

Blockchain und Geldwäscherei – Chancen und Risiken Blockchain-basierter virtueller Währungen in Bezug auf die Bekämpfung der Geldwäscherei



Davide Pinelli

Dr. iur. Davide Pinelli, Rechtsanwalt, MAS Economic Crime Investigation. Als Rechtsanwalt beratend und forensisch tätig bei Kaufmann Rüedi Rechtsanwälte AG in Luzern.

Jede neue Technologie besitzt sowohl Chancen als auch Risiken. Bei Kryptowährungen, welche auf der Blockchain basieren und allen offenstehen, werden von den verschiedenen nationalen sowie supranationalen Behörden besondere Missbrauchsrisiken für Geldwäscherei und Terrorismusfinanzierungen erblickt. Als Gründe dafür werden die im Vergleich zu anderen Zahlungsmethoden erhöhte Anonymität, die inhärent grenzüberschreitende Natur virtueller Währungssysteme und die bis heute damit verbundene Unsicherheit betreffend staatliche Regulationen erachtet. Vor diesem Hintergrund behandelt diese Masterarbeit folgende Fragestellungen: Können Blockchain-basierte virtuelle Währungen für Geldwäschereihandlungen missbraucht werden? Welches sind die technologieimmanenten Gründe, dass Blockchain-basierte virtuelle Währungen geeignete Instrumente darstellen, um Geldwäscherei zu begehen? Können die bestehenden rechtlichen Rahmenbedingungen zur Bekämpfung der Geldwäscherei in Bezug auf Blockchain-basierte virtuelle Währungen angewendet werden? Ist mehr Regulierung notwendig? Sind technische Massnahmen auf Seiten der Behörden notwendig? Wie sind die bestehenden Pflichten des GwG auf die Akteure Blockchain-basierter virtueller Währungen anzuwenden?

Blockchain-basierte virtuelle Währungen stellen Vermögenswerte dar und können daher auch für Geldwäschereihandlungen missbraucht werden. Der technologieimmanente Hauptgrund, dass Blockchain-basierte virtuelle Währungen für Geldwäscher interessant sind, liegt in der pseudonymen Haltung und Transaktionsmöglichkeit derselben. Dadurch ist die Identität der Währungsinhaberinnen und des Währungsinhabers nicht ohne grosse Anstrengungen erkennbar. Somit garantieren diese virtuellen Währungssysteme ein hohes Mass an Anonymität. Das ist auch ein Grund dafür, weshalb sie auch für kriminelle Tätigkeiten im Darknet verwendet werden.

Die bestehenden GwG Sorgfaltspflichten für Finanzintermediäre greifen nur für einen kleinen Teil der Akteure virtueller

Währungssysteme und bieten somit unzureichenden Schutz vor Geldwäschereihandlungen. Das Strafrecht ist zwar anwendbar, aber diesbezüglich ist die Ermittlung von Geldwäschereihandlungen aufgrund des durch die Pseudonymität garantierten Identitätsschutzes mit erheblichen Schwierigkeiten verbunden.

Um vorgenannte Schwierigkeiten einzudämmen werden in dieser Arbeit sowohl präventive als auch ermittlungstechnische Instrumente erarbeitet und vorgestellt.

Als präventives Mittel ist die Erweiterung der GwG Sorgfaltspflichten auf diverse Akteure im Bereich virtueller Währungssystemen vorgesehen. Konkret sollen die bestehenden GwG Sorgfaltspflichten auf Kryptobörsen (diese sind heute zum Teil erfasst, hier wird indes die explizite Nennung und Regelung der Ausnahme – reines Matching – im GwG verlangt), Anbieter von elektronischen Geldbörsen (Wallets) und Händlerinnen und Händler, welche Blockchain-basierte virtuelle Währungen als Zahlungsmittel annehmen, angewendet werden. Zudem soll die Etablierung des Blacklistings als präventives Mittel, um inkriminierte virtuelle Währungen sowie ihre Inhaberinnen und Inhaber zu isolieren nach dem Grundsatz «Verbrechen soll sich nicht lohnen» herbeigeführt werden.

Im Bereich der Ermittlungstechnik wird vorgeschlagen, dass die Strafverfolgungsbehörden automatische Datenanalyse und Datenverknüpfungssysteme, um die realen Nutzer der Transaktionsadressen (bspw. Bitcoin-Adressen) zu identifizieren, entwickeln bzw. entwickeln lassen. Hierzu können OSINT-Techniken verwendet werden. Allenfalls besteht auch die Möglichkeit, das neue OSINT-Portal des NDB (Art. 54 NDG) in diese Entwicklung miteinzubeziehen. Zudem sollen Blockchain-Explorationswerkzeuge beschafft oder entwickelt werden. Diese sollen es den Strafverfolgungsbehörden ermöglichen, sowohl die Transaktionshistorie zurückverfolgen und überschaubar aufzubereiten als auch Kryptozahlungen zu tracken, um somit an die Täter heranzukommen.

Weiterhin bestehen viele offene Fragen. Bspw. steht die Diskussion zwischen Transparenz auf der öffentlichen Blockchain und Datenschutz sowie Schutz der Privatsphäre, insbesondere im Rahmen von staatlicher Regulierung noch an. Des Weiteren sind auch praktische Fragen ungeklärt, wie: Wie lässt sich ermitteltes inkriminiertes Vermögen in der Praxis einziehen. Liegt der private Schlüssel vor, stellt die Einziehung kein Problem dar, da der private Schlüssel den Eigentumsbeweis ermöglicht und somit ein Transfer der inkriminierten virtuellen Währungen auf vom Staat kontrollierte Adressen möglich

wäre. Ist der private Schlüssel nicht auffindbar, so stellt sich die Frage, ob eine Ersatzforderung im Sinne von Art. 71 StGB möglich ist.

Auch wenn die Blockchain-gestützten virtuellen Währungen sich bis heute noch nicht auf breiter Ebene als Zahlungsmittel etabliert haben, geht von ihnen durchaus ein erhebliches Risiko für Geldwäschereihandlungen aus, welches nicht unterschätzt werden sollte.