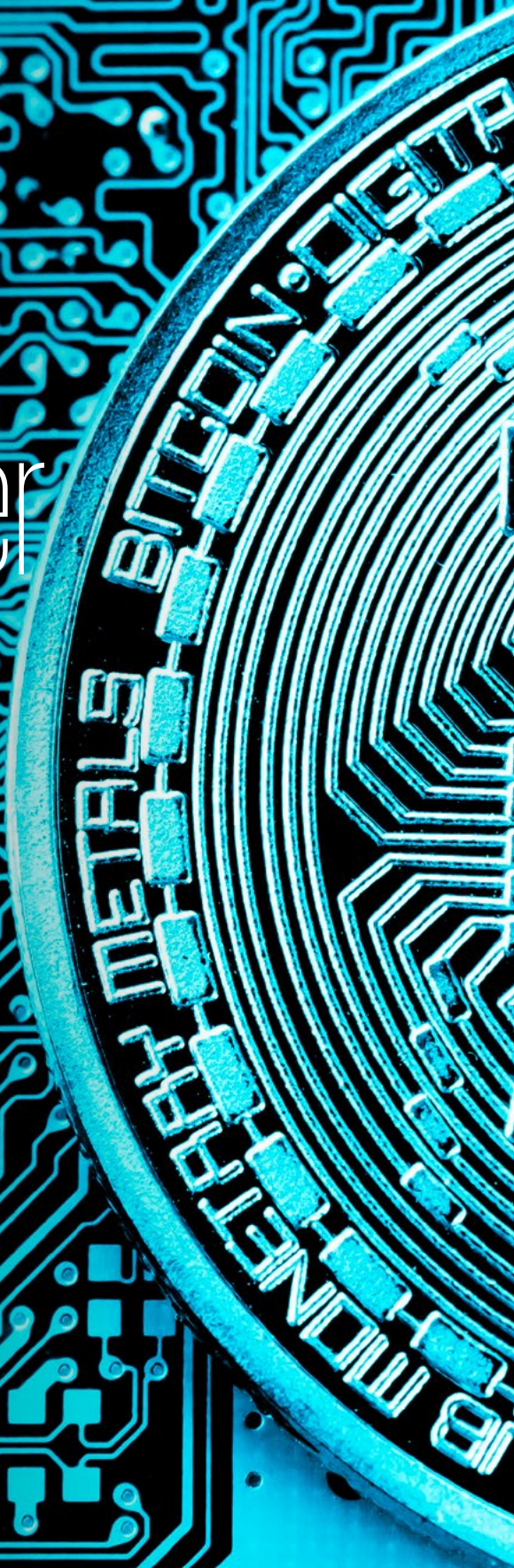
KPMG

Geldwäscherei-bekämpfung im Kryptozeitalter

Kryptowährungen – Neue Herausforderungen

Autoren: Pascal Sprenger, Franziska Balsiger



kpmg.ch

Die ursprüngliche Idee von Kryptowährungen war, Peer-to-Peer Transaktionen ohne Einbezug des traditionellen Bankensystems zu ermöglichen und diese somit kostengünstiger zu gestalten. Die meisten Leute (mit Ausnahme der sogenannten Miner) erwerben aber Kryptowährungen in dem sie Fiatgeld in Kryptowährungen umtauschen, sodass spätestens zu diesem Zeitpunkt der Finanzintermediär dennoch ins Spiel kommt. Sobald jemand Kryptowährungen in Fiatgeld, Güter und Dienstleistungen umwandelt, besteht für Finanzinstitute die Pflicht, spezielle Sorgfalt bei der Durchführung von Geldwäschereiprüfungen anzuwenden.

Während sich Finanzinstitute über die letzten 40 Jahre stetig Wissen und Techniken zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung für herkömmliche Zahlungsmethoden angeeignet haben, sind Kryptowährungen erst seit circa 2008 aktuell. Die meisten Finanzinstitute zögern, sich mit dem Thema Kryptowährungen auseinanderzusetzen, da dieses hochkomplex ist und darüber hinaus Kriminellen eine neue Art bietet, Geld zu waschen und Terrorismus zu finanzieren.

Insbesondere auch im Sanktionswesen stellen sich grosse Herausforderungen für Finanzinstitute in Bezug auf die Verwendung von Kryptowährungen, zumal sie nicht einfach auf die herkömmlichen Konzepte der Gelwäschereibekämpfung zurückgreifen können.

Der inhärente Abbau von Korrespondenzbankendienstleistungen in Bezug auf gewisse Länder oder Regionen, wie z.B. Karibik, Venezuela oder Afrika, hat eine erhöhte Verwendung von Kryptowährungen in diesen Ländern zur Folge. Sehr zur Gefährdung der globalen Risikoabbau-Anstrengungen. Für Finanzinstitute ist es fast unmöglich festzustellen, ob ein anonymes Konto einer sanktionierten Person gehört, da die zugrunde liegende Blockchain meistens keine Aufschlüsse bezüglich IP-Adressen oder Privatdaten mit denen der Kontoinhaber identifiziert werden könnte, erlaubt. Selbst wenn die Blockchain diese Informationen enthalten würde, gibt es immer noch diverse Möglichkeiten die Identität und IP-Adresse zu verbergen, z.B. in dem man blockierte VPN-Netzwerke umgeht oder einmalige Email-Adressen und Proxy-Netzwerke (wie z.B. Thor) benutzt. Im besten Fall können Finanzinstitute nur eine Seite der Transaktion identifizieren, meistens diejenige ihre eigenen Kunden.

Krypto-Cleansing als Methode Geld zu waschen

In gewissen Ländern wird Krypto-Cleansing zur Umgehung von internationalen Sanktionen benutzt. Dieser Prozess involviert meistens organisierte digitale Geldwäscherei. Typischerweise beinhaltet der Waschvorgang folgende Schritte:[1]

1. Zuerst kauft der Kriminelle eine herkömmliche Kryptowährung an einer digitalen Börse oder in Bar oder mit einer Debitkarte an einem digitalen Währungsautomaten. Die erste Option wird bevorzugt, denn die meisten Betreiber von digitalen Währungsautomaten sind regulierte Einheiten, die entsprechend Pflichten zur Vermeidung von Geldwäscherei erfüllen müssen. Beim Kauf von Kryptowährungen an einer digitalen Börse setzen Kriminelle oftmals Strohmänner ohne kriminelle Vergangenheit und mit einem nachweisbaren Anstellungsverhältnis ein. Sie stärken ihre Anonymität weiter, in dem sie Pseudonyme annehmen, anonyme E-Wallets erwerben, VPN-Netzwerke ohne Logs und Blockchain-optimierte Smartphones verwenden.
2. Sobald die Strohmänner von der digitalen Börse verifiziert wurden, werden Primary Coins (z.B. Bitcoin, Etherum, oder Litecoin) mittels Fiatgelder oder Banküberweisungen gekauft. Die Primary Coins wiederum werden dann zum Erwerb von sogenannten Alt-Coins an «Advanced Exchanges» verwendet. Diese Alt-Coins haben spezifische Merkmale, z.B. Privacy Coins, die eine erhöhte Anonymität erlauben.
3. Zur Entfernung des Audit Trails setzen die Geldwäscher eine Taktik ein, die Mixing oder Tumbling heisst. Dabei werden Mixing-Dienstleister wie Bitmixer oder Helix beansprucht, die die Coin-Adressen der Primary Coins auf temporäre E-Wallets übertragen, um so die Blockchain durcheinander zu wirbeln und die Verifikation zu unterbinden.
   Eine weitere Strategie ist es, bewusst eine falsche Empfängeradresse anzugeben, um dann die Transaktion an eine Backup-Adresse zu schicken um damit den Audit Trail zu unterbrechen. In einem nächsten Schritt werden die Primary Coins an einer «Advanced Exchanges» zum Erwerb von Privacy Coins (z.B. Zcash, Verge, Monero, Dash, Desire, usw.) eingesetzt.

[1] Crypto-cleansing: strategies to fight digital currency money laundering and sanctions evation, Josua Fruth, https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I, zuletzt besucht 27. Juni 2018

4. Als nächstes setzen die Geldwäscher verschiedene Privacy Coins, Börsen und digitale Adressen ein, um den Audit Trail zu unterbrechen und so das Schwarzgeld zu waschen, um danach dieses Geld wieder in das herkömmliche Finanzsystem zu integrieren.
5. Nach der Unterbrechung des Audit Trails hat der Geldwäscher verschiedene Optionen, das digitale Weissgeld in Fiatgeld umzutauschen:
   - Burstout-Integration: Privacy-Coin-Bestände werden zuerst in Primary Coins und anschliessend in eine Fiatwährung umgewandelt. Dieser Betrag wird dann auf ein bestimmtes Bankkonto überwiesen oder es werden Immobilien mit der Begründung, dass der Halter Kapitalgewinnsteuer vermeiden möchte, gekauft.
   - Der digitale Betrag wird auf ein physisches Crypto-Wallet geladen oder es wird eine QR-Code als Printout angefertigt, sodass die Gelder weltweit weiter transportiert werden können.

Wie kann man Geldwäscherei mittels Kryptowährungen bekämpfen

1. Finanzinstitute: Verstärkung der Prozesse zur Bekämpfung von Geldwäscherei

Aufgrund ihrer Position innerhalb des Geldwäschereiprozesses bei der Verwendung von Kryptowährungen sollten sich Finanzinstitute hauptsächlich auf ihre Schnittstellenfunktion konzentrieren, d.h. wo Finanzinstitute mit Krypto-Börsen in Kontakt kommen. Um ein normales Kundenverhalten von möglichen Fällen von Geldwäscherei zu unterscheiden, müssen spezifische Überlegungen angestellt werden.

In folgenden Situationen bestehen erhöhte Risiken:[2]

- Kunden, deren überwiegende Geldquelle aus Bargeld oder sonstigen liquiditätsnahen Mitteln besteht oder von digitalen Börsen und Drittzahlungsanbieter stammen,
- Wiederholte internationale Banküberweisungen an digitale Börsen;
- Übermässige Mittelzuflüsse und -abflüsse, die nicht den dem Finanzinstitut bekannten Geldquellen des Kunden entsprechen;
- Rechtseinheiten oder gemeinnützige Organisationen, die digitale Währungen so benutzen, wie man es von einer Privatperson erwarten würde (könnte ein Zeichen für das Bestehen einer Mantel- oder Vorratsgesellschaft sein);
- Transaktionen, die aufgrund ihrer Struktur nicht belegt werden müssen und Grenzwerte umgehen;
- Situationen in denen verschiedene Kunden ähnliche Geldwerte in einem ähnlichen Zeitfenster an digitale Wechselkurssysteme schicken;
- Bei Retailbanken: Bargeld, das in hoher Frequenz die Bank verlässt oder zahlreiche Aktivitäten, die auf Bargeld beruhen;
- Schnelles Durchschleusen von flüssigen Mitteln an externe Finanzinstitute, bei denen Einlagen und Mittelabflussaktivitäten im gleichen Zeitfenster aggregiert ähnlich zu sein scheinen;
- Teure Anschaffungen, wie beispielsweise Immobilien, Autos oder Boote;
- Verbindungen zu, Transaktionen mit oder Reisen in Länder, die als Drehscheiben für Krypto-Geldwäscherei bekannt sind (z. B. Russland, Venezuela, Libanon, Iran, Nordkorea, Ukraine, Türkei, Paraguay) und in solche Länder, die in geografischer Nähe zu Ländern mit Konflikten, hoher Korruption, organisierter Kriminalität und terroristischen Aktivitäten stehen.

Banken sollten zudem ihre Systeme und Prozesse anschauen, um sicherzustellen, dass sie:

- Keine Mittelzuflüsse/-ausflüsse von Börsen annehmen, die keine Identifikation von Kunden durchführen oder keine KYC-Prozesse einsetzen; oder
- Keine Erlöse aus Privacy Coins, sofern identifizierbar, annehmen.

2. Transaktionsüberwachung

Auch wenn Finanzinstitute die Anonymität der Kryptowährungen nur schwer durchbrechen können, um den wirtschaftlich Berechtigten zu identifizieren, können IT-Systeme trotzdem Algorithmen einsetzen, um gewisse Muster und Verhalten zu entdecken, die sie schon für Fiatgeld entwickelt haben und die auf Geldwäscherei hindeuten. Sollte ein Konto aufgrund der zementierten Historie des Journals schon einmal mit kriminellen Aktivitäten in Verbindung gebracht worden sein, kann der Mittelfluss in Kryptowährungen als wichtiger Indikator für die Strafverfolgung hinzukommen.

3. Gesetzesanpassungen

Während Kritiker der Kryptowährungen oft sagen, dass der Mangel an identifizierenden Informationen während der gesamten digitalen Transaktion ein wesentliches Hindernis bei der Überwachung und Bekämpfung von Geldwäscherei darstellt, existieren bei Kryptowährungen – zumindest theoretisch – gewisse Elemente, wie Identifizierung der Parteien und Informationen oder Aufzeichnung von Transaktionen, die dazu dienen könnten, Geldwäscherei aufzudecken oder zu verhindern. Um Risiken von Kryptowährungen effektiv einzudämmen, müssen die KYC-Prozesse bei der Ausgabe von E-Wallets weltweit rigoroser werden. In anderen Worten braucht es globale Standards auf internationaler Ebene. Natürlich verlangen solche Standards, dass es einen Konsens gibt zwischen den Hauptakteuren der Branche und dass eine dazugehörige Regulierung ausgearbeitet wird.

---

[2] Crypto-cleansing: strategies to fight digital currency money laundering and sanctions evation, Josua Fruth, (Fn 1)

Als eine der internationalen Standardsetter für die Geldwäschereiprävention lancierte die FATF im Februar 2018 eine weitere Initiative, die die Geldwäschereirisiken im Bereich von Kryptowährungen adressiert.[3] Die FATF lud die FSC aus Südkorea ein, die anderen 36 Mitgliedstaaten über deren Arbeit zu informieren. Die FSC erarbeitete Regeln zur Geldwäschereiprävention für lokale Kryptowährungsbörsen, nachdem die FSC eine nicht registrierte, von anonymen Investoren durch Börsenmakler platzierte Bewegung von USD 600 Millionen entdeckt hatte. In der Konsequenz erlaubt die FSC heute keine anonymen Handelskonten mehr und verlangt die Verifikation der realen Namen der handelnden Parteien. Zudem müssen unter den neuen Regeln E-Wallets einer realen Person zugeordnet werden, sodass der Handel mit anonymen oder pseudonymisierten E-Wallets nicht mehr möglich ist.

4. Staatliche Kontrolle von Drittpartei-ID-Anbietern
Dritte, die als ID-Anbieter fungieren, könnten ein wichtiges Puzzle-Teil sein, um gesetzestreuen Nutzern ein gewisses Grad an Anonymität zu gewähren und den Behörden trotzdem die Strafverfolgung krimineller Elemente in der Kryptowelt zu ermöglichen. Durch sie könnte die lästige Identifizierung und KYC-Datenerfassung durch in der Kryptowelt tätige Unternehmen, die naturgemäss wenige Kompetenzen bezüglich der Verwahrung von Kundenidentifikationsdaten aufweisen, vermieden werden. Verschiedene Vorkommnisse (z.B. der Vorfall in Korea) zeigen, dass persönliche Information, die durch Krypto-Unternehmen verwahrt werden, besonders auf Daten- und Identitätsdiebstahl anfällig ist. Es wäre daher sinnvoll, Drittpartei-ID-Anbieter, die die Aufbewahrung von Daten für Krypto-Unternehmen übernehmen, unter staatliche Aufsicht zu setzen, sodass deren Rechenschaftspflicht vergrössert wird.

5. Das Regulieren von Börsen, speziell der «Advanced Digital Exchanges» und solcher, die Primary Kryptowährungen anbieten
Das Regulieren von Börsen, die Primary Kryptowährungen anbieten, wäre ein leicht greifbarer Beginn zu einer Verbesserung, denn diese akzeptieren oft Fiatgeld im Austausch für Primary-Kryptowährungen, so z.B. Bitcoin. Der Fokus sollte jedoch auch auf der Regulierung von sogenannten «Advanced Digital Exchanges» liegen, wo Alt-Coins gegen Primary Coins gehandelt werden. Diese sind schwieriger zu regulieren, denn sie akzeptieren kein Fiatgeld sondern nur Primary Coins. Alt-Coins sind meistens dezentralisiert aufgesetzt und daher schwierig zu erfassen, wenn die Regulierung lokal begrenzt und nicht international koordiniert wird. Eine Regulierung der sogenannten «Advanced Digital Exchanges» sollte jedoch auf offene Ohren stossen, da der Audit Trail der Privacy Coins zwar anonym ist, aber die Fähigkeit der Digital Exchanges ihre eigenen Transaktionen und E-Wallets zu überwachen, durchaus besteht. Für eine effektive Geldwäschereibekämpfung ist die Zusammenarbeit mit internationalen Standardsetter, so z.B. die FATF, unvermeidbar, da das Problem mit internationalen Standards angegangen werden sollte.

---

[3] Vgl. global AML Watchdog to Step up Crypto Money Laundering Scrutiny, Wolfie Zhao, https://www.coindesk.com/global-aml-watchdog-to-step-up-crypto-money-laundering-scrutiny/, zuletzt besucht 27. Juni 2018

6. Blockchain als Lösung

Im Vergleich zu Fiatgeld besitzt die Blockchain-Technologie das inhärente Potenzial, Geldwäschereirisiken effektiv zu vermindern. Die Blockchain besteht grundsätzlich aus einem öffentlich zugänglichen Journal, sodass die Überwachung, Validierung und Verbuchung der vollständigen Historie jeder Transaktion leicht ist. Leser des öffentlich zugänglichen Journals sowie Krypto-Miner werden sofort über auftretende Transaktionen benachrichtigt. Dazu kommt, dass es sozusagen unmöglich ist, Kryptowährungen zu fälschen, da jede Art ihre eigenen Merkmale hat, die von End-to-End-Miners verifiziert werden. Eine Transaktion, die nicht in ihren ganzen Phasen (einschliesslich dem Abgangs-Wallet, dem Empfänger-Wallet, der Währungsart und dem Betrag) verifiziert wird, würde sofort ohne menschliche Intervention gestoppt. In diesem Sinne wäre die digitale Geldwäschereibekämpfung einfacher als die für Fiatgeld bestehenden «Paper Trails». Es wäre zudem technisch machbar, ein Blockchain-Protokoll so anzupassen, dass nur KYC-verifizierte Wallets erlaubt wären, sodass alle Transaktionen auf das identifizierte Wallet zurückverfolgt werden können. Durch die Benutzung von Blockchain-Technologie könnten weitere Risikoanalysen zur Geldwäschereibekämpfung sowie Warnmechanismen und Berichterstattungsoptionen in das Kryptowährungssystem eingebaut werden, sodass viel mehr als nur der Eingangs- und Ausgangspunkt überwacht werden könnte. Die Nutzung der inhärenten Merkmale der Blockchain-Technologie könnte letztendlich zur Adressierung von Geldwäschereirisiken beisteuern. Verteuerte Transaktionen und ein Verlust an Anonymität wären der zu bezahlende Preis.

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch

Pascal Sprenger
Partner,
Financial Services,
Regulatory & Compliance
+41 58 249 42 23
psprenger@kpmg.com

Franziska Balsiger
Director,
Financial Services,
Regulatory & Compliance
+41 58 249 68 77
fbalsiger@kpmg.com