BITCRIME

Verfolgung und Prävention organisierter Finanzkriminalität mit virtuellen Währungen - das deutsche Teilprojekt

Johanna Grzywotz johanna.grzywotz@fau.de Friedrich-Alexander-Universität Erlangen-Nürnberg
Olaf Markus Köhler olaf.koehler@wwu.de Westfälische Wilhelms-Universität Münster
Christian Rückert christian.rueckert@fau.de Friedrich-Alexander-Universität Erlangen-Nürnberg

bitcrime.de

Das Verbundprojekt BITCRIME

BITCRIME ist ein bilaterales, deutsch-österreichisches Forschungsprojekt, das sich mit der Prävention und Verfolgung organisierter Finanzkriminalität mit virtuellen Währungen beschäftigt. Die Nutzung solcher virtuellen Währungen im Sinne dezentraler kryptographischer Währungen wie Bitcoin nimmt stetig zu. Sie werden unabhängig von einer zentralen Instanz direkt zwischen den Nutzern gehandelt, was sie für Akteure der organisierten Finanzkriminalität attraktiv macht.

Bedrohung & Handlungsspielraum

Zur Feststellung der Bedeutung virtueller Währungen in der Kriminalität werden national und international vorliegende Informationen ausgewertet.

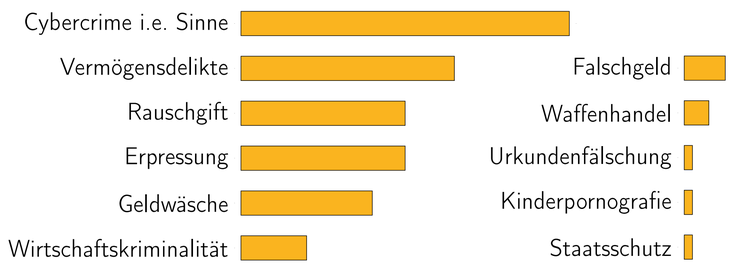

Abb. 1: Schätzung, Kriminalität mit virtuellen Währungen, interne Erhebung

Grundsätzlich sind virtuelle Währungen ein legales Konzept. Die Durchführung einer empirischen Nutzerstudie hat u.a. ergeben, dass 80% der Befragten Bitcoins zum Erwerb von Produkten oder Dienstleistungen nutzen.

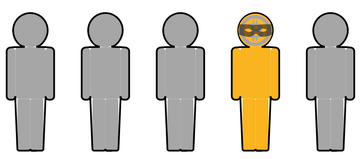

Abb. 2: Jeder fünfte gab an, Bitcoins für illegale Zwecke zu verwenden (N = 106).

Im Rahmen der strafrechtlichen Einordnung sind Tatbestände, die als Tatobjekt „Geld“ oder eine „Sache“ erfordern auszuschließen. Bei vielen Konstellationen dienen virtuelle Währungen als Geldersatz (Abb. 1). In den Blick genommen werden zudem neue Konstellationen, die durch die technische Funktionsweise von Bitcoins entstehen (z.B. (illegales) Bitcoin-Mining).

Technische Bestandsaufnahme

Zentral für Bitcoin ist die öffentliche zwischen allen Teilnehmern verteilte Transaktionshistorie, die sämtliche Transaktionen enthält und damit auch den Konsens der Teilnehmer über die aktuelle Bitcoin-Verteilung. Diese ist für jeden Teilnehmer zugänglich und wird automatisch untereinander verteilt.

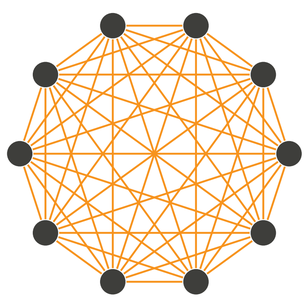

Abb. 3: P2P-Netzwerk

Eine Transaktion ist die Weiterleitung der technischen Zugriffsmöglichkeit bestimmter Bitcoins auf ein anderes Schlüsselpaar. Eine Transaktion besteht aus je einem oder mehreren Eingängen und Ausgängen. Ein Eingang verweist stets auf einen Ausgang und braucht diesen vollständig auf.

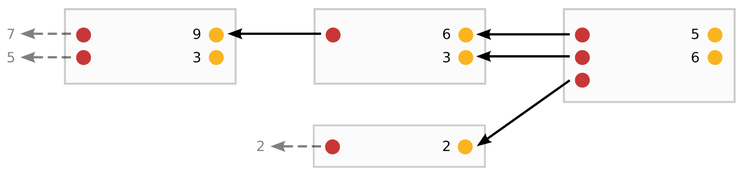

Abb. 4: Ausschnitt Transaktionsgraph, Zeit-/Bitcoinfluss von links nach rechts, ● Transaktionseingang, ● Transaktionsausgang, ← Ein-/Ausgangsverweise

Verfolgbarkeit von Transaktionen

Bezüglich ihrer Verfolgbarkeit unterscheiden sich Transaktionen im Bitcoin-System deutlich von typischen Bank-Transaktionen:

- Transaktionsparteien nicht ohne Weiteres identifizierbar
- Alle Transaktionen öffentlich
- Direkter Verweis zwischen Transaktionen (also implizit auch realen Geschäften) statt regelmäßiger Zusammenführung von Geldern auf Konten

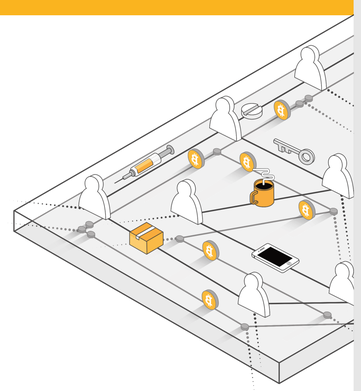

Abb. 5: Verknüpfung zwischen Bitcoin-Transaktionen und dahinterstehenden Geschäften nicht ohne Weiteres möglich
Gestaltung: goldmarie design

⇒ Ermittlungsansätze und Geldwäscheimplikationen

Es ergibt sich so eine unvollständige Information über den Handel zwischen Personen:

- Jeder kann beliebig viele Adressen nutzen
- Aufgrund diverser Dienstleister können BTC mehrerer Personen bei einer Bitcoin-Adresse hinterlegt sein

⇒ Transaktionen ≇ Geschäfte

Testumgebung & Fallstudien

Zum Zweck der Nutzbarmachung von technischen Indizien von virtuellen Währungen in der polizeilichen Praxis wird eine Testumgebung aufgebaut. Ein Bestandteil der Testumgebung ist ein Explorations-Werkzeug, mit dem sich die Transaktionsflüsse nachvollziehen und untersuchen lassen.

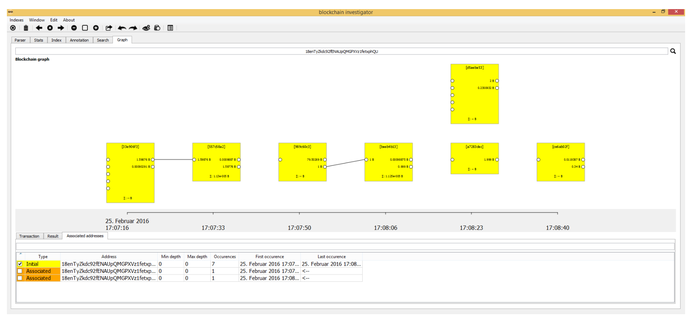

Abb. 6: Screenshot eines Prototypen des Explorations-Werkzeugs

Ein weiterer Teil der Testumgebung ist eine Spiegelung/Simulation der öffentlich genutzten virtuellen Währung. Dadurch können Bedarfsträger beispielsweise zu Schulungszwecken kostensparend mit „Spielgeld“ agieren.

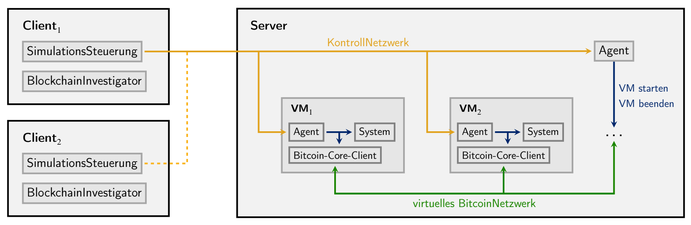

Abb. 7: Architektur der Testumgebung

Zugleich findet eine Fallstudie (anhand ausermittelter Fälle) statt, mit dem Ziel typische Modi Operandi zu identifizieren.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Juristische Grenzen Ermittlung

Dezentralität und Pseudonymität stellen die Strafverfolgungsorgane vor neue Herausforderungen. Die „klassischen“ Ermittlungsmethoden im Bereich der Finanzkriminalität, wie beispielsweise ein staatsanwaltschaftliches Auskunftsersuchen an die Bank, scheiden mangels zentraler verwaltender Stelle im Bitcoin-Netzwerk aus. Einen Ausweg kann das im Projekt entwickelte Transaktionshistorien-Explorations-Werkzeug bieten. Hierbei ist die Anwendbarkeit im Hinblick auf bereits vorhandene Eingriffsermächtigungsnormen der Strafprozessordnung zu überprüfen. Soweit die Schaffung neuer Eingriffsgrundlagen erforderlich sein sollte, werden Vorschläge zu Voraussetzungen und Grenzen solcher (vom Gesetzgeber zu schaffenden) Eingriffsbefugnisse unterbreitet.

Regulierungsansatz Sperrliste

Die Verwendung von Kryptowährungen soll für Kriminelle so unattraktiv wie möglich gemacht werden, ohne dabei zu stark in die Freiheit der legitimen Nutzer einzugreifen. Ein Ansatz dazu ist eine Transaktions-Sperrliste, an die Dienstleister gesetzlich gebunden wären. Diese soll den Tausch von Bitcoin mit Realwährung oder Waren verbieten, wenn sich diese bis zu einer gesperrten Transaktion zurückverfolgen lassen. In die Sperrliste aufgenommen würden Transaktionen, wenn feststeht, dass die Bitcoins durch eine Straftat erworben wurden.

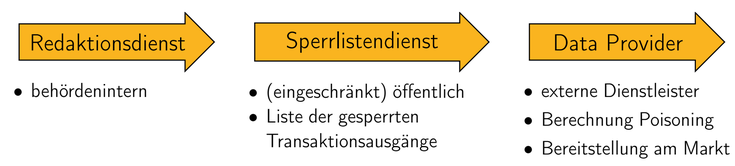

Abb. 8: Komponenten des Sperrlisten-Prozesses

Sperren müssen sich auf Folge-Transaktionen fortsetzen, da ansonsten das Umgehen der Sperrliste trivial ist. Dabei muss insbesondere auch der Fall der Vermischung von „legalen“ und „illegalen“ Bitcoins bedacht werden. Ein dazu untersuchter Ansatz ist die anteilige Sperrung der Bitcoins.

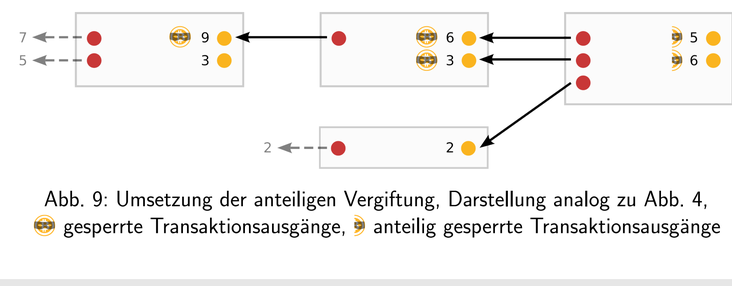

Abb. 9: Umsetzung der anteiligen Vergiftung, Darstellung analog zu Abb. 4, gesperrte Transaktionsausgänge, anteilig gesperrte Transaktionsausgänge

Rechtliche Umsetzung Sperrliste

Aufgrund der Neuartigkeit dieses Sperrlistenansatzes stellen sich zahlreiche rechtliche Herausforderungen. Im Zentrum steht dabei zunächst die grundsätzliche Vereinbarkeit eines solchen Regulierungskonzepts mit den Vorgaben des Grundgesetzes. Daneben müssen Lösungen für die Implementierung des Sperrlistenansatzes in die bestehenden Verwaltungsverfahren gefunden werden.