research institute

Privacy Coins & Regulation: The 5th EU Anti-Money Laundering Directive and its impact on post Bitcoin currencies

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

Research and Consulting at the Interface of Law, Technology and Society

Portfolio:

- **Research** on legal and technical aspects of data protection, privacy, security, cybercrime, technological impact assessment and internet policy
- **Smart Rights Consulting:** Consulting in data protection and related fields
- **Trainings** individually tailored to the needs of your organisation
- **Planning and realisation of multidisciplinary projects** with renowned partners on national and international level
- **Individual technological solutions** (in permanent co-operation with software developers)

research institute

Privacy Coins & Regulation
Agenda

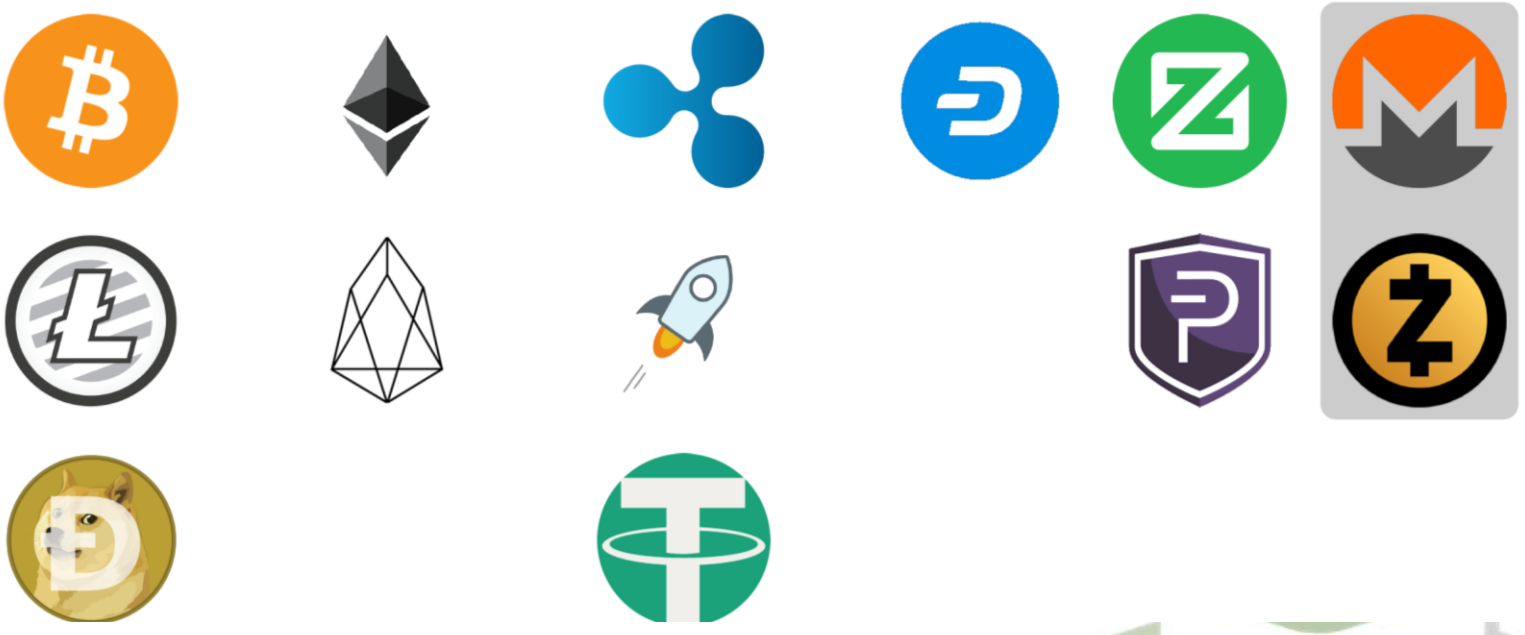
- Privacy Coins
- The VIRTCRIME Project
- KYC & AML
- Preliminary Freezing & Seizure
- Further Regulation

research institute

Privacy Coins & Regulation

Introduction

Altcoins: Cryptocurrencies that keep the essential functions of Bitcoin but add various other functions.

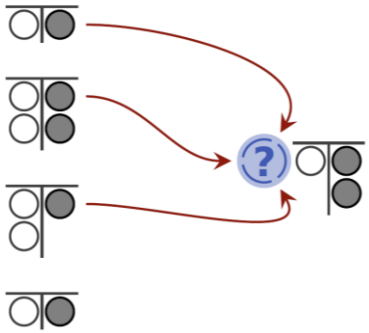


[Köhler 2018, VIRTCRIME Project]

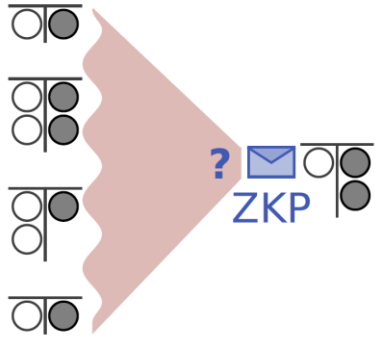
Privacy Coins & Regulation
Introduction

Privacy Coins: Altcoins that allow for anonymous transactions by using special verification systems

Monero: Ring signatures – Pool of currency units is verified by various signers. (Ringsize >7)



Zcash: Zero-knowledge proof – Prover does not convey content, but repeatedly proves that he knows a value *x* which is set by the verifier.



[Köhler 2018, VIRTCRIME Project]

research institute

Privacy Coins & Regulation
The VIRTCRIME Project

- Development of new algorithms and methods for the prosecution of criminal activity in cryptocurrencies and Tor hidden services (darknet markets)
- Funded by the Austrian research promotion programme KIRAS (FFG, Austrian Ministry for Transport, Innovation and Technology)
- Consortium:
  - AIT – Austrian Institute of Technology
  - Research Institute
  - University of Innsbruck
  - VICESSE - Vienna Centre for Societal Security
  - Xylem - Science and Technology Management GmbH
  - Austrian Ministry of the Interior
  - Austrian Ministry of Finance

KIRAS Sicherheitsforschung

research institute

PRIVACY COINS & REGULATION
THE VIRTCRIME PROJECT

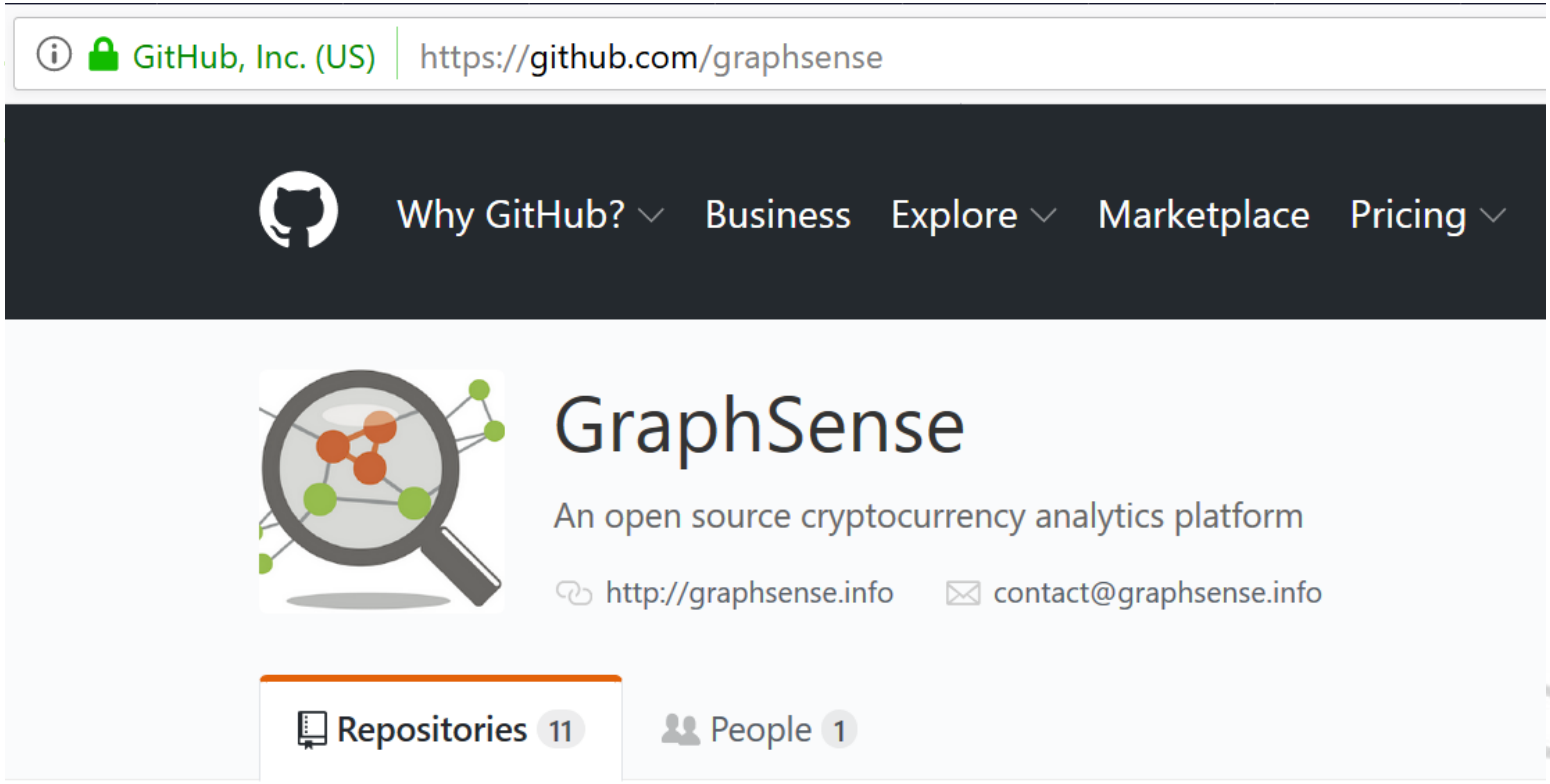
Technological and legal research along 7 scenarios:

1. Regulation and registration of cryptocurrency services
2. AML & KYC duties (FATF, AML Directives)
3. AML checks in practice
4. Seizure of cryptocurrencies
5. Transaction monitoring with blockchain analysis tools for the purpose of prosecution of criminal activities
6. Creating evidence which is admissible in court from transaction monitoring with cryptocurrency analysis tools
7. Crawling and analysis of criminal activity in darknet markets for the purpose of prosecution of criminal activities

research institute

PRIVACY COINS & REGULATION
THE VIRTCRIME PROJECT

- GraphSense: A Scalable Cryptocurrency Analytics Platform build on Apache Spark and Cassandra



research institute

PRIVACY COINS & REGULATION
KYC & AML

- Know your customer / Anti money laundering
- FATF Guidelines
- 4th Anti-Money Laundering Directive (EU 2015/849).
  - Includes various duties: Identification of customers, risk assessment, record keeping, staff training, reporting
  - Does not cover cryptocurrency services.
- 5th Anti-Money Laundering Directive (EU 2018/583)
  - Expands the scope of existing AML / KYC obligations.
  - Based on 114 TFEU: Gold-plating during implementation is possible only within strict boundaries.
  - Article 4/1: Implementation period ends on 10th Jan 2020.

PRIVACY COINS & REGULATION
KYC & AML

- Art 1/1/b EU 2018/583: Widens the definition of "financial institutions" of Art 3 EU 2015/849.
  - (g): *"providers engaged in exchange services between virtual currencies and fiat currencies;"*
  - (h): *"custodian wallet providers;"*

  → Said entities are obliged to fulfil the full scope of KYC / AML duties set up by EU 2015/849

- Custodian Wallet Providers
  - Defined in Art 1/2/d/(19) as:
    - *"an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies."*
  - Applicable to hot-wallet providers.
  - Not applicable to cold-wallets due to the lack of a service provider.
  - Hot-to-cold transactions render units of privacy coins untraceable.

- Exchange Services:
  - If applicable KYC has to be implemented "when starting a business relationship" (=date of user registration).
  - Applicable to exchanges that convert virtual currencies to fiat money and vice versa. (= Gatekeepers)
  - Not applicable to exchanges that convert virtual currencies to virtual currencies rendering these privacy coin markets untraceable.

research institute

Privacy Coins & Regulation
KYC & AML

- Notable possibilities of implementation.
  - Identification: Primarily personal appearance. If no office exists, other methods become available:
    - Presentation of an ID card during a video supported procedure.
    - Electronic ID
    - Qualified electronic signature.
    - Identification by a financial institution during the process of transferring funds to the user account.
  - Risk assessment - Risk based Approach:
    - Questioning during video supported procedure. → Privacy coins increase risk? → Question client about usage.
    - Outsourcing to financial institution by crypto service.
  - Risk assessment - Sanctions lists:
    - OFAC (Office of Foreign Assets Control) / EU
    - Look for overlaps between listed persons and clients.

research institute

Privacy Coins & Regulation
Preliminary Freezing & Seizure

- Austrian code of criminal procedure differentiates between:
  - Seizure of „items“: Physical, mobile things – direct seizure (e.g. the substrate of a cold-wallet).
  - Seizure of “other assets” – only at third parties (e.g. hot-wallet provider): broad catchall element – seizure only by prohibition of transfer to third party.

- Problem: Copies of a wallet might exist.
  - Seized funds might be transferred to different wallet.
  - Solution: Transfer of funds to a wallet of the law enforcing authority.
    - Unclear whether this is allowed under Austrian law.
    - Law states that “persons have to enable seizure” – but does this extend the forms of seizures stated above?

- §§ 78 – 81b Czech code of criminal procedure:
  - Same differentiation as in the Austrian code can be found.
  - However § 79e states clearly that transfer of funds is possible.

Privacy Coins & Regulation
Preliminary Freezing & Seizure

- Special problem due to password protected cold-wallets (e.g. „trezor“)
  - The accused has a constitutional right to remain silent & not to incriminate himself/herself (Art 6 ECHR).
    - ECHR: Saunders v. The United Kingdom
    - “does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers”
  - Coercive instruments may not be applied.

→ Funds may not be accessed.

Privacy Coins & Regulation
Preliminary Freezing & Seizure

- Price gain / loss after seizure
  - Austrian Supreme Court: „Forint case“ – Nominal value principle
  - Public Liability only concerning incurred damages (not potential): Plaintiff must prove that he would have sold the coins at a specific point in time.
  - Austrian Supreme court: Strict on prima facie evidence
    - No empirical principle can be formed towards sale at high price point.
    - Also no principle towards sale at stagnating prices (HODL).
  - Placement of a sale order on an exchange as persuasive evidence.

research institute

Privacy Coins & Regulation
Further Regulation

- Blacklisting / Whitelisting
  - Marking of incriminated (=blacklisting) or certified (=whitelisting) cryptocurrency units.
  - Units gain or loose value upon being marked. → Encroachment of the basic right to property.

  → Private coins are fungible, no encroachment of the right to property possible.

- Restrictions to publishing of cold wallets
  - Encroachment of right to freedom to receive and impart information.

research institute

Privacy Coins & Regulation
Further Reading

- 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 Vienna
  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

Privacy Coins & Regulation: The 5th EU Anti-Money Laundering Directive and its impact on post Bitcoin currencies

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