research institute

ERMITTLUNGSMAßNAHMEN UND KYC IN ANONYMEN KRYPTOWÄHRUNGEN

Walter Hötzendorfer
Senior Researcher
walter.hoetzendorfer@researchinstitute.at

Jan Hospes
Junior Researcher
jan.hospes@researchinstitute.at

Christof Tschohl
Scientific Director
christof.tschohl@researchinstitute.at

Markus Kastelitz
Senior Researcher
markus.kastelitz@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart Rights Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center

Das **Research Institute (RI)** ist ein Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.

Portfolio:

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **Smart Rights Consulting:** Beratung zu rechtlichen, technischen und organisatorischen Fragen des Datenschutzes
- **Schulungen**, auf Wunsch zugeschnitten auf Ihre Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit renommierten Partnern auf nationaler und internationaler Ebene.

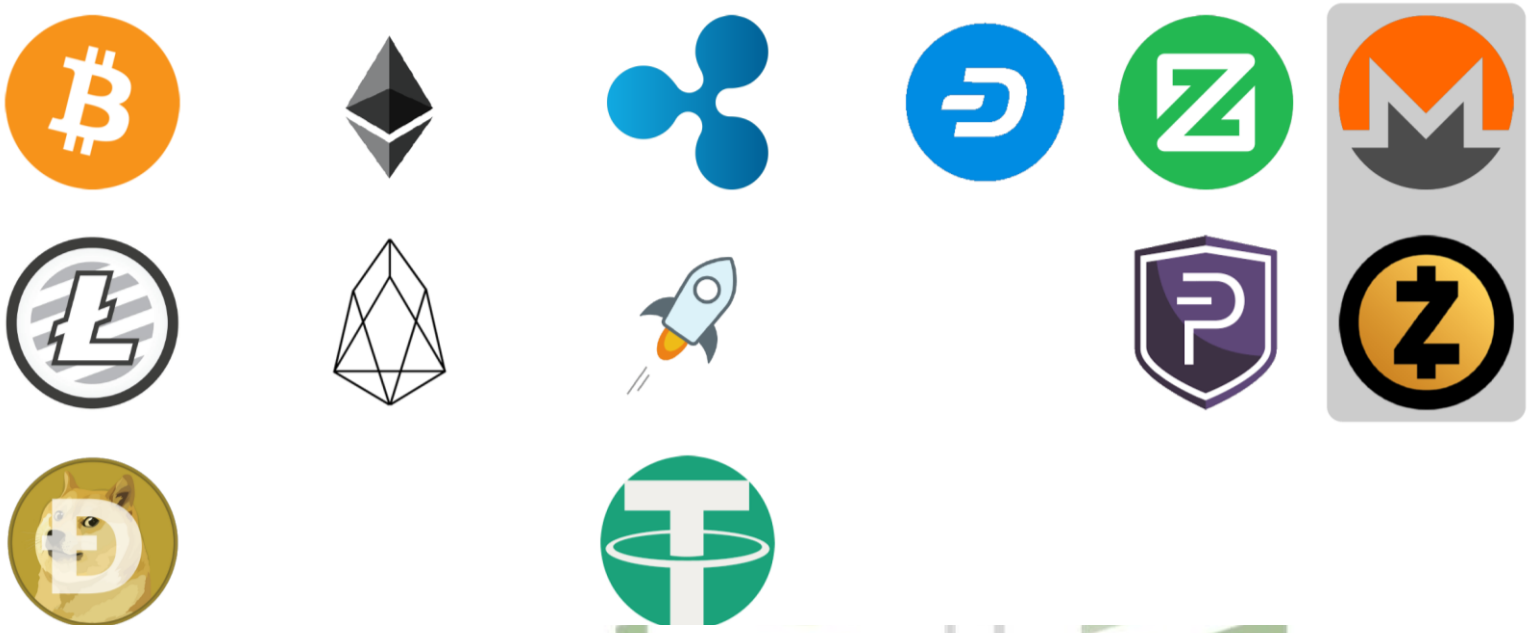
research institute

AGENDA

- Privacy Coins
- Das VIRTCRIME-Projekt
- KYC & AML
- Ermittlungsmaßnahmen

Privacy Coins

Altcoins: Kryptowährungen, welche die technische und wirtschaftliche Grundlage von Bitcoin übernehmen, jedoch unter anderem Namen auftreten und andere Funktionen bieten können.

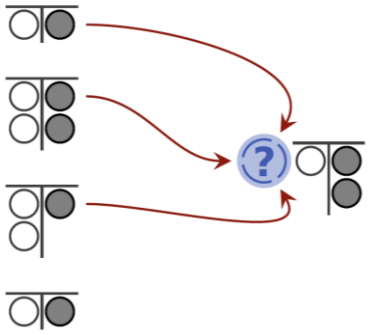


[Köhler 2018, VIRTCRIME Project]

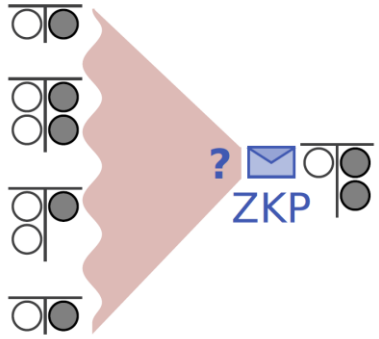
Privacy Coins

Privacy Coins: Altcoins welche sich besonderer Verfahren bedienen um die Identität der Nutzer zu schützen. Nach derzeitigem Wissensstand nicht nachverfolgbar. → Anonym & Fungibel

Monero: Ringsignaturen – Ein Pool mit mehreren Währungseinheiten wird durch mehrere Signatoren verifiziert. (Ringsize >7)



Zcash: Zero-knowledge proof – Die Blockchain enthält Beweise dafür, dass die Parteien bestimmte Voraussetzungen erfüllen



[Köhler 2018, VIRTCRIME Project]

DAS VIRTCRIME-PROJEKT

- Entwicklung neuer Algorithmen und Methoden für die Strafverfolgung in Kryptowährungen und Tor Hidden Services (Darknet-Marktplätzen)
- Finanziert vom Forschungsförderungsprogramm KIRAS (FFG, Bundesministerium für Verkehr, Innovation und Technologie)
- Konsortium:
  - AIT – Austrian Institute of Technology
  - Research Institute
  - Universität Innsbruck
  - VICESSE - Vienna Centre for Societal Security
  - Xylem - Science and Technology Management GmbH
  - Österreichisches Innenministerium
  - Österreichisches Finanzministerium

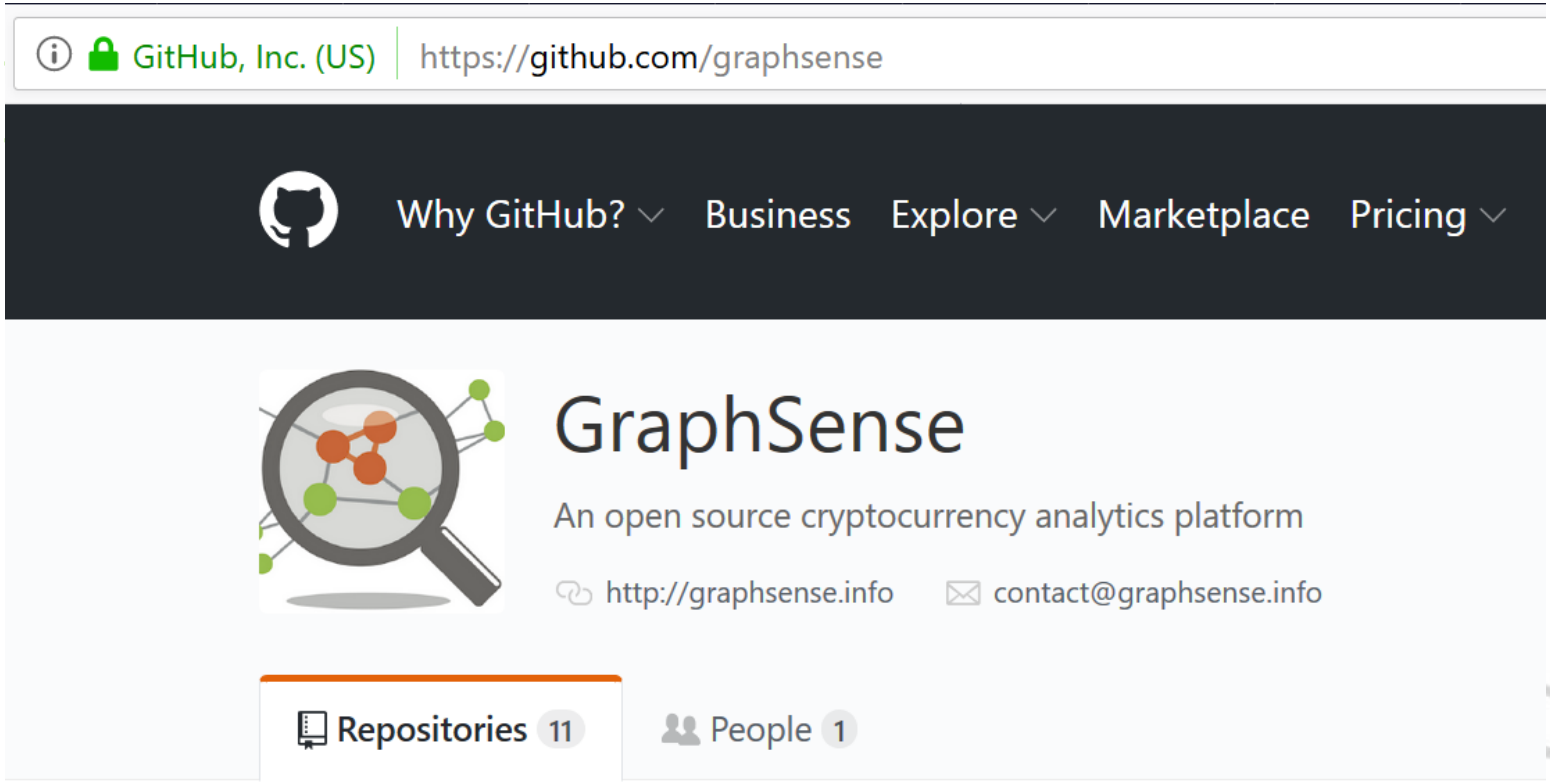
DAS VIRTCRIME-PROJEKT

Technische und juristische Forschung anhand von 7 Szenarien:

1. Regulierung und Registrierung von Krypto-Dienstleistern
2. AML & KYC-Pflichten (FATF, Geldwäscherichtlinien)
3. AML-Überprüfungen in der Praxis
4. Sicherstellung von Währungseinheiten
5. Transaktionsüberwachung mithilfe von Blockchain Analysetools zum Zweck der Verbrechensbekämpfung
6. Extraktion von gerichtlich verwertbaren Beweismitteln
7. Analyse von Darknet-Marktplätzen zum Zweck der Verbrechensbekämpfung

DAS VIRTCRIME-PROJEKT

- GraphSense: Skalierbare Analyseplattform für Kryptowährungen basierend auf Spark & Cassandra



KYC & AML

- FATF Leitlinien
  - Soft Law, faktisch sehr bedeutsam.
- 4. Geldwäscherichtlinie (RL 2015/849)
  - Grundsätze: Kundenindentifikation, Risikobewertung (Geschäftsfeld, Person…), Dokumentation, Personalschulung , Reporting
  - Keine Anwendbarkeit auf Kryptowährungen.
- BWG
  - FM-GwG steckt seinen Anwendungsbereich über § 1 BWG ab.
    - § 1 Abs 1 Z 6 BWG: „…Verwaltung von Zahlungsmitteln wie Kreditkarten, Bankschecks und Reiseschecks…“
    - Anwendbar auf Krypto-Dienstleister?

KYC & AML

- 5. Geldwäscherichtlinie (RL 2018/843)
  - Erweitert den Kreis der Verpflichteten.
  - Überschießende Regelungen nur im Rahmen des Art 114 EUV möglich.
  - Art 4 Abs 1: Umsetzungsperiode endet am 10.01.2020.

- Art 1/1/b RL 2018/843: Erweitert die Definition der "Finanzinstitute" des Art 3 RL 2015/849.
  - „g): Dienstleister, die virtuelle Währungen in Fiatgeld und umgekehrt tauschen;"
  - „h) "Anbieter von elektronischen Geldbörsen;"

  → Damit sind diese in vollem Umfang zu KYC / AML nach RL 2015/849 verpflichtet.

KYC & AML

- Virtuelle Währungen
  - Art 1/2/d/(18) RL 2018/843
    - Nicht zentral, öffentlich emittiert
    - Kein gesetzlicher Status
    - Akzeptanz als Tauschmittel
    - Elektronisch

- Handelsplattformen
  - KYC ist ab der „Begründung einer Geschäftsbeziehung“ durchzuführen. (Registrierungszeitpunkt?)
  - RL Anwendbar nur auf Handelsplattformen welche Krypto zu Fiat wechseln (=Gatekeeper).
  - Letztes FATF Update (10.2018) schließt Krypto zu Krypto sowie Vermittlertätigkeiten mit ein. (6. Geldwäscherichtlinie?)

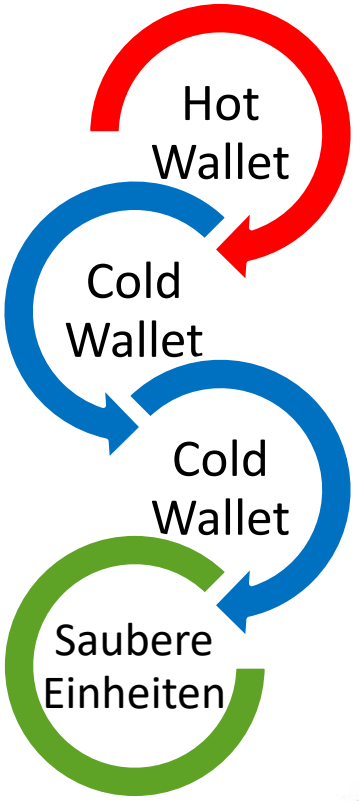
KYC & AML

- Wallets
  - Definiert in Art 1/2/d/(19) RL 2018/843:
    - *Anbieter von elektronischen Geldbörsen" einen Anbieter, der Dienste zur Sicherung privater kryptografischer Schlüssel im Namen seiner Kunden anbietet, um virtuelle Währungen zu halten, zu speichern und zu übertragen."*
  - Anwendbar auf Hot Wallet Provider.
  - Nicht anwendbar auf Cold Wallets, da kein Anbieter ersichtlich.

- Nutzer & Miner
  - Freiwillige Registrierungsmöglichkeit nach Art. 65 Abs. 1 RL 2018/843

KYC & AML

- Schlussfolgerungen & Aussichten
  - Anonyme Währungen: Lücken bei der Nachverfolgbarkeit werden selbst bei Umsetzung der FATF-Leitlinien weiterhin bestehen.
  - Umsetzung von RL 2018/843 ohne Bezug auf das BWG.
  - Verbot von Cold Wallets ist ein Eingriff in Art 10 EMRK und schwer exekutierbar.
  - Whitelisting ist eingriffsintensiv und kann Transaktionen Cold to Cold nicht erfassen.
  - Blacklisting kann in anonymen Währungen keinen Transaktionsbezug herstellen.



ERMITTLUNGSMAßNAHMEN

- Personenbezug anonymer Kryptowährungen
  - Art. 4 Z. 1 DSGVO, ErwGr. 26 der DSGVO
  - VfGH 15.6.2007, G 147/06 (Section Control)
    - "…wenn der einzige Sinn der Datenermittlung darin liege, diese Personen zu identifizieren…"

- Daher sind die Bestimmungen über besondere Ermittlungsmaßnahmen grds. beachtlich:
  - Observation: § 129 StPO, § 54 Abs 2 SPG, § 11 Abs 1 Z 1 PStSG
  - Verdeckte Ermittlung: § 129 Z 2 StPO, § 54 Abs 3 SPG, § 11 Abs 1 SPG
  - Rasterfahndung: § 141 StPO, § 53 Abs 1 SPG und § 10 Abs 2 PStSG

ERMITTLUNGSMAßNAHMEN

- § 109 Z 1 StPO: Sicherstellung
  - lit a: *„die vorläufige Begründung der Verfügungsmacht über **Gegenstände**“*
  - lit b: *„das vorläufige Verbot der Herausgabe von Gegenständen oder anderen Vermögenswerten an Dritte (**Drittverbot**) und das vorläufige Verbot der Veräußerung oder Verpfändung solcher Gegenstände und Werte“*

- Lücke: Keine Begründung der Verfügungsmacht bei unkörperlichen Sachen
  - Nur bewegliche, körperliche Sachen sind „Gegenstände“ – Cold Wallets?
  - Begriff der Vermögenswerte ist sehr weit, auch virtuelle Währungseinheiten.

- Sicherstellung bei einem Hot-Wallet Provider
  - Grundfall des Drittverbotes nach § 109 Z 1 lit b StPO.
  - Der Kreis der Drittverbotsverpflichteten ist nicht eingeschränkt.
  - Auskunftspflichten nach § 116 StPO lassen sich nicht auf Cryptocurrency Services umlegen, da BWG nicht anwendbar.

Privacy Coins & Regulation
Ermittlungsmaßnahmen

- Sicherstellung von Cold Wallets
  - Werden vom Nutzer Geführt. Dieser ist kein „Dritter“ iSd § 109 Z 1 lit b StPO.
- Kopien von Wallets:
  - Kopie einer Hot Wallet als Cold Wallet → Keine Exklusive Verfügungsmacht des Providers.
  - Kopie einer Cold Wallet als Cold Wallet → Physische Sicherstellung einer Wallet bleibt wirkungslos.
- Transfer auf behördliche Wallets:
  - § 111 StPO: „Jede Person, die Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet […] die Sicherstellung auf andere Weise zu ermöglichen“
  - Schwerer Eingriff in die Verfügungsmacht des Hot Wallet Providers, jedoch keine Durchführungsbestimmungen → Unzulässig aufgrund von§ 5 StPO, Art 18 B-VG
- Einfrieren von Transaktionen nach § 17 FM-GwG
  - UVS Wien GZ: 02/13/127/97 zum gleichlautenden § 41 Abs 3 idF vom 06.09.1998: Nur einzelne Transaktionen können Eingefroren werden.
  - Nutzer kann nicht von seiner Hot Wallet ausgesperrt werden. → Erstellung einer Cold Wallet auch nach Transaktionssperre möglich.

research institute

Weiterführende Literatur

- GraphSense: A Scalable Cryptocurrency Analytics Platform build on Apache Spark and Cassandra
  http://graphsense.info/
- Malte Möser et al.: An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, Volume 2018, Issue 3, pp 143-163
  https://arxiv.org/pdf/1704.04299.pdf
- Abraham Hinteregger, Monero Cross-Chain Traceability, Diploma Thesis, TU Wien
  https://www.ac.tuwien.ac.at/files/pub/hinteregger_18.pdf
- Ross Anderson et al.: Bitcoin Redux, WEIS 2018
  https://www.lightbluetouchpaper.org/2018/06/01/bitcoin-redux-crypto-crime-and-how-to-tackle-it/

research institute

ERMITTLUNGSMAßNAHMEN UND KYC IN ANONYMEN KRYPTOWÄHRUNGEN

Walter Hötzendorfer
Senior Researcher
walter.hoetzendorfer@researchinstitute.at

Jan Hospes
Junior Researcher
jan.hospes@researchinstitute.at

Christof Tschohl
Scientific Director
christof.tschohl@researchinstitute.at

Markus Kastelitz
Senior Researcher
markus.kastelitz@researchinstitute.at

Research Institute AG & Co KG
Digital Human Rights Center
Smart Rights Consulting

Annagasse 8/1/8
1010 Wien
www.researchinstitute.at

RECHTLICHE HINWEISE

Zweck: Dieses Dokument dient als Präsentationsunterlage.

Erstellt von den auf der Titelseite genannten AutorInnen

Disclaimer:

Dieses Dokument wurde auf Basis jener Informationen erstellt, die den AutorInnen als für den Zweck des Dokuments relevant erschien. Der Autor(en) übernimmt jedoch keine Haftung/Gewähr für Vollständigkeit und Richtigkeit der in diesem Dokument zur Verfügung gestellten Informationen. Die Angaben in diesem Dokument können von dem Empfänger nicht als Zusicherung oder Garantie verstanden werden. Die in diesem Dokument enthaltenen Informationen können sich im Laufe der Zeit verändern oder zum Übergabezeitpunkt bereits verändert haben. Technische Änderungen vorbehalten.