COMPLIANCE IN DER KRYPTOWELT?

Sabine Kilgus / Caroline Walser Kessel

Prof. Dr. Sabine Kilgus, LL.M., Rechtsanwältin, Titularprofessorin an der Universität St. Gallen; Präsidentin der Selbstregulierungsorganisation zur Bekämpfung der Geldwäscherei (SRO) von TREUHAND|SUISSE
Dufourstrasse 181, 8008 Zürich, Schweiz
sabine.kilgus@lwdlaw.ch; sabine.kilgus@unisg.ch; www.lwdlaw.ch

Dr. iur. Caroline Walser Kessel, Rechtsanwältin und Lehrbeauftragte an der Law School der Universität St. Gallen, Schweiz
Giblenstraße 3, 8049 Zürich, Schweiz
caroline.walser@vtxmail.ch; http://www.walserlaw.ch; http://www.visuellesrecht.ch

Schlagworte: ***Blockchain, Kryptowährung, Kryptoassets, Geldwäschereibekämpfung, Terrorismusfinanzierung, beneficial owner***

Abstract: *Die Schweiz fördert sog. FinTech-Unternehmen und ermöglicht eine Speziallizenz unter dem Bankengesetz, selbst wenn Kundengelder bis CHF 100 Mio. angenommen werden, sofern diese nicht angelegt und nicht verzinst werden. Darunter fallen alle möglichen Anbieter von Kryptowährungen, Blockchainprovider, Wallet-Provider, Miner etc. Im Hinblick auf die Geldwäschereibekämpfung stellen sich FINMA und KGGT auf den Standpunkt, dass die Kryptogeschäftsmodelle mit denjenigen der realen Welt verglichen und die Geldwäschereibekämpfung v.a. an der Schnittstelle Krypto-Asset zu FIAT-Geld angesetzt werden soll. Soweit FinTech Unternehmen überhaupt unter das GwG fallen, müssen sie die zentralen Grundsätze der Geldwäschereibekämpfung einhalten: «know your customer», aber auch «know the beneficial owner». Ob und wie das erfolgen kann, ist noch weitgehend offen und technologieabhängig. Nachvollziehbar ist das für Zahlungstoken; Unsicherheiten bestehen aber für Anlagetoken und erst recht für das Sammelbecken der Utilitytoken.*

1. Ausgangslage

1.1. Geldwäschereibekämpfung in der Schweiz

Die Geldwäschereibekämpfung in der Schweiz folgt den internationalen Vorgaben der Groupe d'action financière (GAFI)[1,2]. Im nationalen Recht werden diese Vorgaben einerseits repressiv im Strafrecht[3], andererseits präventiv im Aufsichtsrecht[4] umgesetzt. Die letzte materielle Revision des GwG trat auf den 1. Januar 2016 in Kraft[5] und setzte die revidierten GAFI Empfehlungen von 2012 um[6]. So macht sich strafbar, *wer eine Handlung vornimmt, die geeignet ist, die Ermittlung der Herkunft, die Auffindung oder die Einziehung von Vermögenswerten zu vereiteln, die wie er weiss oder annehmen muss aus einem Verbrechen oder einem qualifizierten Steuerdelikt stammen* (Art. 305bis Abs. 1 und Abs. 1bisStGB). Aus der Formulierung der Strafbestimmung wird

1 http://www.fatf-gafi.org/.

2 Sämtliche Internetzitate wurden zuletzt am 7. Januar 2019 besucht, auf eine individuelle Nennung wird verzichtet.

3 Art. 305bis StGB (Geldwäscherei), Art. 305ter StGB (mangelnde Sorgfalt bei Finanzgeschäften), Art. 260ter StGB (Zugehörigkeit zu einer kriminellen Organisation) und Art. 260^{quinquies} StGB (Terrorismusfinanzierung), SR 311.0.

4 Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (GwG), SR 955.0.

5 Neu sind bspw. die Erfassung schwerer Steuervergehen als Vortat zur Geldwäscherei und die Feststellung der wirtschaftlich Berechtigten von nicht börsenkotierten operativen Unternehmen.

6 Die GAFI evaluierte darauf die Umsetzung in der Schweiz im Jahre 2016. Der Bericht ist unter http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html abrufbar. Auch wenn die Schweiz gestützt auf die Ergebnisse des Berichts erneut Anpassungen im GwG vornehmen muss (bspw. Nachidentifikation des wirtschaftlich Berechtigten), werden die nachfolgend erläuterten FinTech Entwicklungen in der laufenden Revision nicht explizit angesprochen.

ersichtlich, dass es sich um ein Gemeindelikt handelt. Alle Leute, d.h., nicht nur Finanzintermediäre, können sich der Geldwäscherei (und der Terrorismusfinanzierung) als Täter, aber auch als Anstifter, Mittäter oder Gehilfen strafbar machen. Das trifft folglich auf alle Nutzer, aber auch auf alle FinTech Unternehmen zu, die nicht als Finanzintermediär qualifiziert werden.

Die aufsichtsrechtlichen Präventivmassnahmen sind komplementär zu den strafrechtlichen Bestimmungen und verlangen von den *Finanzintermediären*[7] zusätzlich, dass der Vertragspartner und der/die hinter dem Vertragspartner stehenden wirtschaftlich Berechtigten[8] an den Vermögenswerten oder an Gesellschaften und juristischen Personen (Art. 3 und 4 GwG) mit der nötigen Sorgfalt identifiziert und festgehalten werden[9]. Das Ziel ist grösstmögliche *Transparenz*, und zwar bezüglich der Struktur von Gesellschaften, Trusts oder auch wirtschaftlichen Verflechtungen von Gesellschaften einerseits und der Transaktionen, Zahlungsströme andererseits. Es soll verhindert werden, dass Vertragsbeziehungen bzw. die hinter dem Vertragspartner allenfalls stehenden Personen und Gesellschaften, die wirtschaftlich Berechtigten, anonym bleiben können. Ebenso soll Klarheit über Zahlungsströme herrschen. Das gilt einerseits für alle Formen von Überweisungen, bei denen Absender und Empfänger bekannt sein müssen, andererseits aber auch für Bargeldtransaktionen und Zahlungen innerhalb von Zahlungssystemen (Debit- und Kreditkarten, Warenkarten, Paypal, Western Union etc.). Sodann müssen bei Kassageschäften über CHF 25'000 und bei bar abgewickelten Handelsgeschäften über CHF 100'000 der Vertragspartner und der wirtschaftlich Berechtigte festgehalten werden (Art. 3 Abs. 2 GwG, Art. 8a Abs. 1 GwG, Art. 51 Abs. 1 lit. b GwV-FINMA). Traditionellerweise erfolgen diese Identifikationspflichten durch Ausweiskopien, Registerauszüge etc., mithin durch eine *Dokumentation* über den Kunden und die Geschäftsbeziehung, die vom Finanzintermediär geführt und aktualisiert werden muss (Art. 7 GwG)[10].

Das Mass der anzuwendenden Sorgfalt richtet sich nach dem *Risiko* der Vertragsbeziehung bzw. Transaktion für Geldwäscherei oder Terrorismusfinanzierung, was im Bereich der neuen Technologien wohl generell als hoch einzustufen ist. D.h. die Abklärungen haben vertiefter zu erfolgen und sind streng zu überwachen – was dazu führt, dass ungewöhnliche Transaktionen ungeachtet der Schwellenwerte zu Identifikationspflichten führen.

1.2. Förderung von FinTech

Im Oktober 2016 veröffentlichte der Bundesrat einen Bericht zur Finanzplatzpolitik und hielt fest, dass er den neuen Geschäftsmodellen im Bereich der Digitalisierung im Finanzmarkt *technologieneutral* gegenübersteht und Innovationen in diesem Bereich fördern will.

Auf den 1. August 2017 ist dann folgerichtig eine Revision der Verordnung zum Bankengesetz (BankV)[11] in Kraft getreten, die v.a. für crowdfunding Plattformen Erleichterungen vorsah (sog. Sandbox-Bestimmung in Art. 6 Abs. 2 BankV). Demnach fallen Plattformen (oder Unternehmen, die Publikumseinlagen von bis zu CHF 1 Mio. entgegennehmen) nicht unter das Bankengesetz, wenn sie diese innert 60 Tagen wieder veräussern bzw. den Projektbetreibern zukommen lassen und die Gelder nicht verzinsen, wohl aber allenfalls unter das GwG.

---

7 Art. 2 Abs. 2 und 3 GwG.

8 Der Einfachheit halber wird die männliche Form verwendet. Weibliche Personen sind selbstverständlich miterfasst.

9 Neben Finanzintermediären müssen auch Händler, die Bartransaktionen von über CHF 100'000 abwickeln, die Sorgfaltspflichten gemäss GwG einhalten.

10 Im Frühling 2016 ermöglichte die FINMA die Video- und Online-Identifizierung von Kunden und wirtschaftlich Berechtigten. Vgl. FINMA RS 2016/7 (https://www.finma.ch/de/dokumentation/rundschreiben/ bzw. direkt unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2016-07—20180801.pdf?la=de).

11 Verordnung vom 30. April 2014 über die Banken und Sparkassen (Bankenverordnung, BankV; SR 952.02).

Da in den Jahren 2017 und 2018 insbes. in den Kantonen Zug[12] und Tessin[13] gezielt Standortförderung zur Ansiedelung von FinTech-Unternehmen erfolgte, sah sich die FINMA gezwungen, eine rechtliche Einordnung dieser Geschäftsmodelle im Rahmen der geltenden Aufsichtsgesetze vorzunehmen. Sie tat dies 2017 mit der Veröffentlichung eines Arbeitspapieres zum Thema Crowdfinancing[14] und im Februar 2018 mit einer Analyse der rechtlichen Einordnung der verschiedenen Arten von Token[15]. Dabei stand v.a. zur Diskussion, ob und wie die Emission von (Anlage)-Token Effekten sind und damit unter das Finanzmarktinfrastrukturgesetz[16] fallen und ob und wie Zahlungstoken bzw. ihre Anbieter von der Geldwäschereigesetzgebung erfasst werden. Auf Bundesebene wurde im Januar 2018 eine Arbeitsgruppe eingesetzt, die die Chancen und Risiken der neuen Technologien und FinTech-Unternehmen analysieren soll.

Auf den 1. Januar 2019 ist schliesslich mit dem neuen Art. 1b BankG eine weitere Änderung des Bankengesetzes[17] in Kraft getreten. In Ergänzung zur Sandbox von Art. 6 BankV, die eine Ausnahme von der Unterstellung für kleine FinTech-Unternehmen ermöglicht, wurde nun eine neue Kategorie von Finanzintermediären, nämlich FinTech-Unternehmen, geschaffen, die explizit keine Banken sind, sondern eine eigene Bewilligung erhalten, aber dennoch zumindest teilweise und insbes. bezüglich der Geldwäschereibekämpfung der Finanzmarktregulierung unterstehen. Die Bestimmung trägt das Marginale «Innovationsförderung» und sieht gegenüber Banken eine Reihe von Erleichterungen vor (weniger Kapital, einfachere Rechnungslegung und Revision). Sie dürfen Publikumseinlagen bis CHF 100 Mio. entgegennehmen, müssen die Einleger aber explizit darauf hinweisen, dass die Gelder nicht dem Einlegerschutz unterliegen. Sie müssen ihren Geschäftskreis präzise umschreiben und über ein Risikomanagement sowie über Compliance verfügen.

2. FinTech und Geldwäschereibekämpfung: Neue Technologien – neue Risiken

2.1. FinTech ist nicht gleich FinTech

Bereits die Arbeitsgruppe des Bundesrates erkannte, dass unter FinTech verschiedene Geschäftsmodelle zusammengefasst werden. Die oben erwähnte Wegleitung der FINMA vom Februar 2018 brachte dann eine vorläufige Klärung bezüglich der aufsichtsrechtlichen Erfassung von Initial Coin Offerings (ICO's) und der Differenzierung bezüglich der emittierten Token. Die FINMA hielt an ihrer Technologieneutralität fest und gliedert die verschiedenen Token und damit letztlich indirekt die Emittenten, Provider und Verwahrer solcher Token, in bestehende Rechtsgebiete bzw. Finanzmarktgesetze ein. Sie unterteilt dabei die emittierten Token in *Anlagetoken*, bei denen die Nähe zu Effekten und damit zur Börsengesetzgebung gegeben ist[18], *Zahlungs-*

---

[12] Es wird für den Kanton Zug auch von Cyber Valley gesprochen. Bemerkenswert ist, dass die öffentliche Verwaltung und auch das Handelsregister des Kantons Zug die Bezahlung von Gebühren mit Bitcoin oder Ether erlaubt. Vgl. den Newsletter 2018/1 des Handelsregisters des Kantons Zug über die (Sach-)Liberierung von Aktien mittels Kryptowährungen, https://www.zg.ch/behoerden/volkswirtschaftsdirektion/handelsregisteramt/newsletter. Entsprechend hat die Steuerverwaltung ein Merkblatt zur Besteuerung von Kryptowährungen (Anlage- und Zahlungstoken) herausgegeben. https://www.zg.ch/behoerden/finanzdirektion/steuerverwaltung/kryptowaehrungen.

[13] Der ressourcenarme Kanton Tessin versucht durch die Ansiedelung von High Tech-Unternehmen im südlichen Kantonsteil gezielt italienisches Know-how anzuziehen, um die Verluste, die dem Finanzplatz durch den automatischen Informationsaustausch in Steuersachen entgehen, wieder wett zu machen. Peter Jankovsky, Das Tessin setzt auf FinTech, NZZ vom 28. Dezember 2018, S. 14.

[14] Art. 6 Abs. 2 BankV beendete in der Folge einen Teil der Rechtsunsicherheit. Vgl. auch das Faktenblatt FINMA vom 1. August 2017.

[15] https://www.finma.ch/de/news/2018/02/20180216-mm-ico-wegleitung/.

[16] Bundesgesetz vom 19. Juni 2015 über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz, FinfraG; SR 958.1).

[17] Sowie der Bankenverordnung und des GwG.

[18] Es bildet sich das Verständnis, wonach, Anlagetoken als Wertrecht oder Bucheffekte i.S.d. Finanzmarktinfrastrukturgesetzes (FinfraG, SR 958.1) und des Bucheffektengesetzes (BEG, SR 957.1) (und inskünftig des Finanzdienstleistungsgesetzes [FIDLEG, vermutlich in Kraft per 1. Januar 2020, SR 950.1]), nicht aber als Währung i.S. des Währungsgesetzes (WZG, SR 941.10) qualifiziert werden können. Damit sind die Emittenten zwingend Effektenhändler und der Finanzmarktregulierung unterstellt. Vgl. Bericht des Bundesrates (s. Fn. 20), S. 88–138; KGGT, Risiko (s. Fn. 21), S. 12 f.

token, die als eine Weiterentwicklung von new payment methods (Paypal, moneygram etc.) gesehen werden und die damit unter dem Aspekt der Geldwäschereibekämpfung vertieft analysiert werden müssen sowie die *Utility*- oder *Nutzungstoken*, die als Sammelbecken entweder Hybridformen der vorgenannten darstellen oder aber zu Dienstleistungs- und Warenbezügen innerhalb der emittierenden Systeme berechtigen.

Aus der Optik der Geldwäschereibekämpfung genauer zu betrachten sind die Zahlungstoken bzw. alle Anbieter und Verwalter solcher virtueller Währungen[19]. Das gilt für die bekannten «Währungen» wie Bitcoin oder Ether selbst, die über eine Blockchain übertragen werden, aber auch für andere Handelsformen solcher Token auf zentralen und dezentralen Plattformen. Zu klären ist als erstes, welche Anbieter unter welche Finanzmarktgesetze und insbes. unter das GwG zu *unterstellen* sind. Bei einer Unterstellung ist in einem zweiten Schritt zu analysieren, wie in einer durch kryptographische Protokolle geprägten Kundenbeziehung die bekannten Sorgfaltspflichten der Geldwäschereiprävention eingehalten werden können. Die bis anhin erfolgten Analysen zeigen alle, dass keine einheitliche Qualifikation vorgenommen werden kann, sondern die verschiedenen Geschäftsmodelle individuell analysiert werden müssen.

2.2. National Risk Assessment (NRA)

Bereits im Hinblick auf die Umsetzung der GAFI-Empfehlungen 2012 hat der Bund eine interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT) ins Leben gerufen, welche die Risiken, denen die Schweiz diesbezüglich ausgesetzt ist, sektorübergreifend evaluiert und entsprechende Massnahmen vorschlägt. Die KGGT hat im Oktober 2018 einen Bericht zum «Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding» erarbeitet, der zusammen mit dem Bericht des Bundesrates vom 7. Dezember 2018 über «Rechtliche Grundlagen für *Distributed-Ledger*-Technologie und Blockchain in der Schweiz» am 14. Dezember 2018 publiziert wurde[20]. Am 18. Dezember 2018 erfolgte noch der parallele Risikobericht der KGGT «über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Terrorismusfinanzierung in der Schweiz»[21,22].

Der KGGT Bericht zum Geldwäschereirisiko durch Krypto-Assets[23] lehnt sich an die Wegleitung der FINMA vom Februar 2018 an, vertieft aber deren Aussagen und geht insbes. detailliert auf die verschiedenen möglichen Geschäftsmodelle im Zusammenhang mit Krypto-Assets fallgruppenweise ein. Obwohl der Bericht festhält, dass sich bis zum Publikationsdatum in der Schweiz keine signifikanten Geldwäschereifälle im Zusammenhang mit Krypto-Assets ereignet hätten, kommt er zum Schluss, dass sich im Bereich von Krypto-Assets ganz generell verschiedene erhebliche Risiken für Geldwäscherei und Terrorismusfinanzierung ergeben, die sich schwerpunktmässig wie folgt gruppieren lassen:

– Das Risiko für Geldwäscherei und Terrorismusfinanzierung ergibt sich zunächst – ähnlich wie bei Bargeldtransaktionen – aus der *Anonymität* des Inhabers der Token bzw. der virtuellen Währungen[24] und damit des Vertragspartners (Kunden) und erst recht des wirtschaftlich Berechtigten. Zusätzlich zeichnen

---

19 So Wegleitung FINMA, S. 6 f.; Ebenso differenziert Gabriela Hauser-Spühler, Innovation vs. Regulation, Compliance im Digital-Finance-Bereich, Law & Management Praxis, 2017/6, S. 1 ff., insbes. Rz. 18, Rz. 40 ff. Ihr Aufsatz ist aber vor dem Bericht der KGGT entstanden, der einige ihrer Anliegen betr. risikobasiertem Compliance-Konzept aufnimmt.

20 Bericht des Bundesrats https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-73398.html.

21 Bericht der KGGT https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-73465.html.

22 Diese beiden Berichte der KGGT (Fn. 21) und der Bericht des Bundesrates (Fn. 20) über die rechtliche Einordnung der DLT-Technologie ins Schweizer Recht enthalten je eine umfassende und aktuelle Literaturliste, Stand Dezember 2018. Nachfolgend wird deshalb aus Gründen der Aktualität und des beschränkten Umfangs dieses Artikels weitgehend auf diese Berichte abgestellt.

23 Krypto-Assets wird dabei als Oberbegriff für alle digitalen oder virtuellen Produkte/Tokens/Währungen verwendet. Vgl. KGGT Risiko (Fn. 21), S. 8.

24 Diese Anonymität ist bei Transaktionen im sog. Darknet noch erhöht, da mit Hilfe von geeigneter Software, z.B. Tor, noch eine zusätzliche Stufe der Anonymität erreicht werden kann.

sich diese Transaktionen durch eine erhöhte *Mobilität*[25], d.h. sehr oft internationale Sachverhalte, und eine erhöhte *Geschwindigkeit* in der Execution (smart contracts) aus.

– Sodann lässt sich mit Hilfe der Technik, d.h. von sog. Mixern, die Anonymität der Transaktionen erhöhen, indem die in Auftrag gegebene Transaktion quasi «gehäxelt» und damit verkleinert wird, so dass sich der Datentransfer nur sehr aufwendig oder fast gar nicht mehr zurückverfolgen lässt. Dieses Vorgehen erinnert an smurfing, ein geldwäschereitypisches Muster, das eine grosse Überweisung in mehrere kleine unterteilt, die knapp unter dem Schwellenwert liegen, damit den Identifikationspflichten nicht nachgekommen werden muss[26].
– Die Instrumente der neuen Technologien eignen sich wie alle Finanztransaktionen auch für kriminelle Handlungen. So zeigt sich, dass die Emission von (Anlage)-Token betrügerisch, bspw. als Schneeballsystem erfolgen kann. Damit erfüllt die Emission des Tokens gleichzeitig die Vortat und den Tatbestand der Geldwäscherei. Erfolgt die Anlage in virtuelle, nicht identifizierbare Unternehmen, lässt sich auch Terrorismusfinanzierung nicht ausschliessen.
– Schliesslich kann die organisierte Kriminalität ganz innerhalb des Darknet operieren, wo sie für die reale Welt fast nicht eruiert werden kann[27]. Das betrifft v.a. die schweren Verbrechen, wie Drogen-, Waffen- oder Menschenhandel, aber auch die Terrorismusfinanzierung.

3. Reaktion der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung: Unterstellung von Anbietern und Vertreibern von Krypto-Assets unter das GwG

Wie erläutert haben die FINMA und die KGGT einen *funktionalen* Ansatz gewählt und analysiert, welche Tätigkeiten bzw. welche Geschäftsmodelle zu einer bewilligungspflichtigen Finanzintermediation gemäss den Finanzmarktgesetzen und damit zu einer Unterstellung der entsprechenden Anbieter führen[28] (Art. 2 Abs. 2 GwG)[29]. Entfällt dies, ist zu prüfen, ob sie als «*übrige Finanzintermediäre*» i.S.v. Art. 2 Abs. 3 GwG, qualifiziert werden müssen, nämlich als solche, die *berufsmässig fremde Vermögenswerte annehmen, aufbewahren oder helfen, sie anzulegen oder zu übertragen*[30]. Finanzintermediäre nach Art. 2 Abs. 2 und Abs. 3 GwG haben die Sorgfalts-, Dokumentations- und Meldepflichten gemäss Art. 3–9 GwG einzuhalten.

3.1. Blockchain-Technologie

Bei der *Blockchain* Technologie[31] werden mittels Krypto-Assets Transaktionen dezentral ausgeführt. Eine Validierung bzw. Nachprüfung, ob die Aufträge ordnungsgemäss erfolgen, erfolgt durch die Mehrheit der angeschlossenen Personen, dezentral und grundsätzlich öffentlich mittels der Lösung mathematischer Aufgaben. In ihrer ursprünglichen Form werden sämtliche Transaktionen für alle Teilnehmer einsehbar aneinandergereiht,

---

25 Damit wird sowohl eine aufsichtsrechtliche als auch eine strafrechtliche Anknüpfung schwierig.

26 Z.Z. CHF 5'000 für Geldwechsel und CHF 3'000 für money transmitting, Art. 12 Abs. 2 lit. c und d GwV-FINMA.

27 Vgl. dazu auch ausführlich Gabriela Hauser-Spühler (Fn. 19), Rz. 79 ff. m.H. auf die Guidance der GAFI.

28 Vgl. den Bericht des Bundesrates (Fn. 20), S. 87–138, der für alle Player minutiös analysiert, unter welchen Umständen sie unter welche Finanzmarktgesetze (Bankengesetz [BankG], Finanzmarktinfrastrukturgesetz [FinfraG], Kollektivanlagegesetz [KAG], Versicherungsaufsichtsgesetz [VAG], sowie das erst auf den 1. Januar 2020 in Kraft tretende Finanzinstitutsgesetz [FINIG] und Finanzdienstleistungsgesetz [FIDLEG]) fallen könnten.

29 Die spezialgesetzlichen Finanzintermediäre wie Banken, Versicherungsgesellschaften, FinTech-Unternehmen nach Art. 1b BankG, Effektenhändler, Asset Manager von kollektiven Kapitalanlagen, Fondsleitungen und Investmentgesellschaften, Finanzmarktinfrastrukturen (Handelssysteme und Zahlungssysteme), Casinos müssen die Bestimmungen zur Geldwäschereibekämpfung ohnehin einhalten (Art. 2 Abs. 2 GwG).

30 Es versteht sich von selbst, dass zusätzlich geklärt werden muss, ob überhaupt eine Anknüpfung zur Schweiz in sachlicher und örtlicher Hinsicht besteht.

31 Der KGGT, Risiko (Fn. 21), S. 7, definiert die Blockchain als «Computertechnologie zur Speicherung und Übertragung von Daten ohne zentrale Kontrollstelle», die zumeist eine Transaktionsgeschichte aller getätigten Transaktionen enthält. Da es heute mehrere Formen von Blockchains gibt, wird als übergeordneter Begriff von *Distributed Ledger Technologie (DLT)* gesprochen. So Bericht des Bundesrats (Fn. 20), S. 7.

so dass sich – wenn auch mit grossem Aufwand – die Historie der Transaktionen nachweisen lässt. Die Teilnehmer identifizieren sich durch die Verwendung zweier Schlüssel in ihrem Wallet[32], dem public key, der von der Blockchain ausgegeben wird und dem individuellen private key, der nur für den Berechtigten zugänglich ist. Sie bleiben für die Anderen aber anonym. Die Blockchain selber ist nur die Übertragungstechnologie und wird dadurch nicht zum Finanzintermediär. Indessen gewährleistet sie die Anonymität, die jeder Geldwäschereibekämpfung zuwiderläuft. Sie gewährleistet zwar die Nachvollziehbarkeit der Transaktionen auf technischem Weg, nicht aber einen eigentlichen paper trail. Sie ermöglicht aber auch das (permanente) Abtauchen in eine parallele Welt, bspw. ins Darknet, und lässt so ganze Parallelwelten von Liefer- und Zahlungssystemen (bspw. einen illegalen Kreislauf von Drogen-, Waffen-, Menschenhandel und Terrorismusfinanzierung) gedeihen.

3.2. Wallets

Aus der Optik der Geldwäschereibekämpfung kritisch bzw. sensitiv sind die Vorgänge des *Wechsels* bzw. der Umwandlung von echtem Geld, sog. FIAT Geld, in virtuelles Geld bzw. Zahlungstoken und *vice versa*. An diesen Schnittstellen können oder könnten die Anbieter dieser Technologien (App Provider, Wallet Anbieter, Custodians) gewisse Abklärungen/Identifikationspflichten wahrnehmen. Je nach Ausgestaltung der Vertragsbeziehungen können sie als Wechselstube i.S.d. GwG (Zwei-Parteien-Verhältnis) oder aber als Money Transmitter (Drei-Parteien-Verhältnis) qualifiziert werden[33]. In beiden Fällen sind sie dem GwG unterstellt, *da sie über fremde Vermögenswerte verfügen*[34]. Das setzt aber voraus, dass sie als sog. *Custodian Wallets Verfügungsmacht* über die private keys der Endnutzer, und damit Verfügungsmacht über fremdes Vermögen haben. Bei non-custodian Wallets fehlt es an dieser Befugnis, so dass sie nach heutigem Verständnis überhaupt nicht unter das GwG fallen.

3.3. Plattformen

Eine ähnliche Situation ergibt sich bei den Handelsplattformen[35]. Aus der Sicht der Geldwäschereibekämpfung kommt es wiederum darauf an, ob diese die Möglichkeit haben, *über die Vermögenswerte des Kunden zu verfügen*, was i.d.R. bei echt dezentralen Handelssystemen nicht der Fall ist, weil die User für sie anonym bleiben[36]. Nur bei zentralen Handelssystemen übernimmt die Plattform i.d.R. durch Kenntnis der User bzw. ihrer private keys, ähnlich wie Kartensysteme oder andere Zahlungsmittel, Funktionen, die einer zentralen Gegenpartei oder einem Zahlungssystem[37] ähnlich sind. Dann liegt Verfügungsmacht über fremde Vermögenswerte vor und die Handelsplattform wird zum Finanzintermediär (Art. 2 Abs. 3 GwG), allenfalls auch zu einem Handelssystem gemäss FinfraG.

3.4. Token

Wie erwähnt werden Token als Rechen- Werte- oder Nutzungseinheit verstanden Sie werden nicht selber zu Finanzintermediären, vielmehr sind es ihre Emittenten, Vertreiber, Verwahrer und Nutzer: Die Verwendung von Zahlungstoken führt für die Wallets, die sie verwahren, zumeist zu Money Transmitting, die Emission von Anlagetoken vielfach zu einer Unterstellung des Emittenten als Effekthändler unter das FinfraG.

---

32 Das Wallet wird definiert als «software, die es mittels eines Interface erlaubt, kryptographische Token zu verwalten.» So, KGGT, Risiko (Fn. 21), S. 8.

33 Auf die Einzelheiten der Schweizer Gesetzgebung und die Freigrenze für die Überweisung geringer Summen ist an dieser Stelle nicht im Detail einzugehen. Vgl. Art. 11 und 12 GwV-FINMA.

34 Money Transmitter sind dem GwG immer unterstellt, die anderen Finanzintermediäre nur, sofern sie berufsmässig i.S. v. Art. 7 GwV handeln.

35 Das gilt für Plattformen, an die (Anlage)-Token handeln, evtl. sogar emittieren, aber auch für Plattformen, die «gewöhnliches Crowdfunding» betreiben.

36 Selbstverständlich findet Art. 305bis StGB als Gemeindelikt Anwendung, wenn der Straftatbestand erfüllt ist.

37 In der Schweiz lässt sich das mit dem von der WIR Bank herausgegebenen WIR-Scheinen vergleichen.

4. Folgen der Unterstellung unter das GwG

4.1. Sorgfalts-, Dokumentations- und Meldepflichten

Das GwG bezweckt die Verhinderung der Geldwäscherei durch *Transparenz*: Es soll Klarheit herrschen bezüglich des Kunden, des gegebenenfalls hinter ihm stehenden wirtschaftlich Berechtigten am Vermögen oder an operativ tätigen Gesellschaften und juristischen Personen (Art. 3 und 4 GwG). So sollen im Falle der Bekämpfung der Geldwäscherei die Hintermänner der Transaktionen und damit vermutungsweise die Täter der Vortaten eruiert werden; im Falle der Bekämpfung von Terrorismusfinanzierung muss geklärt werden, wer an welche Personen und Organisationen Gelder überweist[38] und schliesslich will der Staat aus Gründen der Bekämpfung der Steuerhinterziehung wissen, wer hinter welchen Gesellschaften steht und welche Erträge erwirtschaftet werden. Nur so kann der von der OECD 2015 verabschiedete automatische Informationsaustausch in Steuersachen (AIA) funktionieren. Dies alles ist zu dokumentieren (Art. 7 GwG) und im Falle eines Verdachtes auf Geldwäscherei, Terrorismusfinanzierung oder qualifiziertem Steuervergehen ist dies der Meldestelle zur Bekämpfung der Geldwäscherei (MROS) zu melden (Art. 9 GwG). Es ist offensichtlich, dass viele Geschäftsmodelle im Bereich von FinTech diesen Bestrebungen diametral entgegenlaufen.

4.2. Feststellung des wirtschaftlich Berechtigten im Zeitalter von FinTech

Quasi das Herzstück in der Geldwäschereibekämpfung ist die Feststellung und Identifikation des *wirtschaftlich Berechtigten* an Vermögen, Unternehmen und Transaktionen. Dieser kann gleichzeitig der Kunde sein oder aber eine separate Person. Seit der Revision des GwG von 2016 muss er immer eine *natürliche Person* sein, eben der *ultimate beneficial owner*. Der Kunde und Vertragspartner hat den wirtschaftlich Berechtigten offenzulegen. Bei den Banken werden dafür das Formular A (wirtschaftlich Berechtigter am Vermögen) und das Formular K (wirtschaftlich Berechtigter an operativen Gesellschaften und juristischen Personen) verwendet. In der laufenden Revision des GwG ist vorgesehen, dass der Finanzintermediär nicht nur diese Informationen festhält, sondern Abklärungen betr. Identifikation des wirtschaftlich Berechtigten trifft. Es ist offensichtlich, dass alle Formen von Abklärungen über den wirtschaftlich Berechtigten nur getroffen werden können, wenn zunächst der Vertragspartner bekannt und in der Lage ist, dem Finanzintermediär entsprechende Informationen weiterzuleiten[39].

Selbst wenn das Geschäftsmodell so aufgestellt ist, dass der Nutzer und Kunde einer Blockchain-Transaktion durch die Wallet-Anbieter technologisch identifiziert werden kann, i.d.R. über seinen private key, so erfolgt dies (zunächst) nur, aber immerhin, durch eine irgendwie geartete Publikation und Dokumentation der IP Adresse oder eines anderen IT gestützten Codes. Die dahinterstehende Person als natürliche Person ist damit noch nicht identifiziert. Das gilt zunächst für den Vertragspartner, aber erst recht für einen allenfalls dahinterstehenden wirtschaftlich Berechtigten. Dieser kann auch für den Vertragspartner allenfalls nur technologisch bekannt sein.

In praktischer Hinsicht ist unklar, ob nun dieser Code oder diese IP Adresse selbst in der Lage sein kann oder sein müsste, einen wirtschaftlich Berechtigten zu nennen bzw. dessen elektronische Identität zu generieren, was bestenfalls ebenfalls zu einem Code bzw. zu einem private key führen würde. Wie daraus eine natürliche Person als ultimate beneficial owner eruiert werden kann, bleibt nach heutigem Wissensstand unklar und wird weder von der FINMA in der Wegleitung noch im KGGT Bericht oder im Aufsatz von Gabriela Hauser-Spühler effektiv adressiert. Finden noch Vorgänge des Zerstückelns und des Mixens von Transaktion statt, erschwert sich die Identifikation zusätzlich, indem die gleiche Person nun verschiedene Codes oder private keys aufweist. Multiple IP-Identitäten helfen nicht, eine natürliche Person als ultimate beneficial owner zu identifizieren.

---

38 Darum sind neu auch die Empfänger von Transaktionen bekannt zu geben.

39 Es ist interessant, dass selbst das FINMA RS 2016/7 (Online-Identifizierung), Rz. 53 letztlich auch eine dokumentarische oder mit einer elektronischen Signatur versehene Dokumentation verlangt.

Soll nun auf technologischem Wege sowohl eine Identifizierung des Vertragspartners / Users als auch des wirtschaftlich Berechtigten erfolgen, müsste der private key kryptographisch in der Lage sein, den wirtschaftlich Berechtigten abzubilden. Das würde bspw. bedeuten, dass ein Treuhänder, der als Verwaltungsrat von Sitzgesellschaften amtet, unterschiedliche private keys haben müsste, nämlich, für jeden wirtschaftlich Berechtigten einen anderen oder aber, dass der private key selber in der Lage wäre, weitere keys oder Anhänge von keys zu bilden für unterschiedliche wirtschaftlich Berechtigte, ähnlich der früheren Omnibus-Konti, die auf verschiedene Berechtigte aufgeschlüsselt wurden. Denkbar wäre auch die Verwendung eines zweiten key-Paares, ähnlich wie es für den Zugang von Banksafes zwei Schlüssel braucht. U.E. sind Zweifel angebracht, ob solche Transparenzschritte, wenn und soweit sie technologisch möglich wären, überhaupt gewollt sind, da heute vielfach die Wahrung der Anonymität im Vordergrund steht. Gegebenenfalls führt das zukünftig zu einer Gabelung der Geschäftsmodelle in transparente und nicht transparente.

4.3. Dokumentationspflichten im Zeitalter von FinTech

Gelingt es nicht oder nur schwerlich, Vertragspartner und wirtschaftlich Berechtigte zu identifizieren, kann der Dokumentationspflicht, wie sie heute in Art. 7 GwG verlangt wird, nicht im traditionellen Sinne nachgekommen werden. Das stellt die FINMA und die SRO, die als Auffangbecken diese Finanzintermediäre überwachen müssen, vor grosse praktische Schwierigkeiten. In jedem Fall ist «Dokumentation», als eine Art *digital trail*, technologisch und juristisch neu zu denken und den Prüfgesellschaften und den Aufsichtsorganen, die diese Finanzintermediäre überwachen müssen, Möglichkeiten zu eröffnen, diese lesbar zu machen und/oder die Inhalte mit der gleichen Technologie zu überprüfen. Da bleibt aber die nächste Frage, wie (lange) solche Protokolle angesichts des technischen Fortschrittes in der jeweiligen Form lesbar bleiben.

5. Weiterführende Gedanken zum Schluss

Die vorstehenden Ausführungen werfen mehr Fragen auf als dass sie zu Erkenntnissen führen. Das betrifft einerseits die Geschäftsmodelle in der Kryptowelt an sich als auch deren praktische Ausgestaltung:

- Diese rein technologiegesteuerten Geschäftsmodelle und insbesondere die Zahlungsüberweisungen auf blockchainbasierten Systemen sind auf dem Konzept der *Anonymität* aufgebaut. Bitcoin wurde konzipiert, um an den Staaten vorbei transaktionstransparent, aber nutzeranonym, dezentral operieren zu können. Die Geldwäschereibekämpfung hingegen kennt seit Jahren als oberstes Credo *Transparenz* hinsichtlich der beteiligten Personen. Das ist ein Widerspruch *per se*, der gelöst werden muss.
- Neue Herausforderungen stellen sich deshalb auch bezüglich der Dokumentation: Nummernkonti, Bargeld, Inhaberaktien, Offshore-Strukturen waren alles Versuche, der Transparenz zu entgehen, ein Kampf, der zugunsten einer effektiven Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und Steuerhinterziehen verloren wurde. Soll diese Transparenz auch bei digitalen Transaktionen möglich sein, sind neue Modelle der Dokumentation oder gar der Bekämpfung von Geldwäscherei zu entwickeln, die erst angedacht werden müssen.

Die Frage steht im Raum, ob diese neuen Geschäftsmodelle auch deshalb entwickelt wurden, um dank Technologie und Dezentralisierung diese Anonymität wieder zu erhalten und sie dann auch für die schwere Kriminalität im Darknet oder für Terrorismusfinanzierung zu nutzen. Es wird deshalb für den Staat eine Gratwanderung, wenn er gleichzeitig mit Vehemenz alle Formen von Geldwäscherei, Terrorismusfinanzierung und Steuerhinterziehung bekämpft und auf der anderen Seite unter dem Titel Innovationsförderung blockchainbasierte Geschäftsmodelle fördert. Es bleibt die grosse Herausforderung, dass sich Geschäftsmodelle entwickeln können, die technologisch fortschrittlich sind, aber das geltende Recht respektieren.