten gegenüber *dezentralen Netzwerken* erbracht werden, fehle es mangels bestimmbaren Leistungsempfängers an einer Gegenpartei und mithin an einem mehrwertsteuerlichen Leistungsaustausch. Die Transaktionsverarbeitung für die Versender stelle jedoch eine grundsätzlich steuerbare, dem Empfängerortsprinzip unterliegende Dienstleistung dar.

Dabei obliegt es nach Auffassung der Autoren dem Steuerpflichtigen, den Nachweis zu erbringen, dass ein Leistungsempfänger im Ausland ansässig ist (dem Grundsatz folgend, dass steuerbegründende und -erhöhende Umstände von der ESTV, steueraufhebende oder -mindernde vom Steuerpflichtigen nachzuweisen sind). Andernfalls schuldet er die Mehrwertsteuer auf die anteilig ihm zugewiesene Transaktionsgebühr. Um den Steuerpflichtigen Planungssicherheit zu geben, wäre es durchaus denkbar und wünschenswert, dass die Steuerverwaltung sich in einer Praxispublikation dazu äussert, wie der Nachweis der Ansässigkeit des Leistungsempfängers in einem weitgehend pseudonymisierten Umfeld anerkanntermassen gelingen kann, bzw. Alternativen – neben einem einzelfallbezogenen Ruling mit der ESTV – formuliert, welche näherungsweisen Ermittlungsmethoden nach Ansicht der ESTV grundsätzlich denkbar sind (wie sie dies bspw. bei

[38] Vgl. ESTV, MWST-Info 04 Steuerobjekt, Ziff. 2.7.3.5.
[39] BVGer vom 29.08.2023, A-5638/2022.

der Ermittlung einer Vorsteuerkorrektur im Zusammenhang mit gemischter Verwendung durchaus schon macht).

Nicht vollständig geklärt ist, unter welchen Voraussetzungen ein Netzwerk als «dezentral» qualifiziert und wie die mehrwertsteuerrechtliche Situation bei nicht dezentralen Netzwerken zu beurteilen ist.

Für die Beurteilung der mehrwertsteuerlich relevanten Frage, wer als Leistungserbringer der Validierungsleistungen gilt (und damit potentiell als MWST-pflichtige Person), ist zwischen den verschiedenen Modellen von Staking zu differenzieren (siehe oben Ziff. 2.4.2).

#### 10.5.2.1 Self-Staking

Self-Staking ist eine Art des Non-Custodial Stakings. Beim Self-Staking führt die stakende Person alle notwendigen technischen und administrativen Schritte selbst aus: Sie betreibt eine Validator Node, um am Konsensmechanismus des Protokolls teilzunehmen, und ist für die Aufbewahrung der Private Keys der gestakten Token selbst verantwortlich.

Wer als Leistungserbringer zu gelten hat, bestimmt sich laut Art. 20 Abs. 1 MWSTG nach dem Aussenauftritt. Das mehrwertsteuerlich relevante Handeln wird demgemäss grundsätzlich demjenigen zugeordnet, der gegenüber Dritten im eigenen Namen auftritt. Beim Self-Staking dürfte dies regelmässig die stakende Person selbst sein.

#### 10.5.2.2 Staking-as-a-Service

Die ESTV hat sich zu den verschiedenen Formen des Stakings unter Beizug Dritter als Dienstleister noch nicht geäussert. Bei allen Varianten stellt sich vornehmlich die Frage, welche Partei nach Aussen als Validator auftritt: der Kunde oder der Staking-Anbieter.

Wenig hilfreich ist zur Bestimmung des Leistungsempfängers vorliegend das Kriterium des Aussenauftritts. Verträge oder Fakturen an den Empfänger der Validierungsleistung, welche Rückschlüsse auf den Leistungsempfänger zuliessen, werden in diesem Kontext regelmässig nicht erstellt werden. Beim (Non-Custodial) Staking-as-a-Service bezieht der Kunde lediglich die notwendige Software und Hardware von einem Dritten, die Verwahrung der vom Kunden erstellten Private Keys obliegt dem Kunden. Da die im Zusammenhang mit der Validierungstätigkeit relevanten Public Keys dem Kunden zuordenbar sind, tritt der Kunde nach Aussen als Leistungserbringer für die Validierungstätigkeiten auf und diese sind ihm unmittelbar zuzurechnen.

#### 10.5.2.3 (Sub-)Custodial Staking

Beim (Sub-)Custodial Staking ändern sich zwar die Verwahrungsverhältnisse hinsichtlich der Private Keys. Sofern die relevanten Public Keys auch in dieser Konstellation dem Kunden zuordenbar sind, tritt der Kunde nach aussen als Leistungserbringer für die Validierungstätigkeiten auf und die Validierungsleistungen sind ihm und nicht dem Dienstleister unmittelbar zuzurechnen.

# 11. Schlussfolgerungen

Praxis und Lehre haben die FINMA-Aufsichtsmitteilung 08/2023 «Staking» vom 20. Dezember 2023 grösstenteils begrüsst. Die Aufsichtsmitteilung erhöht in bankaufsichtsrechtlicher Hinsicht zwar die Erwartungen an Anbieter von Custodial und Sub-Custodial Staking-Dienstleistungen,

schafft dadurch aber auch Sicherheit für die Marktteilnehmer in der zentralen (und bislang umstrittenen) Frage der Konkursfestigkeit gestakter kryptobasierter Vermögenswerte trotz des Vorliegens von Lock-Ups und Slashing-Risiken im Einzelfall.

Die vorliegende Fassung des Staking-Zirkulars widmet sich vor allem neuen Themen im Konkurs- und Bankenaufsichtsrecht: In konkursrechtlicher Hinsicht stellen sich nunmehr Detailfragen bezüglich der Verfügungsmacht über die gestakten kryptobasierten Vermögenswerte und deren Zuordnung zu Kunden. Demgegenüber wirft der umfassende Anforderungskatalog, welcher die FINMA in der Aufsichtsmitteilung 08/2023 bewilligten Instituten insbesondere im Bereich des Sub-Custodial Stakings auferlegt, neue rechtliche Fragen auf, zu deren Lösung das vorliegende Zirkular hoffentlich beitragen kann.

Neu ist schliesslich der Abschnitt zu steuerrechtlichen Fragestellungen im Zusammenhang mit Staking. Eine Staking-spezifische Rechtsprechung zeichnet sich insbesondere für den Bereich des Mehrwertsteuerrechts ab. Auch hier stellen sich (neue) praktische Herausforderungen für Personen, die kryptobasierte Vermögenswerte staken.