Karlsruher Institut für Technologie

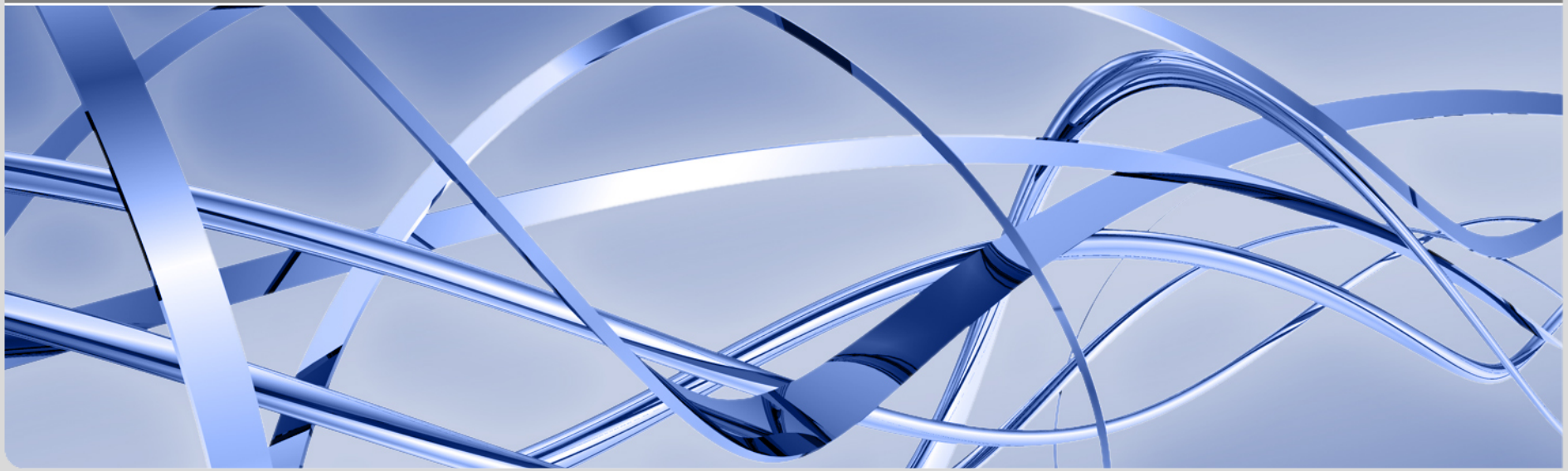
Anwendertag IT-Forensik

Ermittlungen in der Blockchain –

Verfolgung von Straftaten mit Bitcoins und Alt-Coins

26. September 2017

Dr. Paulina Jo Pesch



About

Karlsruher Institut für Technologie

§ Jura-Studium in Münster (Schwerpunkt: Informations-, Telekommunikations- und Medienrecht)

Dissertation zur vertragsrechtlichen Behandlung von Bitcoin-Transaktionen

Wissenschaftliche Mitarbeiterin am Institut für Wirtschaftsinformatik; Koordinatorin des BMBF-geförderten Projekts BITCRIME*

Wissenschaftliche Mitarbeiterin am Karlsruher Institut für Technologie; Leitung der datenschutzrechtlichen Forschung im EU-geförderten Folgeprojekt TITANIUM**

* https://www.bitcrime.de/deutschland/ ** http://www.darkreading.com/threat-intelligence/international-consortium-launches-to-prevent-criminal-use-of-dark-web-and-virtual-currencies/d/d-id/1328917

Agenda

I. Cryptocoin-Basics
II. Ausgangslage
III. Strafverfolgungsansatz
IV. Prozessrechtliche Grenzen
V. Herausforderungen

I. Cryptocoin-Basics – Bsp. Bitcoin

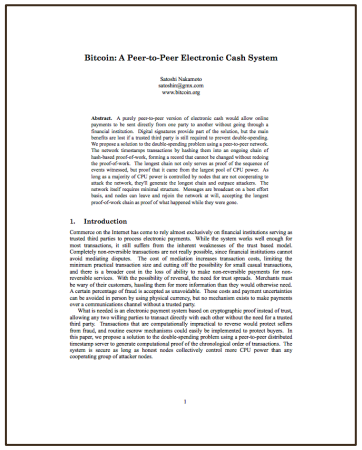
Dezentrale Online-Transaktionen direkt zwischen den Nutzern, also unabhängig von Notenbanken, Staaten und Kreditinstituten

Einsatz von **Kryptographie**

Erstes **Blockchain**-basiertes System

2008 von „Satoshi Nakamoto“ vorgestellt

2009 implementiert



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

I. Cryptocoin-Basics – Bsp. Bitcoin

Dezentrales Online-Transaktions-Netzwerk

Adressen **auf Basis öffentlicher Schlüssel**

Asymmetrische Kryptographie in Bitcoin

= Digitale Signaturen
Ziel: Authentisierung

≠ Verschlüsselung!
Ziel: Geheimhaltung

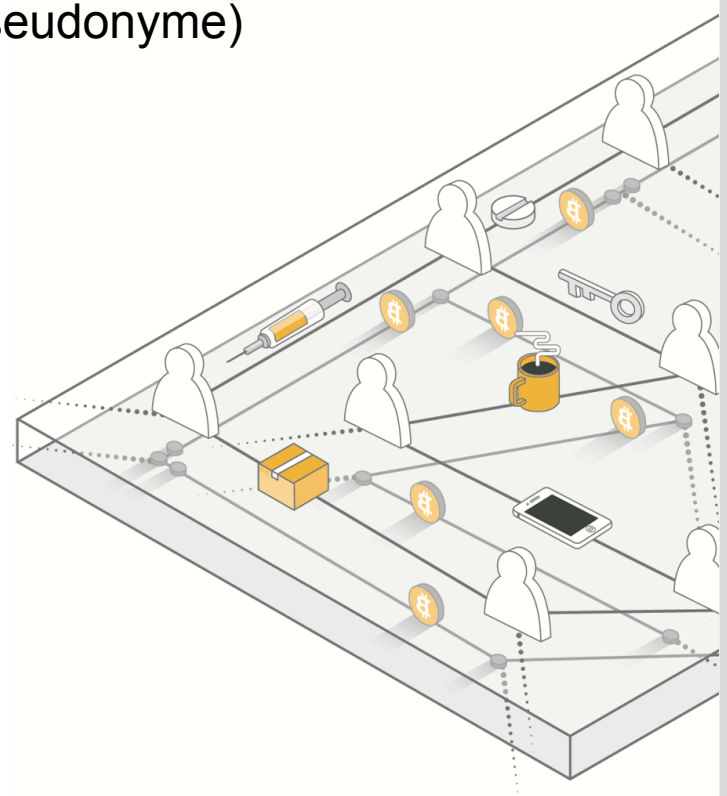
Transaktionen

- Digital signiert
  mit dem passenden privaten Schlüssel
- Abgesendet an das Netzwerk
- Überprüft von anderen Nutzern
- Eingetragen in die **öffentliche**, dezentral gespeicherte **Blockchain**
  Zweck: Verhinderung des doppelten Ausgebens (Double Spending), Wertschöpfung

I. Cryptocoin-Basics – Bsp. Bitcoin

– Eingetragen in die **öffentliche**, dezentral gespeicherte **Blockchain**

Extreme **Transparenz** des Bitcoin-Systems
Einsatz von Kryptographie **≠ Verschlüsselung**/Geheimhaltung
Bitcoin **≠ anonym** (Adressen = Pseudonyme)



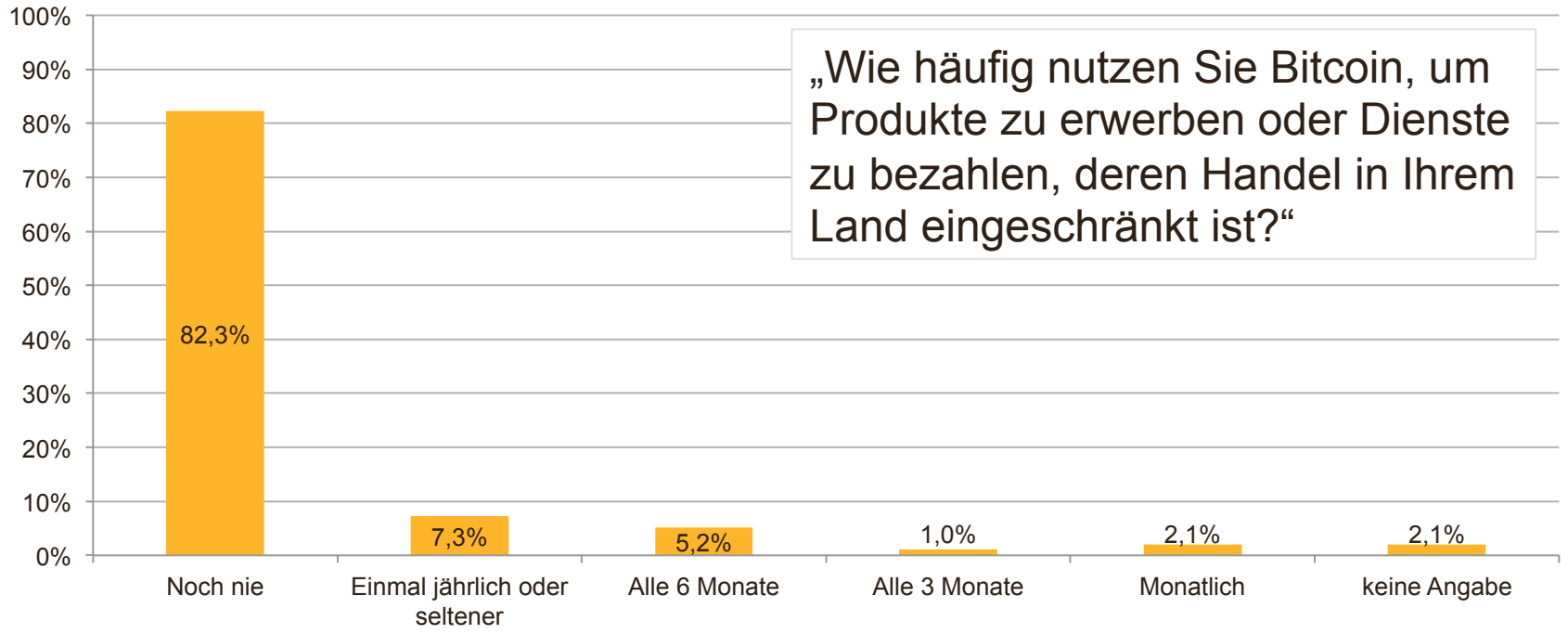
II. Ausgangslage – Darknet-Handel

II. Ausgangslage – Darknet-Handel

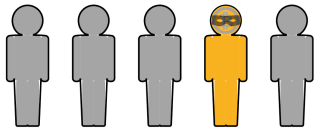
Market	Uptime Status	URL	Open registration?	Offers Multisig?	Had Security Issues?!	Active warnings	Commission	Vendor Bond	2FA	Forced Vendor PGP
Alphabay	98.60%	http://pwoah7foa6au2pul.onion/register.php?aff=41211	Open	✓	☺	None	3.5%	200$	✓	✓
Dream Market	98.58%	http://lchudifyeqm4ldjj.onion/?ai=1675	Open	✗	☺	None	4%	0.25BTC	✓	✗
Valhalla (Silkkitie)	97.98%	http://valhallaxmn3fydu.onion/register/E3we	Ref Only	✓	☺	None	2-5%	1BTC	✓	✓
Hansa Market	99.43%	http://hansamkt2rr6nfg3.onion/affiliate/110	Open	✓	☺	None	3%	0.3BTC	✓	✓
Outlaw Market	98.83%	http://outfor6jwcztwbpd.onion/index.php?id=xx1	Open	✓	☺	None	3%	0.1 - 2BTC	✓	✓
Acropolis Market	99.76%	http://acropol4ti6ytzeh.onion/auth/register/BCBTNUERXY	Referral	✓	☺	None	3.5%	100$	✓	✓

Quelle: https://www.deepdotweb.com/dark-net-market-comparison-chart/

II. Ausgangslage



Fast jeder fünfte der befragten Bitcoin-Nutzer hat Bitcoins für **illegale Zwecke** benutzt.



BITCRIME-Nutzerumfrage (2015), N = 106

II. Ausgangslage

Strafbarkeit nach dem StGB („keine Strafe ohne Gesetz“)

Problem: Rechtsnatur von Bitcoin

Tatbestände, die...

... Geld oder Sachen (= körperliche Gegenstände) als Objekte erfordern

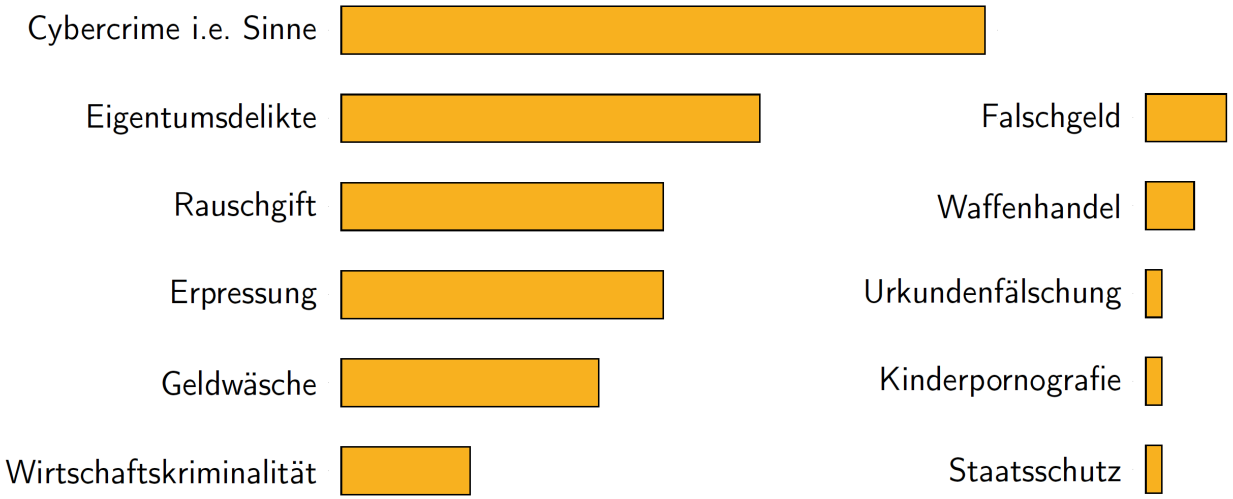
z.B. Geldfälschung, Diebstahl → (–)

... typischer-, aber nicht notwendigerweise (etwa) Geld zum Gegenstand haben

z.B. Geldwäsche, Erpressung, Betäubungsmitteldelikte → (+)

II. Ausgangslage

Erfahrungen bei Polizeidienststellen des Bundes und der Länder



BITCRIME-Auswertung (2015).

II. Ausgangslage

Bsp. Ransomware

Cybercrime i.e. Sinne 

Erpressung 

II. Ausgangslage

Bsp. Ransomware

Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde

```
!!! 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/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/66CCAB8A005BF0AF
    2. http://twbers4hmi6dx65f.onion.to/66CCAB8A005BF0AF
    3. http://twbers4hmi6dx65f.onion.cab/66CCAB8A005BF0AF

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/66CCAB8A005BF0AF
    4. Follow the instructions on the site.

!!! Your personal identification ID: 66CCAB8A005BF0AF !!!
```

II. Ausgangslage

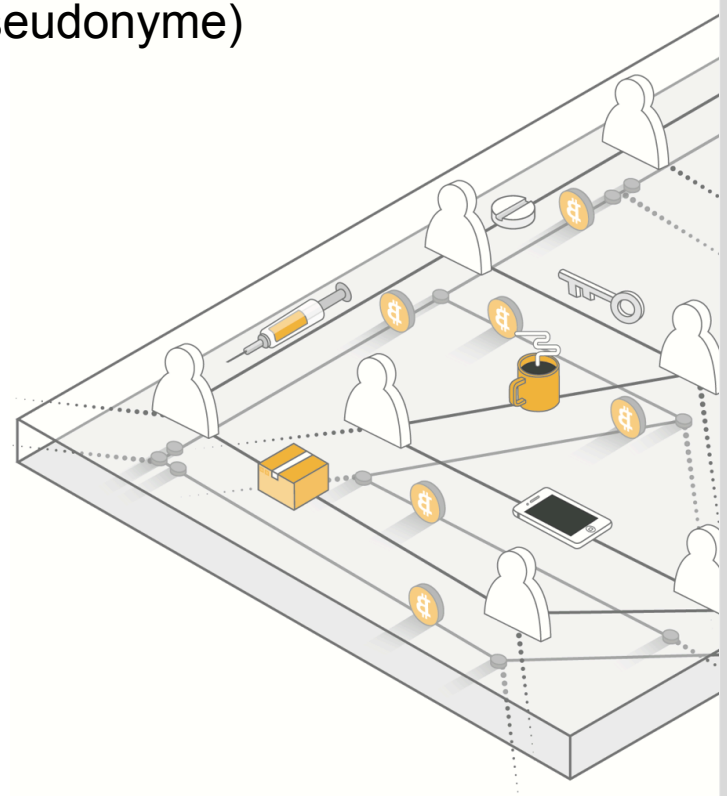
Bsp. Ransomware

Bitcoin als Lösegeld: WannaCry-Ransomware greift Systeme weltweit an

III. Strafverfolgungsansatz

– Eingetragen in die **öffentliche**, dezentral gespeicherte **Blockchain**

Extreme **Transparenz** des Bitcoin-Systems
Einsatz von Kryptographie **≠ Verschlüsselung**/Geheimhaltung
Bitcoin **≠ anonym** (Adressen = Pseudonyme)

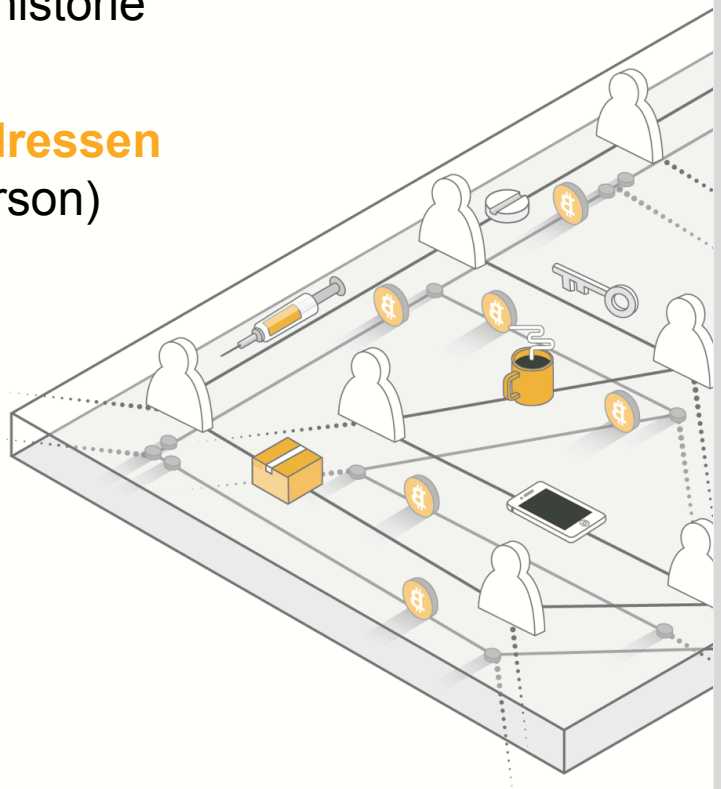


III. Strafverfolgungsansatz

– Eingetragen in die **öffentliche**, dezentral gespeicherte **Blockchain**

(1.) Ermöglicht jedermann die **Nachverfolgung jedes Bitcoin-Betrags** durch seine gesamte Transaktionshistorie

(2.) Ermöglicht jedermann das **Clustern von Adressen** (mit hoher Wahrscheinlichkeit derselben Person) und mit den nötigen Zusatzinformationen auch die **Identifizierung** von Nutzern



III. Strafverfolgungsansatz

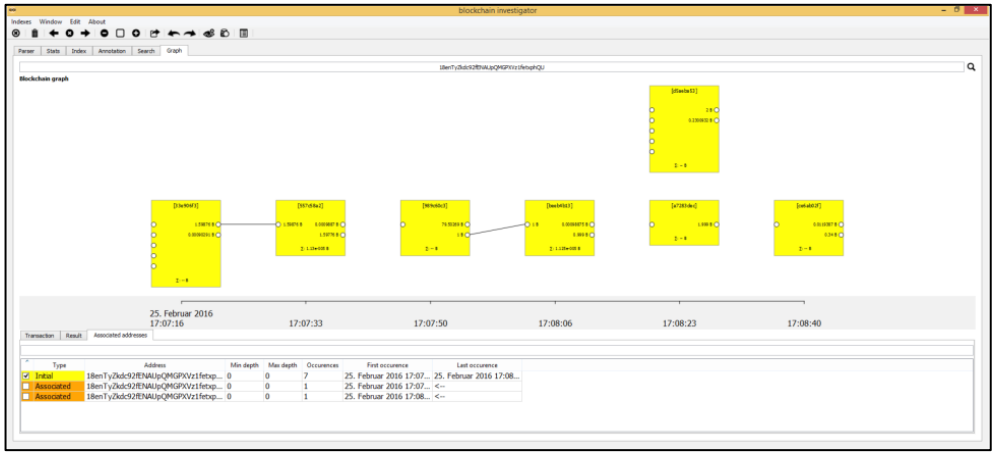
BITCRIME-Ermittlungswerkzeug

Simulationsumgebung: Simulation des Bitcoin-Systems

- Transaktionen zu Trainingszwecken
- Reproduktion und Untersuchung echter Fälle
- Vorteile: Keine beobachtbaren Vorgänge in der echten Blockchain, Datensparksamkeit, keine Transaktionskosten

dence Blockchain investigator

- Verfolgung von Transaktionsflüssen
- Nähere Analyse der Transaktionsflüsse, z.B. Clustern von Adressen



IV. Prozessrechtliche Grenzen

Datenschutz(-grundrecht)

Schutz personenbezogener Daten

= Informationen, die sich auf eine identifizierte oder **identifizierbare** natürliche Person beziehen

Mehr zu den technischen Grundlagen und datenschutzrechtlichen Fragen der Blockchain-Technologie: **CAST-Workshop „Blockchain – Sicherheit und Anwendungen“**, 26.10.2017, Fraunhofer SIT

Potentielle Personenbeziehbarkeit von Blockchain-Daten (mit **Zusatzinformationen/Hilfe Dritter**)

Verarbeitung nur unter Beachtung datenschutzrechtlicher Anforderungen, insb. nur mit **Rechtsgrundlage**

→ für Ermittlungen: Ermächtigungsgrundlagen der Strafprozessordnung

IV. Prozessrechtliche Grenzen

Ermächtigungsgrundlage

– Telekommunikationsüberwachung („TKÜ“), 100a StPO?
(–) Blockchain ≠ nicht-öffentliche Kommunikation

– Ermittlungsgeneralklauseln, 161, 163 StPO

→ rechtfertigen **nur Eingriffe geringer Intensität**

Grund: Grundrechtseingriff; intensive Grundrechtseingriffe bedürfen detaillierte Regelung der Befugnisse und ihrer Grenzen

Problem: Grenzziehung

Jedenfalls nicht zulässig: Dauerüberwachung des Gesamtsystems

Jedenfalls zulässig: Durch Verdacht begründetes gezieltes Suchen nach bestimmten Transaktionen/Adressen

V. Herausforderungen

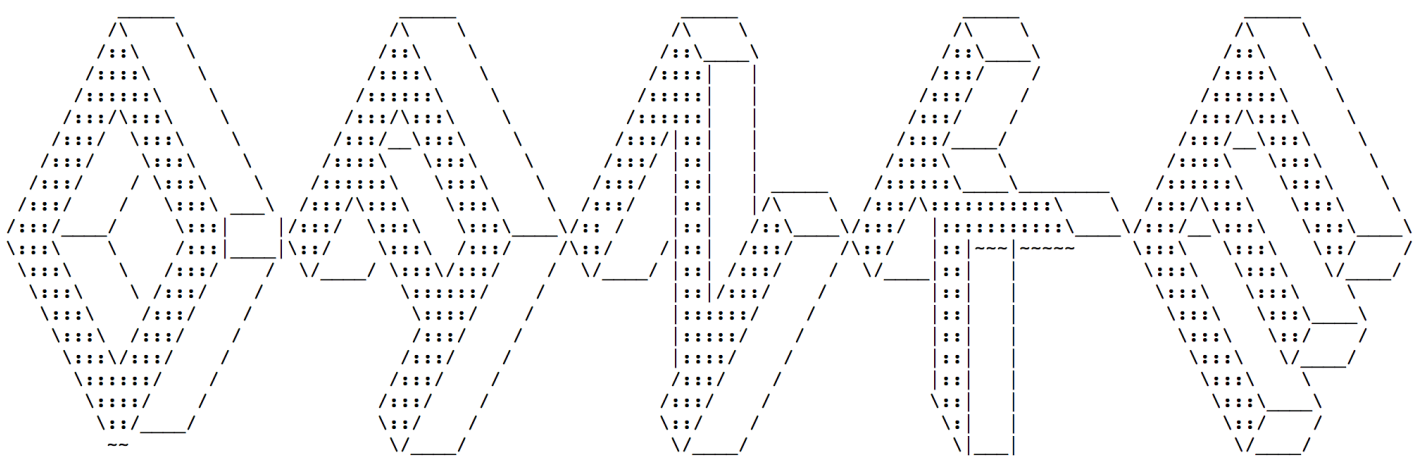
Heuristiken im steten **Wandel**

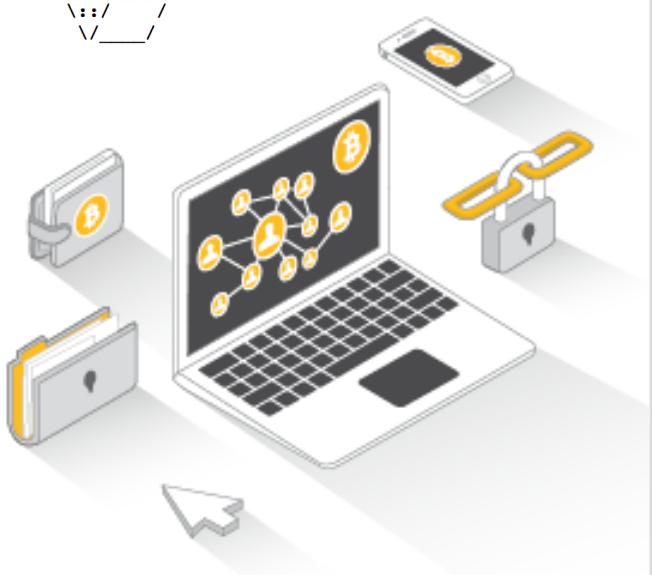
Eingeschränkte Transparenz **anonymerer Cryptocoin-Systeme**

Rechtsrahmen für Strafverfolgung **international kaum harmonisiert**

Unzureichende Compliance vieler am Markt verfügbarer Dienste und Datenbanken

[…]





paulina.pesch@kit.edu

Graphiken: goldmarie design (Münster)

BITCRIME wurde gefördert ...

im Rahmen der Förderrichtlinie „Zivile Sicherheit – Schutz vor organisierter Kriminalität“ des Bundesministeriums für Bildung und Forschung

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Gemeinsamer Sprecher und Sprecher des deutschen Teilprojektes:
Prof. Dr. Rainer Böhme
Westfälische Wilhelms-Universität Münster
E-Mail: rainer.boehme@uni-muenster.de