www.jusletter-it.eu

Björn Wegberg

# Compliance im Zeitalter von Kryptowährungen und ICOs

Der vorliegende Beitrag beschäftigt sich mit dem Spannungsverhältnis zwischen der inhärent dezentralen Natur der distributed-ledger Technologie und dem Transparenzverlangen der Geldwäschereibekämpfung. In einem zweiten Schritt analysiert der Autor die Möglichkeit, mittels LegalTech Anwendungen die Automatisierungslösung goAML der MROS und die Video- und Onlineidentifizierung der eidgenössischen Finanzmarktaufsicht (FINMA) in einer geeigneten Form zu verknüpfen, die den Bedürfnissen aller Parteien gerecht wird.

Beitragsart: Blockchain
Region: Schweiz
Rechtsgebiete: Blockchain

Zitiervorschlag: Björn Wegberg, Compliance im Zeitalter von Kryptowährungen und ICOs, in: Jusletter IT 12. November 2020

## Inhaltsübersicht



## 1. Einleitung

[1] Zur Frage nach der zulässigen Anwendbarkeit und dem wertschöpferischen Nutzen der Blockchain-Technologie sind äusserst unterschiedliche Stimmen zu finden. Mittels der inhärenten dezentralisierten Erstellung, Verifizierung und Aufbewahrung von ökonomischen Transaktionen entsteht eine eindeutige Wertschöpfung durch Kryptowährungen als ein von Finanzintermediären unabhängiges peer-to-peer Zahlungssystem.[1] Jedoch stellt diese Unabhängigkeit für die Geldwäschereibekämpfung – als wichtiger Bestandteil der Compliance – eine nicht unbeachtliche Schwierigkeit dar, denn mittels Blockchain können Finanzintermediäre, als frühere Drittpartei der Geldwäscherei, umgangen werden.[2]

[2] Der Bundesrat beschäftigte sich ebenfalls mit dieser Problematik und im anschliessenden Bericht sieht die interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und Terrorismusfinanzierung (KGGT) das Risiko von kryptobasierten Währungen für die Geldwäscherei als unbestritten an.[3]

[3] Hinsichtlich der vorgehend erläuterten Problemstellung beschäftigt sich die vorliegende Arbeit mit der – auf einer Literaturrecherche basierenden – Beantwortung der folgenden Forschungsfrage: Inwiefern müssen Compliancestrukturen zur Geldwäschereibekämpfung hinsichtlich der distributed ledger Technologie angepasst werden und welche LegalTech-Anwendungen können dabei hilfreich sein?

[4] Nach der nachfolgenden Begriffserläuterung wird anschliessend die Problematik der Blockchain-Technologie für die Geldwäschereibekämpfung genauer beleuchtet. Im Anschluss werden mögliche Massnahmen und LegalTech-Anwendungen vorgestellt, worauf das Fazit die vorliegende Arbeit komplettiert.

## 2. Begriffserläuterungen

[5] Hinsichtlich der technischen Natur der Blockchain-Technologie sind genauere, wenn auch bewusst kurz gehaltene Begriffsdefinitionen angebracht.

[6] Die sog. distributed ledger Technologie (DLT) kann als eine, auf zahlreichen Computern dezentral betriebene, Datenbank definiert werden. Die Blockchain-Technologie ist als eine angewandte Form der DLT zu betrachten, die eine dezentrale Transaktion von digital gespeicherten

1 Hsieh/Vergne/Wang, in: *Campbell-Verduyn Malcom* (Hrsg.): Bitcoin and Beyond, Cryptocurrencies, Blockchain, and Global Governance, Abingdon/New York 2018, 48, 52 (zit. Bitcoin/Bearbeiter).

2 Bitcoin/Campbell-Verduyn/Goguen (FN 1), 74.

3 Bericht des Bundesrates betr. rechtliche Grundlagen für *Distributed Ledger*-Technologie und Blockchain in der Schweiz vom 14.12.2018, 145 (zit. Bericht DLT).

Vermögenswerten (sog. Crypto-Assets) ermöglicht.[4] Dabei ist mithilfe des Transaktionsbuches (sog. ledger) eine Übersicht über alle bisherigen Transaktionen, inkl. der (u.U. anonymisierten) ausführenden Person, ersichtlich. Der Übergang zwischen den Bestandteilen der Blockchain wird mit Hashes – einer Verschlüsselung – gesichert, womit eine Überprüfung auf Richtigkeit der Blockchain jederzeit gewährleistet ist.[5] Die generelle Validierung des Systems geschieht durch die Mehrheit (d.h. 51 %)[6] der beteiligten Personen mittels der Lösung kryptographischer Problemstellungen.[7]

[7] Neben den reinen Kryptowährungen ist im Besonderen bei Initial Coin Offerings (ICO), die eine digitale Kapitalbeschaffung für Unternehmen darstellen, zu differenzieren.[8] Hinsichtlich der Unterstellung unter das GwG[9] ist zwischen den drei durch die FINMA vorgebrachten Tokens zu unterscheiden:[10] Generell stellt ein Token eine im ledger aufgezeichnete digitale Information dar, über die der Eigentümer mittels Zugangsdaten bestimmen kann.[11] Erstens sind Anlagetokens, die ihren Wert aufgrund der Verknüpfung zu realen Vermögenswerten besitzen, als Effekte zu behandeln. Somit erfolgt die Regulierung gemäss dem FinfraG[12], dem BEG[13] und insb. dem kürzlich in Kraft getretenen FIDLEG[14], womit eine Qualifikation als Währung i.S. des WZG[15] zu verneinen ist.[16]

[8] Zweitens sind die Zahlungstokens näher zu betrachten. Sie stellen eine innovative Zahlungsmethode dar und benutzen die Infrastruktur der Blockchain zur Übertragung. Gemäss der FINMA sind sie ausdrücklich klassischen Kryptowährungen gleichgesetzt und deshalb dem GwG unterstellt, sofern sie nicht als Effekte behandelt werden.[17]

[9] Drittens sind Nutzungstokens differenziert zu analysieren. Sie fallen i.d.R. nicht unter das GwG, wenn der Zweck lediglich als Zutrittsbeschaffung zur Nutzung der Blockchain angesehen wird. Jedoch wird bei Bejahen einer wirtschaftlichen Anlage der Nutzungstoken analog zum Anlagetoken geregelt.[18]

---

4 Weber Rolf H./Baisch Rainer: Internationale Entwicklungen in der Crypto-Asset-Regulierung (ICO/Token), Jusletter vom 18. Februar 2019, 4.

5 Fasching Joachim Galileo: Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, Masterarbeit, Wien 2017, 4.

6 Fasching (FN 5), 7.

7 Kilgus Sabine/Walser Kessel Caroline: Compliance in der Kryptowelt?, Jusletter IT vom 21. Februar 2019, 5.

8 Müller Lukas/Reutlinger Milena/Kaiser Philippe J.A.: Entwicklung in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, EuZ 2018, Nr. 3, 80 ff., 91.

9 Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 10. Oktober 1997, Stand 18. Februar 2020 (SR 955.0).

10 FINMA: FINMA publiziert Wegleitung zu ICOs, Medienmitteilung vom 16. Februar 2018 (zit. FINMA, Wegleitung ICOs).

11 Weber/Baisch (FN 4), 4.

12 Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 19. Juni 2015, Stand am 1. Januar 2020 (SR 958.1).

13 Bundesgesetz über Bucheffekten vom 3. Oktober 2008, Stand am 1. Januar 2020 (SR 957.1).

14 Bundesgesetz über die Finanzdienstleistungen vom 15. Juni 2018, Stand am 1. Januar 2020 (SR 950.1).

15 Bundesgesetz über die Währung und die Zahlungsmittel vom 22. Dezember 1999, Stand am 1. Januar 2020 (SR 941.10).

16 Kilgus/Walser Kessel (FN 7), 3.

17 FINMA, Wegleitung ICOs (FN 10), 2.

18 FINMA, Wegleitung ICOs (FN 10), 3.

[10] Insofern ist eindeutig, dass sich die Problemstellung der Geldwäscherei in der Blockchain auf klassische Kryptowährungen einerseits, und Zahlungstoken als ICO andererseits zu fokussieren hat.

## 3. Blockchain und Geldwäscherei – Problematiken

[11] Wie bereits vorangehend erläutert, ist die dezentrale Natur der Blockchain-Technologie das Kernproblem der Regulierungsbemühungen. Gewisse Autoren werfen die Frage auf, ob aufgrund des inhärent unabhängigen Designs der DLT eine Regulierung wirklich dem Sinn hinter der Technologie entspricht.[19] Diese Frage wird jedoch in der vorliegenden Arbeit ausgeklammert.

[12] Strafrechtlich sanktioniert wird die Geldwäscherei durch Art. 305$^{bis}$ StGB[20], welche durch die für Finanzintermediäre geltenden aufsichtsrechtlichen Vorschriften des GwG komplementiert werden. Neben den klassischen Finanzintermediären sind gemäss Art. 1b BankG[21] FinTech-Unternehmen ebenfalls dem GwG unterstellt.[22] Des Weiteren gelten gemäss dem Bericht des Bundesrates die herkömmlichen Geldwäschereivorschriften analog für Kryptowährungen, da das GwG technologieneutral formuliert ist.[23]

[13] Infolgedessen sind bei Handhabung von Kryptowährungen und Zahlungstokens die Sorgfaltsgrundsätze *know your costumer* (Art. 3 GwG) und *know the beneficial owner* (Art. 4 GwG) zu beachten. Demgemäss muss die wirtschaftlich berechtigte Person registriert und im Rahmen von Art. 7 GwG dokumentiert werden.[24]

[14] Die Blockchain-Technologie steht den Sorgfaltspflichtgrundsätzen von Art. 3 und 4 GwG jedoch diametral entgegen. Die Dezentralisierung und (begrenzte) Anonymität stellen die grössten Problemfaktoren dar. Aufgrund der nicht mehr zwingenden Zwischenschaltung von Finanzintermediären bei Transaktionen, ermöglicht eine Blockchain eine unabhängige Transaktionslösung. Des Weiteren sind bei öffentlichen Blockchains die Namen der eine Transaktion in Auftrag gebenden Person lediglich in verschlüsselter Form sichtbar. Die Identifizierung einer Person aufgrund einer digitalen Signatur gestaltet sich zwar als schwierig, aber nicht als unmöglich.[25] Jedoch sind Einwände von Autoren berechtigt, die die Ermittlung von Personen aufgrund von sog. Mixern, die die Anonymität der Transaktion aufgrund deren Verkleinerung unter den meldepflichtigen Schwellenwert erhöhen, kritisch betrachten.[26] In der Folge ist die Methode der Kettenanalyse, d.h. die historische Nachverfolgung der Transaktionen von Kryptowährungen, erschwert.[27]

[15] Der Sorgfaltspflichtmassstab für die Dokumentationspflicht i.S.v. Art. 7 GwG ist, aufgrund des in den vorangehenden Erläuterungen ersichtlichen gewichtigen Risikos, hoch anzusetzen.[28]

---

19 Bitcoin/Musiani/Mallard/Méadel (FN 1), 133.

20 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, Stand am 3. März 2020 (SR 311.0).

21 Bundesgesetz über die Banken und Sparkassen vom 8. November 1934, Stand am 1. Januar 2020 (SR 952.0).

22 Kilgus/Walser Kessel (FN 7), 2–3.

23 Bericht DLT (FN 3), S. 145.

24 Kilgus/Walser Kessel (FN 7), 2.

25 Bitcoin/Campbell-Verduyn/Goguen (FN 1), 74.

26 Kilgus/Walser Kessel (FN 7), 5.

27 Bericht DLT (FN 3), 145.

28 Kilgus/Walser Kessel (FN 7), 2.

[16] Erfolgt eine für den Finanzintermediär zwielichtige Transaktion, untersteht dieser nach Art. 9 GwG bei begründetem Verdacht einer Meldepflicht an die Meldestelle für Geldwäscherei (MROS). Dieser begründete Verdacht ist als eine Gesamtbeurteilung der vorliegenden Informationen zur Person des Kunden, der wirtschaftlich berechtigten Person der Vermögenswerte und deren Herkunft anzusehen. Ein vorsätzliches oder fahrlässiges Unterlassen dieser Meldepflicht nach Art. 9 GwG hat für den Finanzintermediären rechtliche Konsequenzen, weshalb ein eindeutiges Spannungsverhältnis zu den Blockchain-Charakteristiken herrscht.[29]

## 4. Massnahmen zur Geldwäschereibekämpfung

[17] Einleitend zu den nachfolgenden Erläuterungen zu geldwäschereibekämpfenden Massnahmen sind berechtigterweise Abwägungen zwischen der Bekämpfung der negativen Externalitäten und der Innovationskraft der Blockchain-Technologie vorzunehmen.[30] Ein gänzliches Verbot von Kryptowährungen und ICOs würde dem liberalen Geist der Wirtschaftsordnung und dem Innovationsstandort der Schweiz widersprechen,[31] da selbst auch der Bund aktiv FinTech unternehmen fördert.[32] Insofern sind differenzierte Massnahmen vorzubringen.

[18] In der vorherrschenden Literatur wird vermehrt der Fokus zur Geldwäschereibekämpfung auf das Tauschgeschäft von Kryptowährungen bzw. Zahlungstokens in Fiat-Währung und umgekehrt gelegt.[33]

[19] Die Anbieter von sog. Krypto-Wallets sind bzgl. der Geldwäschereibekämpfung vorliegend genauer zu betrachten. Wallet-Dienstleister bewahren die Tokens ihrer Kunden auf und nehmen u.U. Transaktionen in deren Auftrag vor.[34] Infolgedessen unterstehen sie bedingterweise den Abklärungs- und Informationspflichten nach dem GwG. Dabei muss zwischen custodian und non-custodian Wallet-Anbietern differenziert werden. Bei custodian Wallets besitzt der Dienstleister Verfügungsmacht über die aus ihrer Perspektive fremden Vermögenswerte, da er den Privat Key des Endkunden aufbewahrt. Folglich ist es dem Anbieter möglich, Zahlungen im Namen und Auftrag des Kunden zu tätigen und verrichtet so eine Dienstleistung für den Zahlungsverkehr. Insofern sind custodian Wallet-Anbieter dem GwG unterstellt.

[20] Bei non-custodian Wallets wird lediglich die Nutzung der Software durch den Anbieter zur Verfügung gestellt, wobei dieser über keinen Zugriff auf das Wallet des Endkunden verfügt. Der Kunde tätigt somit alle Zahlungen selbständig, und aufgrund der fehlenden rechtlichen Verfügungsmach über die Vermögenswerte durch den Wallet-Anbieter ist dieser nicht dem GwG als Finanzintermediär unterstellt.[35]

[21] Das Kernziel des GwG ist immer die Identifikation der natürlichen Person, welche die wirtschaftlich Berechtigte am Vermögen darstellt. Diese Feststellung der Person durch den Finanz-

29 Baltensperger Jürg: Geldwäschereibekämpfung in der Blockchain, Jusletter IT vom 23. Mai 2019, 5.

30 Bitcoin/Jia/Zhang (FN 1), 96–97.

31 Baltensperger (FN 29), 6.

32 Kilgus/Walser Kessel (FN 7), 2.

33 Bitcoin/Campbell-Verduyn/Goguen (FN 1), 78; Bitcoin/Jia/Zhang (FN 1), 96; ebenso Kilgus/Walser Kessel (FN 7), 6.

34 Weber/Baisch (FN 4), 25.

35 Bericht DLT (FN 3), 145–146; Kilgus/Walser Kessel (FN 7), 6.

intermediär ist bei verselbständigten Blockchains jedoch nicht möglich, weshalb eine zentrale Identifikationsstelle einen Lösungsansatz darstellen könnte. Dabei wären die in der Blockchain teilnehmenden Personen gezwungen, sich bei dieser u.U. staatlichen Stelle zu identifizieren.[36] Dazu wäre der Einwand möglich, dass die Benutzer einer Blockchain zum Zweck der dezentralen Transaktion von Vermögenswerten i.d.R. keine staatliche Kontrolle wollen und Anonymität verfolgen. Insofern würden diese u.U. einen anderen Blockchain-Dienstleister wählen.[37]

**LegalTech Anwendungen**

[22] Mit Hilfestellungen durch Systeme aus der Rechtsinformatik soll zum einen die Effizienz erhöht, aber auch den Gesichtspunkten der Sicherheit und Anonymität Sorge getragen werden.

[23] Mit dem 1. Januar 2020 wurde das neue Datenverarbeitungssystem goAML durch die MROS eingeführt.[38] Dabei waren Digitalisierungsbestrebungen Anlass zur Modernisierung, denn bis anhin erfolgte die Verdachtsmeldung mehrheitlich über den Postweg. Nun kann die Verdachtsmeldung durch einen Finanzintermediär entweder manuell online ausgefüllt, oder als XML-Datei[39] hochgeladen werden, worauf die Verarbeitung automatisiert erfolgt.[40] Diese Neuerung soll insb. die Effizienz bei einer grossen Anzahl von jährlichen Meldungen erhöhen.

[24] Des Weiteren führte die FINMA 2016 aufgrund der digitalen Natur der Blockchain-Technologie die Möglichkeit der Video- und Online-Identifizierung ein. Dabei werden u.a. Bilder der Vertragspartei im Rahmen der Identitätsprüfung erstellt.[41] Problematisch dabei ist, dass Blockchain-Benutzer u.U. ihre Anonymität wahren und sich nicht direkt ablichten lassen möchten, weshalb auch bereits App-Lösungen entwickelt worden sind.[42]

[25] Hinsichtlich der Automatisierungslösung von goAML und der digitalisierten Vorgehensweise zur Identifizierung des wirtschaftlich Berechtigten wäre eine Verbindung dieser zwei Prozesse in irgendeiner Form wünschenswert. Jedoch stellen sich diverse technische Schranken für dessen Durchführbarkeit.

[26] Zu Beginn wäre eine Anonymisierung des Kunden in dessen Vertrag mit dem Finanzintermediär mittels eines Hash problemlos möglich und zwei Serien könnten mittels einer automatisierten Vertragserstellung produziert werden, wobei der Finanzintermediär lediglich Einsicht in die anonymisierte Form hätte. Um deren Unabänderbarkeit abzusichern, wäre ein Abspeichern der Verträge auf einer Blockchain theoretisch möglich, jedoch praktisch nicht durchführbar. Erstens stellen sich datenschutzrechtliche Fragen, die sich auch mithilfe privater Blockchains nur begrenzt lösen lassen. Zweitens wird in der Praxis lediglich der Hash einer Datei in der Blockchain gespeichert, da die Daten sonst schlichtweg zu gross und die Transaktionskosten stark erhöht werden. Insofern wäre eine Mitwirkung der Parteien im Verdachtsfall zwingend notwendig.

---

36 Baltensperger (FN 29), 6.

37 Bitcoin/Musiani/Mallard/Méadel (FN 1), 133.

38 Vgl. https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html (aufgerufen am 11.05.2020).

39 XML ist eine Programmiersprache mit dem Zweck, grosse Datenmengen zu strukturieren (vgl. MROS: Frequently Asked Questions (FAQ) zur Einführung eines neuen Datenverarbeitungssystems bei der MROS, Version 2.5, 2019, Ziff. 17).

40 MROS: goAML Web – Handbuch, MROS-spezifische Systemanpassungen, Version 2.1, 2019, 6.

41 FINMA: Video- und Onlineidentifizierung, Sorgfaltspflichten bei der Aufnahme von Geschäftsbeziehungen über digitale Kanäle, Rundschreiben 2016/7, Rz. 13 (zit: FINMA, RS 16/7, Rz. . . . ).

42 Baltensperger (FN 29), 6.

[27] Des Weiteren wäre das Einsetzen eines in der Blockchain kodierten smart contracts denkbar, der auf Geheiss des Finanzintermediär die auf der Blockchain gespeicherten Dokumente in Form einer XML-Datei an das goAML System der MROS sendet. Wie bereits erläutert, werden Dateien i.d.R. nur in Form ihrer Hashes auf der Blockchain gespeichert, weshalb dieser Ansatz bereits scheitert. Zweitens ist es smart contracts aus technologischer Sicht verwehrt, mit jeglicher Technologie ausserhalb der eigenen Blockchain zu interagieren. Dazu ist ein sog. Orakel nötig, welches als Element zwischen dem smart contract und der realen Welt fungiert.[43]

[28] Eine weiterführende Automatisierung der Video- und Online-Identifizierung der FINMA gestaltet sich ebenfalls als schwierig. Auch bei der Online-Identifizierung, welche ein hohes Mass an Mitarbeit des Endkunden verlangt, ist eine vollständige anonymisierte Automatisierung schwierig. Das durch den Kunden eingesendete Identifizierungsdokument muss u.a. durch einen, den Voraussetzungen des ZertES[44] erfüllenden, Drittanbieter authentifiziert werden. Insofern wird wiederum eine Drittpartei einbezogen.[45]

[29] Infolgedessen ist eindeutig, dass nach dem heutigen technologischen Stand eine Weiterführung der bis jetzt bereits erfolgten Digitalisierung im Bereich der Geldwäschereibekämpfung schwierig ist. Eine Blockchain-Lösung wäre hinsichtlich des Anonymitätsbedürfnisses der Kunden und der Manipulationssicherheit der Dateien (ohne eine Abänderung des Hashes zu bewirken) sicherlich wünschenswert. Jedoch sind die technologischen und ökonomischen Schranken zu beachten.

## 5. Fazit

[30] Die Anonymität ist der Grundbaustein von Kryptowährungen und Zahlungstokens, da mittels DLT dezentral und ohne Mitwirkung von Finanzintermediären Transaktionen vorgenommen werden können. Gegensätzlich fordert die Geldwäschereibekämpfung eine Transparenz geltend für alle Strukturen, die unter das GwG fallen.

[31] Unter das GwG sind Kryptowährungen und Zahlungstokens als ICOs zu subsumieren, weshalb damit in Berührung kommende Finanzintermediäre ebenfalls die Sorgfaltsgrundsätze nach Art. 3 und 4 GwG und die Meldepflicht nach Art. 9 GwG beachten müssen. Die Pflichten *know your customer* und *know the beneficial owner* stehen jedoch in einem starken Spannungsverhältnis zur dezentralen Natur der Blockchain-Technologie. Die wirtschaftlich berechtigten Personen an den Vermögenswerten sind lediglich in einer begrenzt anonymisierten Form ersichtlich und sind auch aufgrund ihres Anonymisierungsbedürfnis nicht auf eine freiwillige Herausgabe ihrer Daten erpicht.

[32] Die Geldwäschereibekämpfung hat sich infolgedessen an der Schnittstelle zwischen Fiat-Währung und Kryptowährung zu fokussieren. Dabei unterstehen insb. die custodian Wallet-Anbieter, die über den Privat Key des Kunden und somit über dessen Vermögenswerte bestimmen können, dem GwG. Ferner wäre bei verselbständigten Blockchains eine zentrale Identifikationsstelle ein Lösungsansatz, wobei deren Einsatz durch die Benutzer der Blockchain fraglich ist.

---

43 Zum Ganzen: Fink, in: *Fries Martin/Paal Boris P.* (Hrsg.): Smart Contracts, Tübingen 2019, 7–8.

44 Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18. März 2016, Stand am 1. Januar 2020 (SR 943.03).

45 FINMA, RS 16/7 (FN 41), Rz. 38–40.

[33] Um dem technologischen Fortschritt gerecht zu werden, führte die MROS das System goAML ein, welches eine automatische Verarbeitung der durch die Finanzintermediären eingesendeten Dateien erlaubt. Des Weiteren ermöglicht die FINMA die Video- und Online-Identifizierung der Kunden durch die Finanzintermediäre. Die erste Anwendung bezweckt eine Effizienzsteigerung der Compliance, wobei die Online-Identifizierung eine Standortunabhängigkeit ermöglicht. Jedoch gestaltet sich eine Koppelung dieser zwei Lösungen, die dem Anonymitätsbedürfnis der Kunden und dem Transparenzverlangen der FINMA gerecht wird, technologisch und ökonomisch als schwierig.

---

Björn Wegberg ist Rechtsstudent im 5. Semester des BLaw an der Universität St. Gallen (HSG).