Zirkular 2023/01

Staking

Genehmigt von der Swiss Blockchain Federation am 29.08.2023

Publikationsdatum: 05.09.2023

Autoren: Digital Assets Arbeitsgruppe (Sub-Gruppe Staking) bestehend aus: Fabio Andreotti (Bitcoin Suisse), Diego Benz (Kaiser Odermatt & Partner), Sandro Brühlmann (PostFinance), Mauro Capiello (Blockchain Innovation Group), Nina Gartmann (Crypto Helvetica AG), Hans Kuhn (Lawside), Silke Nock Widmer (SDX), Ricardo Schlatter (Allegra LAW), Alexander Thoma (PostFinance), Rolf H. Weber (Bratschi).

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

Inhaltsverzeichnis

1. Einleitung

Der innovative Charakter öffentlicher Blockchains bringt bekanntlich eine Reihe neuartiger Rechtsfragen 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 zu einer für alle verbindlichen Sicht der Dinge.

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. Aus Transaktionen werden Blöcke, deren Korrektheit unter Anwendung der Regeln eines Protokolls validiert wird. Die Teilnehmer dieser Systeme werden für ihre Leistungen zugunsten der Blockchain 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 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 deshalb verschiedene Modelle des Stakings herausgebildet. Die Modelle tragen den unterschiedlichen Bedürfnissen der Marktteilnehmer Rechnung, die regelmässig an einer arbeitsteiligen Erbringung von Staking-Dienstleistungen interessiert sind. Für die Schweizer Krypto-Dienstleister stellt Staking eine attraktive Möglichkeit dar, mit ihrem Dienstleistungsangebot den erwähnten Bedürfnissen nachzukommen.

Dieses Zirkular nimmt eine *rechtliche* Beurteilung von Staking vor. Neben einer zivilrechtlichen Einordnung stehen je nach Staking-Modell v.a. konkurs-, bank- und finanzmarktrechtliche Fragestellungen im Vordergrund. Es zeigt sich dabei, dass das Custodial Staking die meisten neuartigen Rechtsfragen aufwirft. Der Schweizer Gesetzgeber hat allerdings mit dem DLT-Mantelerlass[1] vorausschauend einen Rechtsrahmen eingeführt, der auch auf solche Fragen geeignete Antworten geben kann.

[1] Siehe 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 14. August 2023.

2. Staking

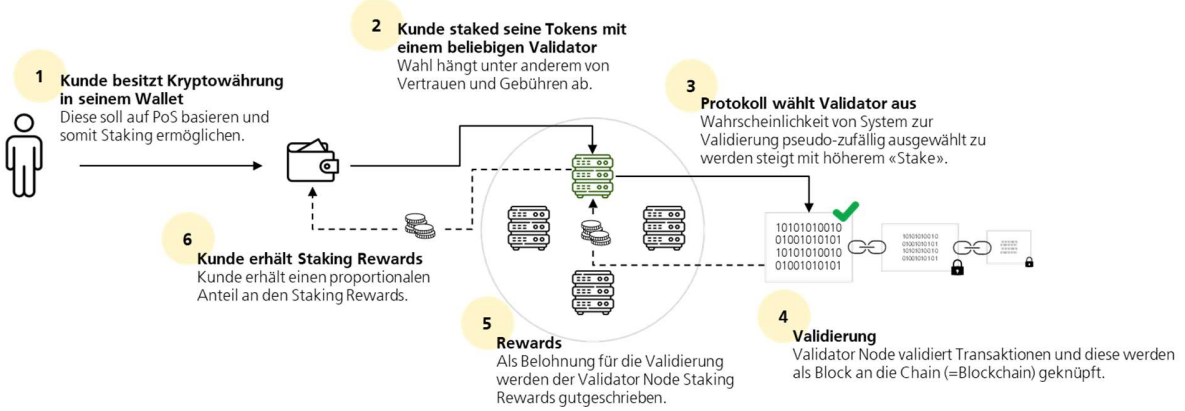
2.1 Funktionsweise

Proof-of-Stake (PoS) 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 motiviert die Validatoren eines Blockchain-Netzwerks, ehrlich und richtig zu handeln, d.h. Transaktionen korrekt zu validieren, weil ihr Stake analog einem Pfand als Sicherheit dient. Validatoren können 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*). 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 jeweils stark unterscheiden kann und die obige Abbildung somit lediglich als illustratives Beispiel verstanden werden soll. Auf eine detaillierte Analyse der Unterschiede zwischen den einzelnen Protokollen wird im vorliegenden Zirkular verzichtet.

2.2 Marktentwicklungen

Der Markt für Staking ist in den letzten Jahren rapide gewachsen, da immer mehr Blockchain-Netzwerke PoS-Konsensmechanismen übernommen haben. Laut einem Bericht der Webseite «Staking Rewards» (stakingrewards.com) erreichte die Gesamtmarktkapitalisierung der gestakten Vermögenswerte in PoS-Netzwerken per Mitte August 2023 über 320 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-Provider. 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*
Ethereum	ETH	4.41%	19.15%	$43.22 Mrd.
Solana	SOL	7.00%	70.83%	$9.9 Mrd.
Cardano	ADA	3.07%	62.45%	$6.54 Mrd.
BNB Chain	BNB	2.08%	14.74%	$5.45 Mrd.
Avalanche	AVAX	7.42%	62.13%	$3.32 Mrd.
Tron	TRX	3.48%	47.70%	$3.31 Mrd.
Polkadot	DOT	14.37%	46.89%	$3.14 Mrd.
Polygon	MATIC	4.79%	39.28%	$2.49 Mrd.
Hedera	HBAR	2.50%	68.09%	$2.25 Mrd.
Cosmos	ATOM	20.36%	69.90%	$2.14 Mrd.

*Quelle: stakingrewards.com, per 15.08.2023

Quelle: stakingrewards.com, per 15. August 2023.

2.3 Erscheinungsformen

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

2.3.1 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, sowie deren Vor- und Nachteile erläutert.

2.3.1.1 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.

2.3.1.2 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.

2.3.1.3 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.

2.3.1.4 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.

2.3.1.5 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.

2.3.1.6 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 ressourcen intensiver sein als andere Staking-Mechanismen.

2.3.1.7 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.

2.3.2 Custody

2.3.2.1 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 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.

2.3.2.2 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-Provider 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 nicht selbst die Hard- und Software betreiben und unterhalten, die für das Staking erforderlich sind. Eine spezielle Art des Custodial Stakings ist das *Sub-Custodial Staking*: In diesem Fall zieht der Staking-Provider eine Drittperson 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 nämlich regelmässig dazu, die Token des Kunden sicher aufzubewahren. Darüber hinaus können Kunden von Custodial Staking-Providern 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.[2]

Das Custodial Staking ist nicht frei von Risiken. Namentlich vertrauen stakende Kunden einer Drittperson, dass sie ihre Token sicher aufbewahren und das Staking mit ihrer Zustimmung ausführen.

[2] Für Staking in Ethereum ist ein Minimum-Stake von 32 ETH notwendig, der bei den heutigen Marktpreisen rund 50’000 Fr. entspricht.

2.3.3 Lock-Up Mechanismen

2.3.3.1 Native Staking

Native Staking bezieht sich auf die Praxis, eine Kryptowährung mit Hilfe des Blockchain-Protokolls zu staken, welches 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 Staking und die 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.

2.3.3.2 Liquid Staking

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

Konkret ermöglicht Liquid Staking den Nutzern des Protokolls, ihre Staking-Positionen in liquiden Token abzubilden, welche 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.

2.4 Rollen

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

2.4.1 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.

2.4.2 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-Provider liegen für den Staker in der einfachen Handhabung des Stakings und dem Wegfall der Anschaffungskosten.

2.4.3 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.

2.5 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.

2.5.1 Chancen

2.5.1.1 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.

2.5.1.2 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.

2.5.1.3 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.

2.5.1.4 Sicherheit und Integrität

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

2.5.1.5 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».

2.5.2 Risiken

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

2.5.2.1 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 Rewards aus.

2.5.2.2 Netzwerkprobleme

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

2.5.2.3 Slashing-Risiko

Je nach PoS-Protokoll besteht für die Staker ein Slashing-Risiko. Konzeptionell können unterschiedliche Formen von Slashing unterschieden werden, die teilweise auch als «Penalties» bezeichnet werden. Ist eine Validator Node länger inaktiv oder handelt sie sogar protokollwidrig, so kann der Staker je nach Protokoll einen Teil oder alle Rewards und im Extremfall selbst die gestakte Position verlieren. Das Slashing-Risiko besteht unabhängig davon, ob Staking in Non-Custodial oder in Custodial Form betrieben wird. Wie weiter unten erwähnt (siehe Ziff. 4.3), können die Risiken des Slashings transparent gemacht und die Risikotragung vertraglich offengelegt und entsprechend zwischen dem Staking-Provider 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. 2.3.2).

3.1 Self-Staking

Self-Staking ist eine Art des Non-Custodial Stakings. Beim *Self-Staking* führt die stakende Person alle notwendigen technischen und 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. Diese Form der Teilnahme setzt je nach Protokoll und gewähltem Setup die technische Expertise des Nutzers voraus. Abgesehen von allfälligen Software-Lizenzvereinbarungen zwischen Entwickler und Nutzer bestehen beim Self-Staking grundsätzlich keine Rechtsverhältnisse. Namentlich möchte sich der Staker in aller Regel auch nicht gegenüber den anderen Validatoren des dezentralen Netzwerks 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-Providers zurück. Die Dienstleistungen des Staking-Providers beschränken sich in der Regel auf die Zurverfügungstellung der notwendigen Hard- und Software.

Ob dem Kunden tatsächlich Staking Rewards ausbezahlt werden, liegt ausserhalb des Einflussbereiches des Staking-Providers. Dies zeigt sich darin, dass (i) die Auswahl der zu vergütenden Nodes bei verschiedenen Staking-Protokollen auf Zufall beruht, (ii) keine Garantie für die Auszahlung von Rewards besteht, (iii) ein allfälliges Slashing die Auszahlung von Rewards verhindern oder verringern kann, (iv) keine fixe, regelmässige Frequenz für die Auszahlung der Rewards besteht und (v) die Höhe allfälliger Rewards nicht vorab bestimmt werden kann. Folglich

schuldet der Staking-Provider dem Kunden kein Ergebnis, sondern nur ein sorgfältiges Tätigwerden gemäss Auftragsrecht.[3]

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

3.3 Custodial Staking

Beim *Custodial Staking* führt der Staking-Provider nicht nur die Validierung der Transaktionen auf der Blockchain selbst durch, sondern bewahrt auch die kryptobasierten Vermögenswerte für den Auftraggeber auf. Der Staking-Provider hält somit in seinem Wallet die Private Keys der stakenden Kunden. Der Kunde hat keine Möglichkeit, direkt auf seine Vermögenswerte zuzugreifen und diese selbst zu staken bzw. zu unstaken. Im Unterschied zum vorstehend beschriebenen Non-Custodial Staking erfolgt somit jegliche Interaktion mit dem Staking-Protokoll durch den Staking-Provider. Zu diesem Zweck kann der Staking-Provider eigene Hard- und Software betreiben oder aber er greift auf die Validator-Node einer Drittperson zurück (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.[4] 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,[5] das nunmehr Elemente der Aufbewahrung mit Elementen des Stakings kombiniert: Der Custodial Staking-Provider hat für den Kunden die Private Keys, welche den Zugriff auf die gestakten kryptobasierten Vermögenswerte vermitteln, weiterhin sicher aufzubewahren. Die vorbestehende hinterlegungsähnliche bzw. fiduziarische Aufbewahrung wird somit durch den Staking-Auftrag nicht aufgehoben, sondern lediglich vom Staking-Rechtsverhältnis *überlagert*.

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

---

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

[4] 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.

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

3.4 Sub-Custodial Staking

Beim sog. *Sub-Custodial Staking* nutzt der Staking-Provider (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 Zweck wiederum eine Drittperson beizieht), um im Auftrag der Kunden des Staking-Providers am Konsensmechanismus des Protokolls teilzunehmen. Zwischen dem Staking-Provider bzw. Custodian und dem Sub-Custodian besteht ein Rechtsverhältnis mit (treuhänderischen) Hinterlegungscharakter. Demgegenüber ist aufgrund der jeweiligen Verfolgung eigener Interessen mit unterschiedlichen Mitteln nicht von einer einfachen Gesellschaft zwischen den beiden Parteien auszugehen.

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

3.5 Fazit

Mit Ausnahme des Self-Stakings schulden Staking-Provider ihren Kunden ein sorgfältiges Tätigwerden gemäss Auftragsrecht (Art. 394 ff., Art. 398 OR). Hinterlegungs-, lizenz- und/oder werkvertragsähnliche Pflichten können hinzutreten, soweit der Staking-Provider auch den Betrieb und Unterhalt von Hard- und Software schuldet.

Die zivilrechtliche Einordnung von Staking-Rechtsverhältnissen als Auftrag legt nahe, dass der Staking-Provider 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 Verlustrisiken der gestakten Token aufgrund von Slashing).

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-Provider grundsätzlich erlöschen, sofern nicht das Gegenteil aus der Natur des Geschäfts hervorgeht. Dies wäre bei einer Qualifikation als Werkvertrag anders, da dieser auch nach Konkurseröffnung weiter bestehen würde. Die Regelung von Art. 405 Abs. 1 OR ist dispositiv, weshalb es sich u.E. empfiehlt, in den Staking-Verträgen eine ausdrückliche Bestimmung vorzusehen, welche das Schicksal der Staking-Verträge nach Konkurseröffnung im Interesse der Kunden 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 Auf-

bewahrers geführt. Davon erfasst ist nicht nur die bankrechtliche Absonderbarkeit von Depotwerten (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 tatsächliche Verfügungsmacht über den Vermögenswert innehaben. Es fallen ausschliesslich 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.[6] 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.[7]

Das Aussonderungsregime von Art. 242a SchKG ist nicht nur für die reine Krypto-Verwahrung 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-Providers Anwendung finden. Dabei stehen insbesondere Fragen im Zusammenhang mit den eingangs erläuterten *Lock-Ups* und *Slashing-Risiken* im Vordergrund der Betrachtung.[8]

4.2 Aussonderung im Konkurs

Die Aussonderung kryptobasierter Vermögenswerte gemäss Art. 242a Abs. 2 SchKG ist grundsätzlich an zwei Voraussetzungen geknüpft:

[6] 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.
[7] Siehe BBl 2020, S. 292.
[8] Hinsichtlich Lock-Ups und Slashing siehe Ziff. 2.1.

4.2.1 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, zu welchem bislang noch keine gefestigte Praxis existiert. Unklar ist insbesondere, ob es genügt, wenn die kryptobasierten Vermögenswerte ständig vorhanden sind, oder aber ob der Aufbewahrer sie auch jederzeit frei übertragen können muss.

Nachfolgend soll der Begriff der Pflicht zur jederzeitigen Bereithaltung anhand der gängigen Methoden ausgelegt werden.[9]

4.2.1.1 Grammatikalische Auslegung

Gemäss Wortlaut von Art. 242a Abs. 2 SchKG verpflichtet sich der Gemeinschuldner, die kryptobasierten Vermögenswerte für den Dritten jederzeit bereitzuhalten. Es geht mit anderen Worten um die Übernahme einer rechtsgeschäftlichen Obligation, die Token für den Kunden jederzeit «[ständig] griffbereit» und «zur Benutzung bereit[zu]halten».[10] Entscheidend ist, dass der Gemeinschuldner vertraglich *verpflichtet* ist, die kryptobasierten Vermögenswerte jederzeit bereitzuhalten. Demgegenüber ist nicht massgeblich, ob die Token *tatsächlich* jederzeit bereitgehalten werden. Ebenso wenig dürfte es ohne entsprechende Verpflichtung genügen, dass der Gemeinschuldner die Token tatsächlich jederzeit bereithält.

Aus dem Begriff der Bereithaltung lässt sich ferner nicht ableiten, dass der Gesetzgeber die faktische Möglichkeit des Krypto-Verwahrers zur jederzeitigen *Übertragung* der kryptobasierten Vermögenswerte vor Augen hatte.

In diesem Sinne haben protokollbedingte Lock-Ups keinen Einfluss auf die Aussonderung im Konkurs.

4.2.1.2 Systematische Auslegung

In systematischer Hinsicht ist das Augenmerk auf Vorschriften mit vergleichbarem Regelungsinhalt zu legen.

Namentlich dient Art. 242 SchKG der konkursrechtlichen Aussonderung von Sachen, die sich im Besitz des Gemeinschuldners befinden. Die Vorschrift setzt keine Pflicht zur jederzeitigen Bereithaltung voraus. Sie verlangt ferner auch nicht, dass eine Sache jederzeit übertragbar ist. Praxisgemäss ist auch nicht zu erwarten, dass hinterlegte Sachen vom Gemeinschuldner tatsächlich jederzeit herausgegeben werden können. Namentlich kann die Auslieferung eines Gegenstandes in der Praxis einige Zeit in Anspruch nehmen. Als Beispiel kann etwa die bei der Auslieferung von traditionellen Depotwerten geltenden üblichen Lieferfristen von Banken angeführt werden. Weitere Mechanismen, die mit Lock-Ups beim Staking vergleichbar sind, kennt man sodann auch z.B. bei Mitarbeiteraktien, welche einer vertraglichen Sperrfrist unterliegen, jedoch grundsätzlich als Depotwerte eingestuft und darum im Konkurs der Verwahrungsstelle aus- bzw. absonderbar sind.

---

[9] Ausführlich hierzu etwa BGE 145 III 324, E. 6.6.

[10] https://www.duden.de/rechtschreibung/bereithalten, zuletzt besucht am 14. August 2023.

Hinzu kommt, dass auch die Beschädigung der hinterlegten Sache (z.B. aufgrund einer Vertragsverletzung des Aufbewahrers) nicht dazu führt, dass die Sache im Konkurs des Aufbewahrers nicht mehr gestützt auf Art. 242 SchKG oder einen anderen Aussonderungsgrund herausgegeben werden kann. Etwas Anderes wäre überraschend und kaum je im Interesse des hinterlegenden Kunden.

Mit anderen Worten legt eine systematische Auslegung nahe, dass das Bestehen von Lock-Ups und Slashing-Risiken die Aussonderung von gestakten Token nicht behindert.

4.2.1.3 Historische Auslegung

Im Rahmen des Gesetzgebungsprozesses wurde Art. 242a SchKG nicht in Bezug auf Staking-Tätigkeiten thematisiert. Der Bundesrat war sich aber sehr wohl bewusst, dass Staking ein bedeutender Konsensmechanismus öffentlicher Blockchain-Netzwerke ist.[11]

Gemäss Botschaft hat der Gemeinschuldner ab dem Zeitpunkt der Übertragung der Verfügungsmacht über die Vermögenswerte durch den Dritten auf ihn oder ab dem Zeitpunkt der Erlangung der Verfügungsmacht über die Vermögenswerte für den Dritten ununterbrochen die Verfügungsmacht über die Vermögenswerte zu haben, wobei es gemäss Bundesrat allerdings ausreicht, wenn sich die entsprechende Pflicht darauf beschränkt, die jeweils für Dritte gehaltene Anzahl Einheiten ununterbrochen in seinem Gewahrsam zu halten.[12]

Die Botschaft führt aus, dass mit einer Aufbewahrung der Token auf einer Sammeladresse die Sicherheit für die Kunden unter Umständen erhöht werden kann, weil dann nicht sämtliche Token aller Kunden einem ständigen Zugriff unterliegen müssen, sondern ein Teil der Token, auf die nicht oder nur selten zugegriffen werden muss, *unter qualifizierten Zugriffsberechtigungen* und damit sicherer aufbewahrt werden können.[13]

Daraus ergibt sich, dass der Gesetzgeber die Verwahrungsformen des «Cold Storage» als durchaus mit der Pflicht der jederzeitigen Bereithaltung vereinbar erachtet, obwohl die Vermögenswerte praxisgemäss nicht sofort aus der Verwahrung entnommen werden können. Es wird also wiederum keine ständige Übertragbarkeit der Token vorausgesetzt. Die Situation des Cold Storage ist mit der Blockierung von kryptobasierten Vermögenswerten auf einer Validator Node oder in einem Smart Contract mit dem Ziel der Teilnahme am Konsensmechanismus vergleichbar, wobei Lock-Ups auf die vorübergehend blockierten Token zur Anwendung gelangen.[14]

Schliesslich führt die Botschaft an unterschiedlichen Stellen aus, dass die «Schlüssel» für den Zugriff auf die kryptobasierten Vermögenswerte zentral sind.[15] Gemeint sind damit die *Private Keys*, welche über ein kryptobasiertes Zugangsverfahren die Verfügungsmacht über die Token vermitteln. Das Staking von Token führt gerade nicht zu einer Verschiebung der Verfügungsmacht oder zu Veränderungen an den Kontrollverhältnissen. Im Gegenteil, während dieser besonderen Form der Verwahrung, kann weiterhin ausschliesslich der Custodial Staking-Provider im Auftrag

[11] Vgl. BBl 2020, S. 282.
[12] Siehe BBl 2020, S. 292.
[13] Siehe BBl 2020, S. 247.
[14] So auch Thomas Jutzi/Andri Abbühl, Fintech und DLT. Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023, Rz. 150.
[15] Siehe BBl 2020, S. 263 ff., 292, ferner 278.

des Kunden über dessen gestakte Token verfügen. Die Private Keys, selbst wenn die Token zwecks Stakings auf die Adresse eines Smart Contracts übertragen werden müssen, können nach dem Gesagten ohne Weiteres als jederzeit bereithalten i.S.v. Art. 242a Abs. 2 SchKG betrachtet werden.

4.2.1.4 Teleologische Auslegung

Gemäss Botschaft ging es dem Gesetzgeber bei der Statuierung der Pflicht des jederzeitigen Bereithaltens um die Unterbindung von Eigen- bzw. Aktivgeschäften im Sinne des Kundenschutzes.[16] Entscheidend ist somit, dass weder die Krypto-Verwahrerin noch ein Dritter über die gestakten Token auf eigene Rechnung und eigenes Risiko verfügen kann und dass die Vermögenswerte nach Konkurseröffnung noch «da» sind, d.h. den Gläubigern noch ausbezahlt werden können.

Staking wird in der Botschaft nicht als Anwendungsfall eines möglichen Eigengeschäfts des Staking-Providers bezeichnet. Dies scheint denn auch offenkundig, erfolgt Staking doch in aller Regel instruktionsgemäss auf Rechnung und Risiko des Kunden. Staking ohne Weisung des Kunden stellt proprietäres Stakig dar. Darüber hinaus stehen Token, wenn sie gestakt sind, dem Staking-Provider *technisch* nicht für Anlagezwecke zur Verfügung, was ihn daran hindert, sie für eigene Zwecke zu nutzen.

Damit sollte der Aussonderung im Konkurs grundsätzlich so lange nichts im Wege stehen, als der Staking-Provider keine Eigen- und Aktivgeschäfte mit dem Kundenvermögen vornimmt, soweit er hierzu überhaupt fähig ist. Auch in teleologischer Hinsicht lässt sich somit *nicht* der Schluss ziehen, dass der Aufbewahrer die kryptobasierten Vermögenswerte seiner Kunden jederzeit frei übertragen können muss.

4.2.2 Einzel- und Sammelverwahrung

Zweitens müssen neben der Pflicht zur jederzeitigen Bereithaltung 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 resp. in einer speziellen Wallet gehalten werden, die der berechtigten Person zugewiesen ist.[17] Dabei reicht es aus, wenn sich diese Zuordnung aus einem internen Register des Gemeinschuldners ergibt (z.B. eine Kundenbuchungssoftware).[18] Soweit es technisch vorgesehen ist, dass die Token individualisiert werden können, indem beispielsweise 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

[16] Siehe BBl 2020, S. 292, 303.
[17] Siehe BBl 2020, S. 293.
[18] Siehe BBl 2020, S. 293.

beim Gemeinschuldner verfügbaren Zuordnungstabelle der berechtigten Person zugeordnet werden kann.[19]

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 resp. einer Sammelwallet aufzubewahren.[20]

Im Zusammenhang mit der Verwahrung der gestakten Token ist festzuhalten, dass *Staking* protokollbedingt unterschiedlich ausgeführt wird. In gewissen Fällen verbleiben die Token im ursprünglichen Wallet des Kunden beim Custodial Staking-Provider (so z.B. Tezos). In anderen Fällen werden sie an einen Smart Contract übertragen (so z.B. Polygon), wobei der ursprüngliche oder aber ein 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-Provider.

Schliesslich 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 (siehe hierzu sogleich).[21]

4.3 Fazit

Die Auslegung von Art. 242a SchKG nach den bekannten Methoden macht deutlich, dass der Gesetzgeber keine ständige technische Übertragbarkeit der kryptobasierten Vermögenswerte voraussetzt. Vielmehr wird es als genügend erachtet, wenn eine vertragliche Verpflichtung des Custodial Staking-Dienstleisters besteht, die Verfügungsmacht über die Token aufrechtzuerhalten und diese ständig vorhanden *sind, z.B. indem ein ständiger Zugriff auf die Private Keys gewährleistet ist.*

Für gestakte kryptobasierte Vermögenswerte sind die der Verfügungsmacht über die Token zugrundeliegenden Private Keys ungeachtet des konkreten Staking-Setups grundsätzlich jederzeit für den Kunden bereitgehalten. Damit stehen Lock-Ups einer Aussonderung im Konkurs des Staking-Providers nicht im Wege.

In diesem Sinne stellen vergleichbare Sachverhalte, wie etwa IT-Systemunterbrüche und Vermögenssperren nach Art. 10 GwG, richtigerweise auch nicht die Herausgabefähigkeit von Vermögenswerten im Konkurs in Frage. Etwas Anderes wäre auch kaum je im Interesse der Kunden eines konkursiten Staking-Providers.

[19] Siehe BBl 2020, S. 293.
[20] Siehe BBl 2020, S. 293.
[21] Siehe BBl 2020, S. 291.

Dass ein Lock-Up im Konkursfall unproblematisch ist, wird auch daran ersichtlich, dass die Konkursbehörden die Private Keys, mit welchen die gestakte Position kontrolliert wird, «off-chain» an die Kunden herausgeben könnte (z.B. auf einem verschlüsselten USB-Stick oder schlicht mittels Versands einer verschlüsselten E-Mail). Vor diesem Hintergrund wären die kryptobasierten Vermögenswerte selbst *jederzeit übertragbar*. In der Praxis wird es allerdings im Interesse des Kunden sein, dass die Konkursbehörden trotz grundsätzlicher Übertragbarkeit der Private Keys ein Unstaking vornehmen und die Lock-Up-Periode abwarten, um auf dem herkömmlichen Weg die Vermögenswerte herauszugeben. Das Abwarten müssen eines Lock-Ups scheint sodann die Länge der konkursrechtlichen Auseinandersetzung kaum negativ zu beeinträchtigen.[22]

Ein latent bestehendes, aber praktisch unwahrscheinliches Slashing-Risiko ändert an der Aussonderbarkeit ebenfalls nichts. Der Kunde ist aber im Rahmen einer umfassenden Risikoaufklärung darüber zu informieren. Das Slashing-Risiko wird dadurch auf der zivilrechtlichen Ebene genügend adressiert, welche die Hinterlegungsstelle zu einem sorgfältigen Tätigwerden verpflichtet. Dabei ist zu beachten, dass Staking-Provider in der Praxis nicht jegliche Fehler anlässlich des Stakings vertraglich auf den Kunden überwälzen können (vgl. Art. 100 Abs. 1 OR). Der Kunde wird somit regelmässig schadlos gehalten, wobei es dem Dienstleister selbstredend freisteht, die finanziellen Auswirkungen von Slashing-Ereignissen vollständig selbst zu tragen. Alternativ kann er dem Kunden ggf. eine Versicherung gegen Slashing-Risiken anbieten.

Custodial Staking stellt im Vergleich zu den Modellen des Non-Custodial Stakings (Self-Staking und SaaS) einen weiteren Schritt in der *Arbeitsteilung* und Spezialisierung von Staking-Dienstleistungen dar. Anders als beim Non-Custodial Staking übernimmt der Dienstleister beim Custodial Staking alle Elemente des Stakings. Damit sind *dienstleistungsspezifische* Risiken verbunden, welche typischerweise von der Rechtsordnung adressiert werden (namentlich durch das Auftragsrecht). Demgegenüber unterscheiden sich die unterschiedlichen Staking-Modelle, unabhängig davon, ob sie in Form eines Custodial oder Non-Custodial Stakings ausgestaltet sind, nicht in Bezug auf die *der Technologie inhärenten* Risiken. Namentlich sind protokollbedingte Slashing-Risiken und Lock-Ups, soweit sie von einer Blockchain vorgesehen sind, in allen Staking-Modellen gleichermassen relevant. Der Kunde eines Custodial Staking-Providers ist mit anderen Worten denselben Technologierisiken ausgesetzt wie der Self-Staker, der ohne Hilfe einer Drittperson mit der Blockchain interagiert. Vor diesem Hintergrund scheinen die Interessen wenig erfahrener Staker bei Inanspruchnahme der Dienstleistungen von etablierten Staking-Providern in der Schweiz regelmässig besser geschützt als bei Modellen des Non-Custodial Stakings.

5. Bankenrecht

5.1 Einleitung

Gemäss Art. 1 Abs. 2 BankG ist die gewerbsmässige Entgegennahme von *Publikumseinlagen* Banken vorbehalten, ausser es liegt ein Ausnahmetatbestand gemäss Art. 5 Abs. 2 und Abs. 3 BankV vor. Ferner kann es trotz Vorliegens von Publikumseinlagen an der Gewerbsmässigkeit

[22] Einer der längsten Lock-Ups ist mit rund 28 Tagen derjenige der Polkadot Blockchain.

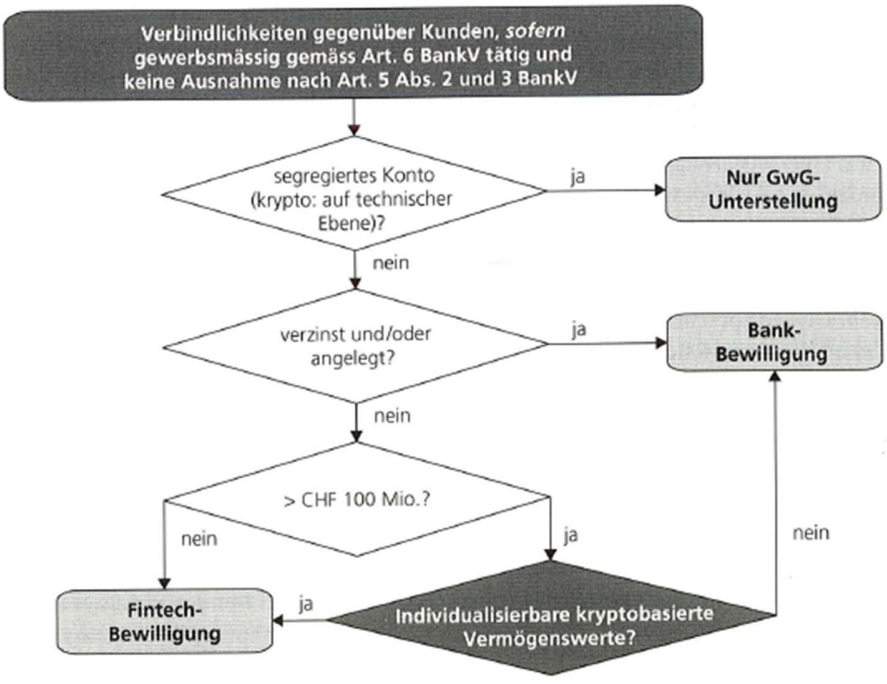
der Tätigkeit fehlen, wenn eine Person etwa die Bedingungen der *Sandbox* erfüllt (vgl. Art. 6 BankV).

Es handelt sich nach ständiger Rechtsprechung des Bundesgerichts um eine Publikumseinlage, wenn eine Person Verpflichtungen gegenüber Dritten eingeht und dadurch zur Rückzahlungsschuldnerin der entsprechenden Leistung wird.[23]

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 Fintech-Unternehmen. In diesem Fall handelt es sich zwar 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, aufsichtsrechtlich einem ähnlichen Regime wie Publikumseinlagen unterstellt.

Grafik 3: Überblick Bewilligungen beim Krypto-Verwahrungsgeschäft



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

[23] 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.

Entgegennahme und Aufbewahrung von kryptobasierten Vermögenswerten, die in Einzelverwahrung gehalten werden, sind demgegenüber bewilligungsfrei möglich. In diesem Fall hat der Aufbewahrer die Kundenvermögen auf der Blockchain sowohl von den Beständen anderer Kunden als auch von seinen Eigenbeständen zu trennen.

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 Publikumseinlagen 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 Tätigkeit der Bank mit den entgegengenommenen Kundengeldern mit Eigenmitteln zu unterlegen (siehe hierzu auch Ziff. 5.4).

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. 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 «Pooled»-Lösung am Staking teilnehmen. Vorbehaltlich der Anwendbarkeit bankrechtlicher Ausnahmen ist für das Staking aus der *Sammelverwahrung* heraus 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 Verwahrerin. Auch im Rahmen eines Slashing erlangt in der Regel keine Drittperson die Verfügungsmacht über die gestakten Token.[24] 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 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*.

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

5.3 Absonderung im Konkurs

Art. 16 Ziff. 1bis BankG stellt gemäss Botschaft die «gespiegelte» Bestimmung zu Art. 242a SchKG für bankrechtliche Depotwerte dar.[25] Aufgrund der Regelung in Art. 37d BankG sind kryptobasierte Vermögenswerte nach Art. 16 BankG im Konkurs einer Bank *absonderbar*. Es kann hinsichtlich der Anforderungen an die Absonderbarkeit von gestakten Token auf die Ausführungen zum Konkursrecht verwiesen werden (siehe oben Ziff. 4.2).

Soweit Banken das Sub-Custodial Staking-Geschäft betreiben und darum selbst keinen Zugriff auf die Private Keys haben, die vom Sub-Custodian verwahrt werden, ist im Konkurs der Bank gestützt auf Art. 16 Ziff. 1bis i.V.m. Art. 37d BankG eine Absonderung zugunsten der Bankkunden allenfalls nicht möglich. Jedoch kommt Art. 16 Ziff. 2 BankG in diesem Fall ungeachtet des eng umschriebenen gesetzlichen Wortlauts zur Anwendung, mit der Folge, dass Kunden solcher Banken die von letzteren fiduziarisch begründeten und gehaltenen kryptobasierten Vermögenswerte gegenüber dem Sub-Custodian herausverlangen können, weshalb auch in diesem Fall im Konkurs der Bank absonderbare Depotwerte vorliegen. Alternativ kann in Sub-Custody-Verhältnissen eine Aussonderung gestützt auf Art. 401 Abs. 1 i.V.m. Abs. 2 OR infrage kommen.

5.4 Fazit

Die Absonderbarkeit gestakter Token in Einklang mit den Anforderungen von Art. 16 BankG ist sachgerecht und im Interesse der Bankkunden. Dass die Vermögenswerte trotz Staking weiterhin dem Kunden «gehören» sollen, entspricht in aller Regel dem Willen der Parteien. Die Bank darf nach Auffassung der Parteien gerade nicht frei über die gestakten kryptobasierten Vermögenswerte verfügen. Damit sollte Staking nicht nur Banken, sondern auch Personen nach Art. 1b BankG offenstehen.

Eine abweichende Auffassung, die zum Schluss kommt, dass gestakte Token aufgrund eines Lock-Ups oder Slashing-Risikos nicht als Depotwerte, sondern als Publikumseinlagen qualifizieren, könnte mit erheblichen Konsequenzen für den Finanzplatz Schweiz verbunden sein: Banken müssten in diesem Fall die den Kunden zurechenbaren Staking-Positionen auf die Bilanz nehmen und mit *Eigenmitteln* unterlegen. Aufgrund der einschneidenden Eigenmittelvorschriften des Basler Ausschusses für Aktivitäten mit «Crypto Assets» könnte dies zu prohibitiven Kosten für Schweizer Banken führen, sodass sie allenfalls das Staking-Geschäft aufzugeben hätten.

Ferner wäre diese Auffassung auch nicht im Interesse der stakenden Kunden einer Bank: Auf Krypto lautende Publikumseinlagen wären aufgrund der ausdrücklichen Regelung in Art. 42a Abs. 1 lit. a Ziff. 1 BankV im Konkurs der Verwahrerin weder privilegiert noch würden sie von der Einlagensicherung profitieren.

Wie bereits im Kontext des Konkursrechts ausgeführt (siehe Ziff. 4.3), sollte auch das Aufsichtsrecht nicht die *technologiespezifischen Risiken*, wie namentlich Lock-Ups und Slashing-Risiken, sondern die *mit der Dienstleistung zusammenhängenden Risiken* in den Regulierungsfokus stellen. Eine generelle und nicht auf den Einzelfall bezogene Statuierung, dass Lock-ups und Slashing-Risiken einer Aussonderung immer entgegenstehen, wäre mit der stark proklamierten

[25] So ausdrücklich BBl 2020, S. 301.

Technologieneutralität der DLT-Revision nicht vereinbar und würde im Ergebnis zu einer Ungleichbehandlung der Risiken beim Self-Staking und beim Staking durch einen Drittanbieter führen (*same risks, same rules*). Unter diesen Umständen scheint das zivilrechtliche Haftungs- und das (bank)konkursrechtliche Aus- bzw. Absonderungsregime genügend Handhabe zu bieten, um den Schutz stakender Kunden von Dienstleistern in der Schweiz effektiv zu gewährleisten.

Denkbar ist hingegen, dass die FINMA die Anforderungen unter dem Titel «Digital Asset Recovery Package» (DARP) auf die Verwahrung gestakter Token durch Banken und ggf. auch Staking-Provider ausweitet.[26] Darin würden idealerweise v.a. die mit dem Staking verbundenen operationellen Risiken abgebildet und mit adäquaten Massnahmen adressiert werden, sodass der Konkursliquidator im Konkursfall einen transparenten Überblick über die für Kunden gestakten Token hätte.

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. des KAG vor, sondern lediglich die technisch notwendige Zusammenführung von kryptobasierten Vermögenswerten zum Zweck des Stakings. Jede Kundin des Staking-Providers 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).

[26] Betreffend DARP siehe Ronald Kogens/Patrick Niklaus, Digital Asset Resolution Package (DARP), 12. Juli 2023, https://www.mme.ch/de-ch/magazin/artikel/digital-asset-resolution-package-darp, zuletzt besucht am 14. August 2023.

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-Provider 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.[27]

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. 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

[27] Siehe auch Thomas Jutzi/Andri Abbühl, Fintech und DLT. Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023, Rz. 606, die Staking als ein untrennbares «Feature» von PoS-Token betrachten und somit eine Anlagetätigkeit verneinen; im Ergebnis gleich Reto Luthiger, Staking von Kryptowährungen aus regulatorischer Sicht, EIZ-Seminar zum Blockchain-Recht, 10. März 2022, S. 18.

Finanzinstrumente zum Gegenstand haben. In diesem Fall werden Aufträge des Kunden im Hinblick auf den Geschäfts- und Transaktionsabschluss angenommen und üblicherweise an Dritte übermittelt.[28] Beim Ausführen eines Staking-Auftrags des Kunden, der in die Blockierung der kryptobasierten Vermögenswerte im PoS-Protokoll resultiert, kommt demgegenüber kein solcher Abschluss zustande.

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 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).

[28] 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.

9.2 Unterstellung und GwG-Pflichten

Unabhängig von der Notwendigkeit einer Bewilligung als Bank oder Person nach Art. 1b BankG sind Staking-Provider 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-Provider über eine vergleichbar gesteigerte Form der Kontrolle der Vermögenswerte des stakenden Kunden verfügt.[29] 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. 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 resp. 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-Provider 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-Provider an die Kunden weitergeleitet. Da es sich bei Staking Rewards um

[29] Siehe EFD, Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Erläuterungen, 18.06.2021, S. 11, 22.

ein Entgelt für Validierungsleistungen handelt, liegt in der Regel ebenfalls keine Zahlungsfunktion vor.

10. Steuerrecht

Überlegungen zu steuerrechtlichen Aspekten von Staking zu einem späteren Zeitpunkt bleiben vorbehalten.

11. Fazit

Zivilrechtlich schulden Staking-Provider ihren Kunden ein sorgfältiges Tätigwerden gemäss Auftragsrecht (Art. 398 OR); es können Pflichten aus Werkvertrag oder Hinterlegungsvertrag hinzutreten.

Konkursrechtlich ist Art. 242a SchKG so auszulegen, dass vom Gesetzgeber keine ständige technische Übertragbarkeit der kryptobasierten Vermögenswerte verlangt wird. Vielmehr muss es genügen, dass eine vertragliche Verpflichtung besteht, die Verfügungsmacht über die Token aufrechtzuerhalten und einen ständigen Zugriff auf die Private Keys zu gewährleisten. Die Aussonderbarkeit der gestakten Token ist damit gegeben.

Finanzmarktrechtlich steht die Anwendung des Bankengesetzes im Vordergrund. Angesichts der ähnlichen Formulierungen zur Aussonderbarkeit von kryptobasierten Vermögenswerten im SchKG und im BankG ist von der Möglichkeit der Absonderung kryptobasierter Vermögenswerte auszugehen, weshalb gute Gründe dafür sprechen, solche Vermögenswerte nicht als Publikumseinlagen, sondern als (absonderbare) Depotwerte zu qualifizieren. Dass die Vermögenswerte trotz Staking weiterhin dem Kunden «gehören» sollen, entspricht dem Willen der Parteien, denn die Bank darf gerade nicht frei über die gestakten kryptobasierten Vermögenswerte verfügen; dasselbe gilt für Personen nach Art. 1b BankG.