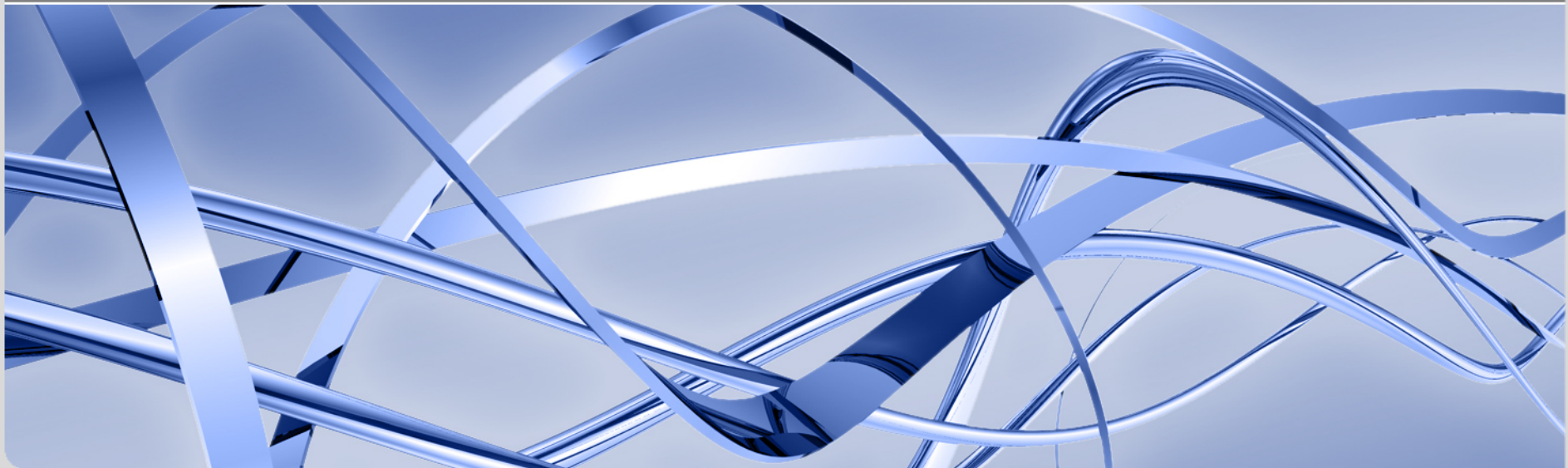


Symposium On Post-Bitcoin Cryptocurrencies

# **Chances and Risks of Cryptocurrencies' Transparency – A Legal Perspective**

Vienna, 19 October 2018

Dr. Paulina Jo Pesch – [paulina.pesch@kit.edu](mailto:paulina.pesch@kit.edu)



## Background



Law studies at University of Münster (with focus on information, telecommunication and media law)



PhD thesis on cryptocurrency transactions under German civil law



\*



Research assistant at Department of Information Systems (University of Münster); coordinator of the German BITCRIME project



Post-doc at Karlsruhe Institute of Technology; lead of the legal research in the EU follow-up project TITANIUM

# Agenda

- I. Cryptocurrency Basics
- II. Data Protection
- III. Criminal Investigations
- IV. Regulation



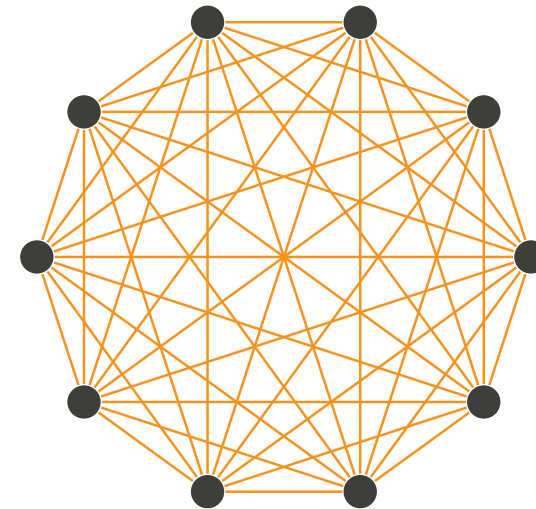
# I. Cryptocurrency Basics

Decentral online transaction systems

Peer-to-peer networks

Anyone can **join or leave the system anytime** and **create addresses** ( $\approx$  accounts)

Participants themselves **verify transactions**



Valid transactions are fed into the **distributed ledger** (most systems use a **blockchain**) that... is **public**,  
is decentrally consented on and **largely immutable**,  
contains the system's **full transaction history**,

# I. Cryptocurrency Basics

## What can be apparent from a cryptocurrency blockchain?

Transactions, including sender's and receiver's **addresses and amount transferred**

Implied by transactions: all **addresses' balances**

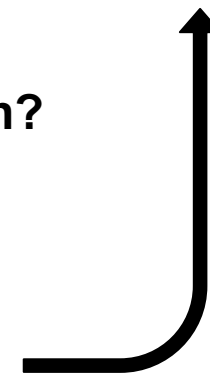
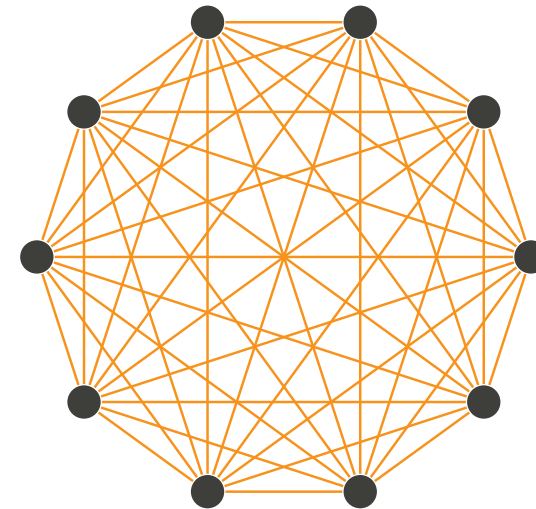
Through cryptocurrency analytics heuristics: clusters of **addresses likely to be owned by same entity**

Maybe **additional information**, e.g. smart contracts

## What is not apparent from a cryptocurrency blockchain?

**Identities** of address owners

The **data processing** on **participants' local computers / in the peer-to-peer network**



## II. Data Protection Law

### Blockchain data = (partially) personal data

Defined as any information relating to an identified or **identifiable** natural person

Art. 4 I Nr. 1 GDPR, Art. 3 (1) Dir. (EU) 2016/680 (LED)

- Considering all **means reasonably likely to be used** Recital (26) GDPR
- Maybe by use of **additional information; with assistance of others**

In more detail: *CJEU – C-582/14*, paras 42 ff., NJW 2016, 3579, 3581

### Blockchain data

Addresses = pseudonyms

Identification of address owners by use of **additional information**

Sometimes **publicly available**, e.g. blog or fora posts

## II. Data Protection Law

### Decentralized data processing in cryptocurrency systems

**Transparency** of **blockchain data** ≠ transparency of **data processing**

Art. 5 I a GDPR; Recital (26) LED

Responsible **controllers**: network participants Art. 4 I Nr. 7 GDPR, Art. 3 (9) LED

- Mostly unknown
- Little influence of single participants
- Rules on joint control does not fit decentralized systems Art. 26 GDPR, Art. 21 LED

No **recitification/erasure** due to blockchains' immutability Art. 16 f. GDPR, Art. 16 LED

**Data transparency** runs counter to principle of **data minimisation** Art. 5 I c GDPR

**Public blockchains particularly risky and not sufficiently covered by GDPR**

# III. Criminal investigations

## Example: Drug trading

**Browse by category**

- ▶ **Drugs 73822**
  - ▶ Barbiturates 39
  - ▶ Benzos 3590
  - ▶ Cannabis 23236
  - ▶ Dissociatives 2723
  - ▶ Ecstasy 10745
  - ▶ Opioids 5080
  - ▶ Prescription 4285
  - ▶ Psychedelics 5051
  - ▶ RCs 690
  - ▶ Steroids 3405
  - ▶ Stimulants 11992
  - ▶ Weight loss 157
- ▶ Digital Goods 58250
- ▶ Drugs 73822
- ▶ Drugs Paraphernalia 289
- ▶ Services 5461
- ▶ Other 6571

---

**Exchange**

BTC	1.0
mBTC	1000.0
BCH	14.6
USD	6443.3
EUR	5597.0
GBP	4919.8
CAD	8423.6
AUD	9095.2
mBCH	14635.0
BRL	24464.8
DKK	41771.0
NOK	52875.6
SEK	57996.9
TRY	37992.9
CNH	44717.8
HKD	50703.9
RUB	427445.6
INR	476971.9

**Drugs (73822)**

Filter


Ships to  Ships from  Escrow  Category  Cryptocurrency

Price  Searchtext  Sort by  Vendor

**Apply filter**

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17  
18 19 20 ... 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 →


**\*\*5 Pack of THC Infused 300 mg Brownies \*\***



**฿0.00403**  
Houseofdank2.0 (780) (4.62★)  
US → WW

**Order**


**Armodafinil (Waklert) 150mg - 200x**



**฿0.0266**  
MS-FI (240) (4.60★)  
WW → WW

**Order**

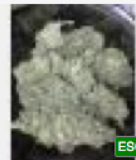
**FLASH SALE! SHARDY Ketamine - 28g (S Isomer)**



**฿0.0739**  
Kreams (520) (4.77★)  
GB → WW, EU

**Order**


**2 LB Green Crack {\$2,500}**



**฿0.403**  
CaptainCannabis (1000) (4.91★)  
US → US

**Order**


**Oxycontin 40mg x 10 Tablets \$40 each**



**฿0.0645**  
purepharm (1050) (4.99★)  
US → US

**Order**

**10X 2MG XANAX BARS PHARMACY GRADE (FREE NDD)**



**฿0.00317**  
F1RSTCLASS (3450) (4.95★)  
GB → GB, EU

**Order**



### III. Criminal investigations

#### Example: Ransomware, e.g. Locky

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

[http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. <http://twbers4hmi6dx65f.tor2web.org/> [REDACTED]

2. <http://twbers4hmi6dx65f.onion.to/> [REDACTED]

3. <http://twbers4hmi6dx65f.onion.cab/> [REDACTED]

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>

2. After a successful installation, run the browser and wait for initialization.

3. Type in the address bar: [twbers4hmi6dx65f.onion](http://twbers4hmi6dx65f.onion), [REDACTED]

4. Follow the instructions on the site.

!!! Your personal identification ID: [REDACTED] !!!

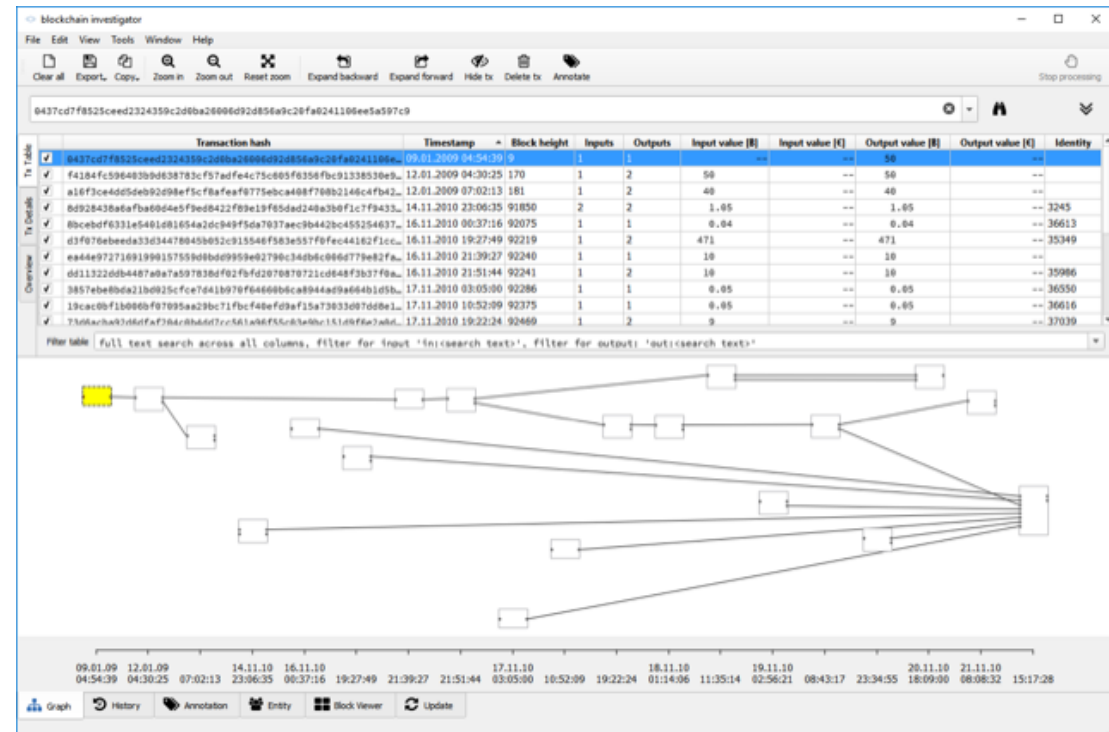
# III. Criminal investigations

What can investigators do?

Tracing **transaction flows**

**Identifying** address owners with additional information

**Clustering** addresses likely to be owned by same entity



## III. Criminal investigations

### Legal boundaries

**Legal basis** required

- **General clauses**: only low-intensity interferences with fundamental rights
- High-intensity interference requires **specific legal basis**

Compliance with **data protection** law – Directive (EU) 2016/680



# IV. Regulation

## The AML Directive (EU) 2018/843

19.6.2018 EN Official Journal of the European Union L 156/43

DIRECTIVES

**DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
of 30 May 2018  
amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU  
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank <sup>(1)</sup>,

Having regard to the opinion of the European Economic and Social Committee <sup>(2)</sup>,

Acting in accordance with the ordinary legislative procedure <sup>(3)</sup>,

Whereas:

- (1) Directive (EU) 2015/849 of the European Parliament and of the Council <sup>(4)</sup> constitutes the main legal instrument in the prevention of the use of the Union financial system for the purposes of money laundering and terrorist financing. That Directive, which had a transposition deadline of 26 June 2017, sets out an efficient and comprehensive legal framework for addressing the collection of money or property for terrorist purposes by requiring Member States to identify, understand and mitigate the risks related to money laundering and terrorist financing.
- (2) Recent terrorist attacks have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations. Certain modern technology services are becoming increasingly popular as alternative financial systems, whereas they remain outside the scope of Union law or benefit from exemptions from legal requirements, which might no longer be justified. In order to keep pace with evolving trends, further measures should be taken to ensure the increased transparency of financial transactions, of corporate and other legal entities, as well as of trusts and legal arrangements having a structure or functions similar to trusts (similar legal arrangements), with a view to improving the existing preventive framework and to more effectively countering terrorist financing. It is important to note that the measures taken should be proportionate to the risks.
- (3) The United Nations (UN), Interpol and Europol have been reporting on the increasing convergence between organised crime and terrorism. The nexus between organised crime and terrorism and the links between criminal and terrorist groups constitute an increasing security threat to the Union. Preventing the use of the financial system for the purposes of money laundering or terrorist financing is an integral part of any strategy addressing that threat.

<sup>(1)</sup> OJ C 459, 9.12.2016, p. 3.  
<sup>(2)</sup> OJ C 34, 2.2.2017, p. 121.  
<sup>(3)</sup> Position of the European Parliament of 19 April 2018 (not yet published in the Official Journal) and decision of the Council of 14 May 2018.  
<sup>(4)</sup> Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

KYC, monitoring,  
and reporting obligations  
for exchanges and  
wallet providers

### Weaknesses:

- ineffective, **circumvention possible**
- weakens **data protection**
- tailored to **conventional financial sector**

## IV. Regulation

### Tailored Approach: Transaction Blacklisting

Mandatory list of **illicit transactions**

Intermediaries **demande to reject cryptocurrencies** originating from listed transactions

No circumvention by **follow-up transactions** due to transparency of transaction history

Does not require identification of concerned address owners (**data protection friendlier**)

Objective: decreasing or even eliminating criminal offenders' financial benefits → **preventive effect**

### Requirements

Compatibility with **fundamental rights**

**International** adoption



## V. Conclusion

Cryptocurrencies' transparency has implications for  
**data protection, criminal investigations, and regulation**

**Trade-off** between users' privacy and investigators'/regulators' capabilities

### **Open questions:**

How much privacy is possible?

How much transparency is desirable?

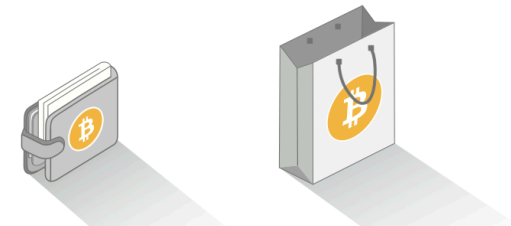
What should law stipulate?

```

TTTTTTTTTTTTTTTTTTTTTTTTTHHHHHHHHH      HHHHHHHHH      AAA      NNNNNNNN      NNNNNNNKKKKKKKK      KKKKKK
T:::::::::::::::::::::TH:::::::::H      H:::::::::H      A:::A      N:::::N      N:::::NK:::::K      K:::::K
T:::::::::::::::::::::TH:::::::::H      H:::::::::H      A:::A      N:::::N      N:::::NK:::::K      K:::::K
T:::::TT:::::TT:::::THH:::::::::H      H:::::HH      A:::::A      N:::::N      N:::::NK:::::K      K:::::K
TTTTTT T:::::T TTTTTT H:::::H      H:::::H      A:::::A      N:::::N      N:::::NKK:::::K      K:::::KKK
      T:::::T      H:::::H      H:::::H      N:::::N      N:::::N      K:::::K      K:::::K
      T:::::T      H:::::HHHHH:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      T:::::T      H:::::HHHHH:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      T:::::T      H:::::HHHHH:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      T:::::T      H:::::H      H:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      T:::::T      H:::::H      H:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      TT:::::TT      HH:::::H      H:::::HH      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      T:::::T      H:::::H      H:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      T:::::T      H:::::H      H:::::H      A:::::A      A:::::A      N:::::N      N:::::N      K:::::K:::::K
      TTTTTTTTTT      HHHHHHHHH      HHHHHHHHHAAAAAA      AAAAAANNNNNNN      NNNNNNNKKKKKKKK      KKKKKK

YYYYYYY      YYYYYYY      OOOOOOOO      UUUUUUUU      UUUUUUUU
Y:::::Y      Y:::::Y      OO:::::OO      U:::::U      U:::::U
Y:::::Y      Y:::::Y      OO:::::OO      U:::::U      U:::::U
Y:::::Y      Y:::::YO:::::OO      U:::::OU:::::U      U:::::UU
YYY:::::Y      Y:::::YYYO:::::O      O:::::O      U:::::U      U:::::U
      Y:::::Y      Y:::::Y      O:::::O      O:::::O      U:::::D      D:::::U
      Y:::::Y:::::Y      O:::::O      O:::::O      U:::::D      D:::::U
      Y:::::Y:::::Y      O:::::O      O:::::O      U:::::D      D:::::U
      Y:::::Y      O:::::O      O:::::O      U:::::D      D:::::U
      Y:::::Y      O:::::O      O:::::O      U:::::D      D:::::U
      Y:::::Y      O:::::O      O:::::O      U:::::D      D:::::U
      Y:::::Y      O:::::O      O:::::O      U:::::U      U:::::U
      Y:::::Y      O:::::OOO:::::O      U:::::UUU:::::U
      YYYYY:::::YYYY      OO:::::OO      UU:::::UU
      Y:::::Y      OO:::::OO      UU:::::UU
      YYYYYYYYYYYY      OOOOOOOO      UUUUUUUU

```



Grafiken: goldmarie design (Münster)