Bitcoin & Co-Kryptowährung

Fachhochschule Güstrow

Heiko Franke, Wirt.-Inf., M.A. in Education

Agenda

in 30 Minuten!!

1 Ausgangs-Situation

„Unbekannte in Kolumbien möchten

4 kg Heroin verkaufen.

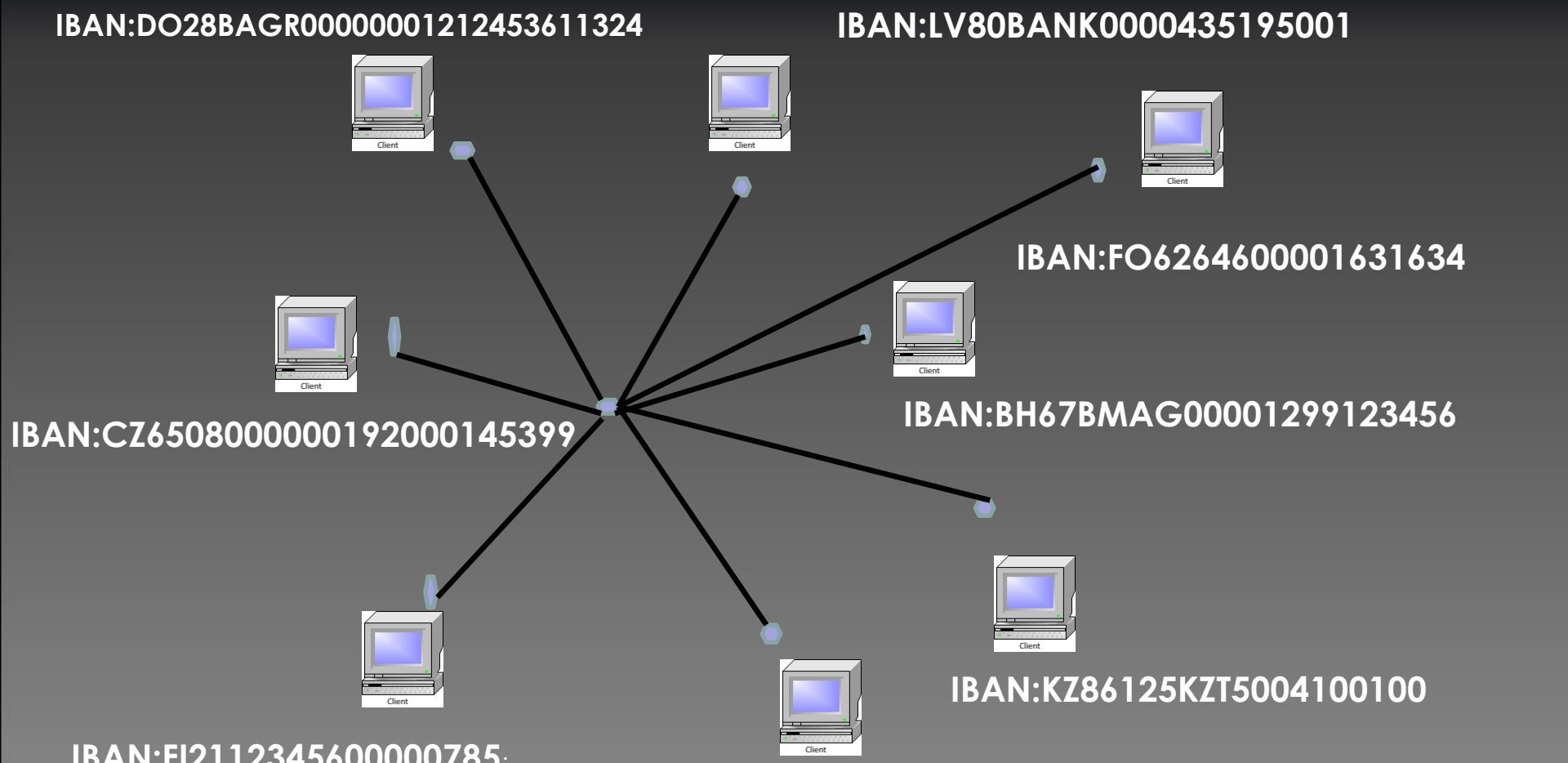
Ein Käufer ist bereits gefunden.

Der Käufer möchte schnell zahlen und anonym bleiben. “

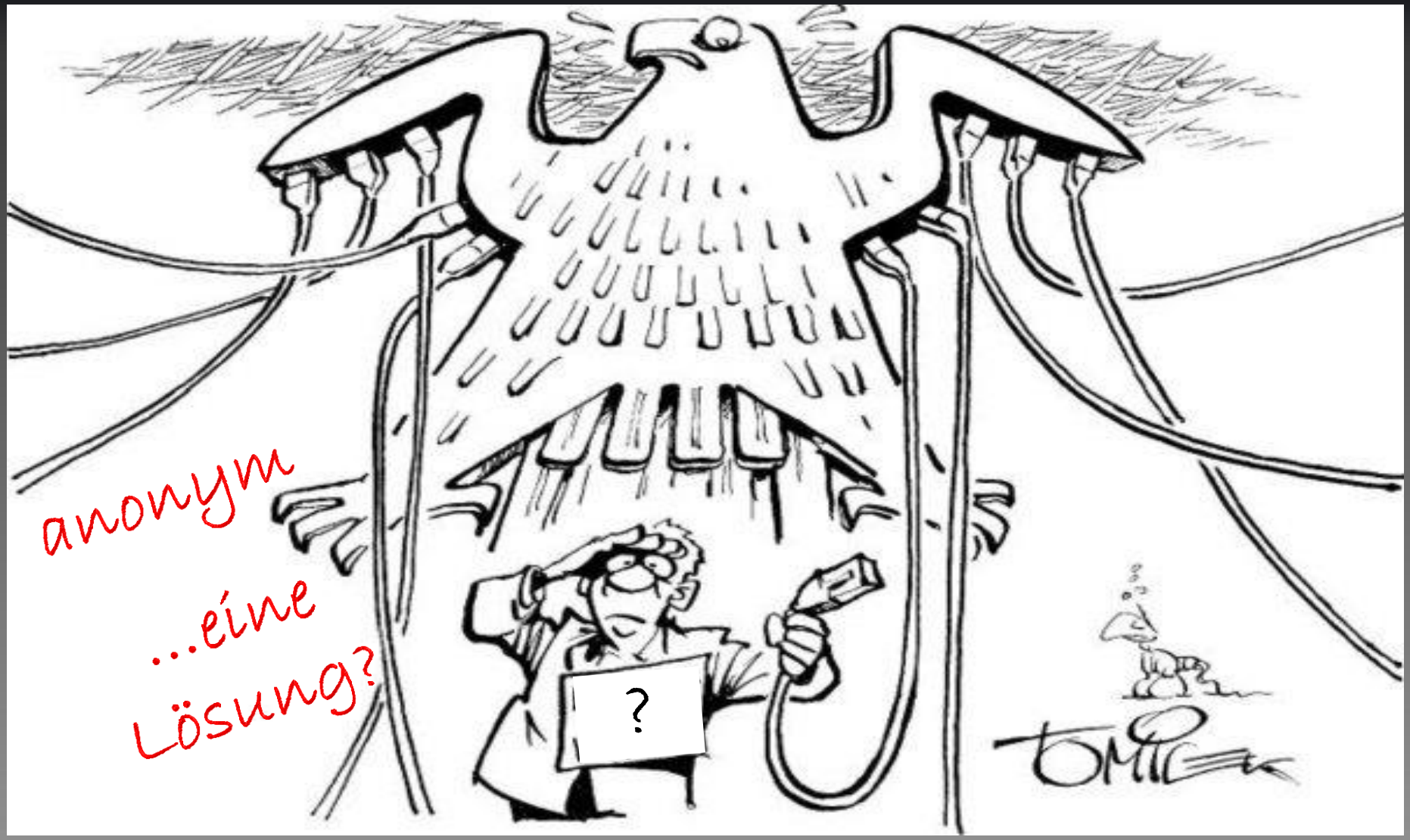
1.1 klassische Zahlungsarten

https://www.cartoonstock.com/

1.2 Topologie klass. Zahlungsarten



1.3 Anwendbarkeit



https://www.onetz.de/deutschland-und-die-welt-r/vermischtes-de-welt/trojaner-netzwerkkarikatur-tomicek-m206770,1068511.html

2 Lösung - Kryptoware

„Darknet-Marktplatz AlphaBay setzt auf anonyme Kryptowährung Monero“

29. August 2016 , 19:21 Uhr

http://www.zdnet.de/88277669/darknet-marktplatz-alphabay-setzt-auf-anonyme-kryptowaehrung-monero/?inf_by=5963cae8681db8544f8b4729

„Das besondere an einer Kryptowährung ist ihre Anonymität der User. Keine Bank oder ein Staat hat einen Einfluss auf die Kryptowährung. Eine Kryptowährung ist dadurch gekennzeichnet“

27.03.2017

http://erfolgreicher.eu/kryptowaehrung/

2.1 Kryptowährungen

Rang	Währung	Symbol	Start	Mining
1	Bitcoin	BTC	2009	SHA-256
2	Ethereum	ETH	2015	Ethash
3	Ripple	XRP	2013	nein
4	Litecoin	LTC	2011	Scrypt
5	Ethereum Classic	ETC	2015	Ethash

Autorisierung erfolgt über:

öffentlicher Schlüssel → Verschlüsselung → bitcoin-Adresse

1BvayiASVCmGmg4WUJmyRHoNevWWo5snqC.

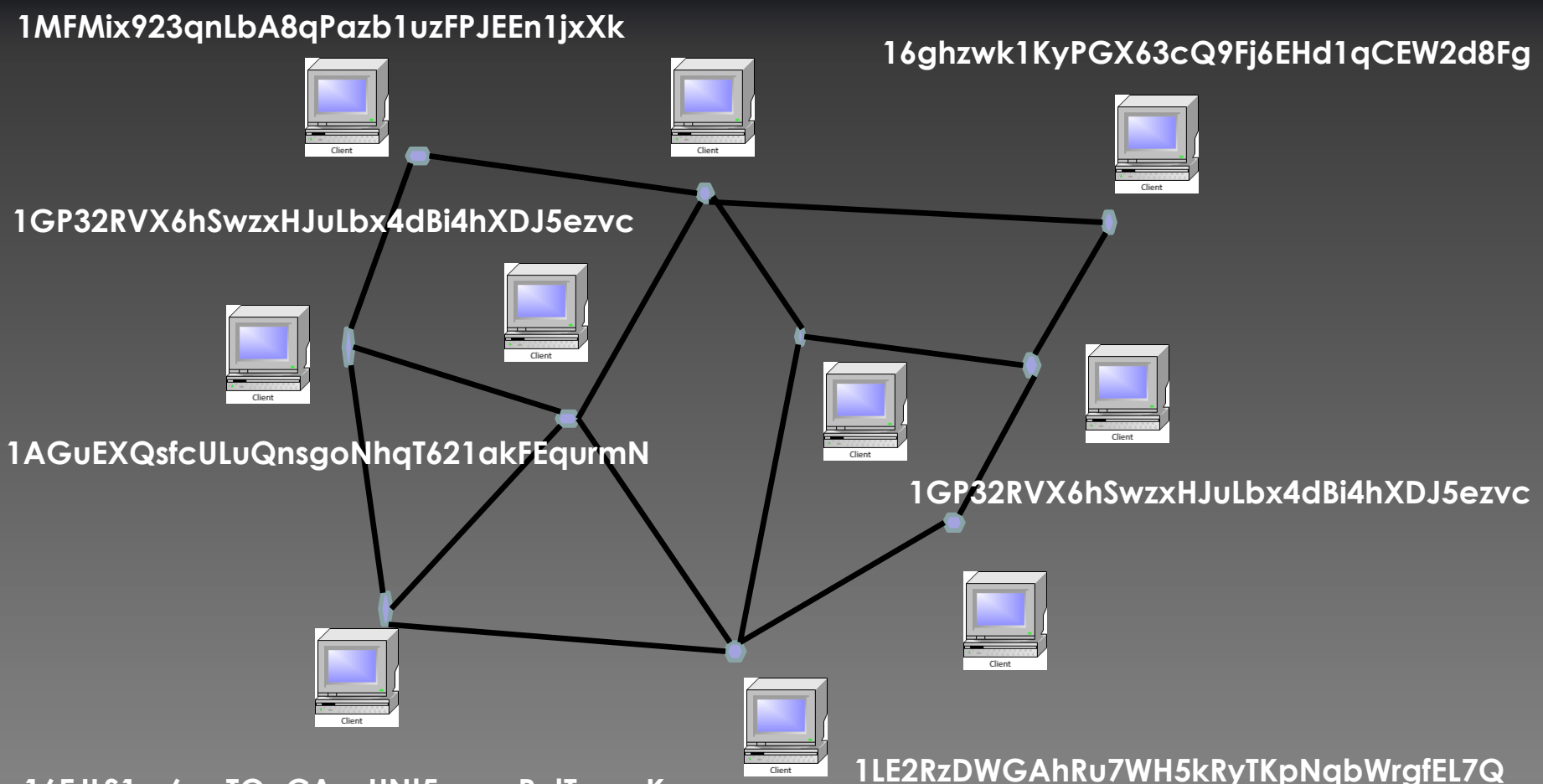
privater Schlüssel – digitale Autorisierung:

L2UO jQYm2WBC4r2V AfZqmH3iTd4HpF91chEWKqwZihZj3DWp4

Der öffentlicher Schlüssel lässt sich aus dem privaten Schlüssel errechnen.

Quelle: https://www.bitaddress.org

2.2 Topologie der Kryptowährung



2.3 Bestandteile von Kryptowährungen

klassisch

Tresor

* Bar-Geld
* IBAN
* TANs

krypto

Wallet(s)

* verwaltet digitales „Geld“
* verwaltet private Schlüssel
* verwaltet die Bitcoinadresse(n)

2.4 Bestandteile von Kryptowährungen

klassisch

Buchungsregister

* Registrierungen
* Kontostand
* regelt den Ablauf

krypto

Blockchain

* reg. alle Transaktionen
* liegt jedem Client vor
* persistend

2.5 Bestandteile von Kryptowährungen

klassisch

Revisor

* prüft die Buchung
* autorisiert die Buchung
* schreibt den Buchungssatz

krypto

Miners

* Verifizierung des Blocks
* Blockbildung f. Buchungen
* Block-Konsistenz

2.6 Bestandteile von Kryptowährungen

Bestandteile des Bitcoinhandlings sind somit…

Blockchain:	**Buchungsregister**
Wallet:	**Tresor**
Miner:	**Revisor**

2.7 Beschreibungen

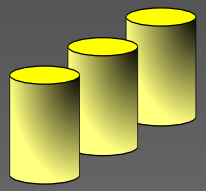
Wallet, weniger als ein Tresor?

* einfache Software auf Client \Web-Basis
* meist ohne Benutzeranmeldung
* vorgefertigte Eingabemasken
* keine verschlüsselte Ablage in der Software
* auch mobil einsetzbar.

Ein Wallet ist nicht Voraussetzung für eine Transaktion.
Der private Schlüssel und die bitcoin-Adresse kann auch auf Papier festgehalten werden.
(1BvayiASVCmGmg4WUJmyRHoNevWWo5snqC)
(L2UO jQYm2WBC4r2VAfZqmH3iTd4HpF91chEWKqwZihZj3DWp4) ☺

2.8 Beschreibungen

Blockchain, mehr als nur ein Buchungsregister



* stellt „Geldwerte“ als Datenbereiche bereit
* stellt Besitzverhältnisse da
* Buchungen werden als Block registriert
* etwa alle 10 min. entsteht ein neuer Block

Ein Bitcoin ist keine Datei auf der Festplatte
sondern lediglich ein Eintrag in der Blockchain.

2.9 Beschreibungen

Miner, mehr als nur ein Revisor?

* komplexe Algorithmen zur Erstellung
* jeder Teilnehmer kann minig betreiben
* Sourcecode in unterschiedlichen Sprachen
* Voraussetzung für Konsistenz u. Integrität

3 Bitcoins näher betrachtet

Transaktion mit Bitcoins…

1. Max möchte an Katrin „Geld“ überweisen.
2. Katrin teilt Max ihren bitcoin – Adresse mit.
   (1BvayiASVCmGmg4WUJmyRHoNevWWo5snqC)
3. Max teilt nun dem Netzwerk mit, dass er Bitcoins überweisen möchte.
4. Max signiert mit seinem privaten Schlüssel
   (L2UO jQYm2WBC4r2V AfZqmH3iTd4HpF91chEWKqwZihZj3DWp4)
   die Buchung und sendet diese ab.
   (Mit Software auf dem PC oder einem Web-Client)

Folge:

Überprüfung des Kontostandes in der Blockchain
Verifizierung an Hand des privaten Schlüssels.

3 Bitcoins näher betrachtet

Die Buchung befindet sich jetzt in einem schwebenden Zustand!

Einsatz des Miners

5. **Berechnung des nächsten(neuen) Blocks, anhand der letzten Blockinformation.**

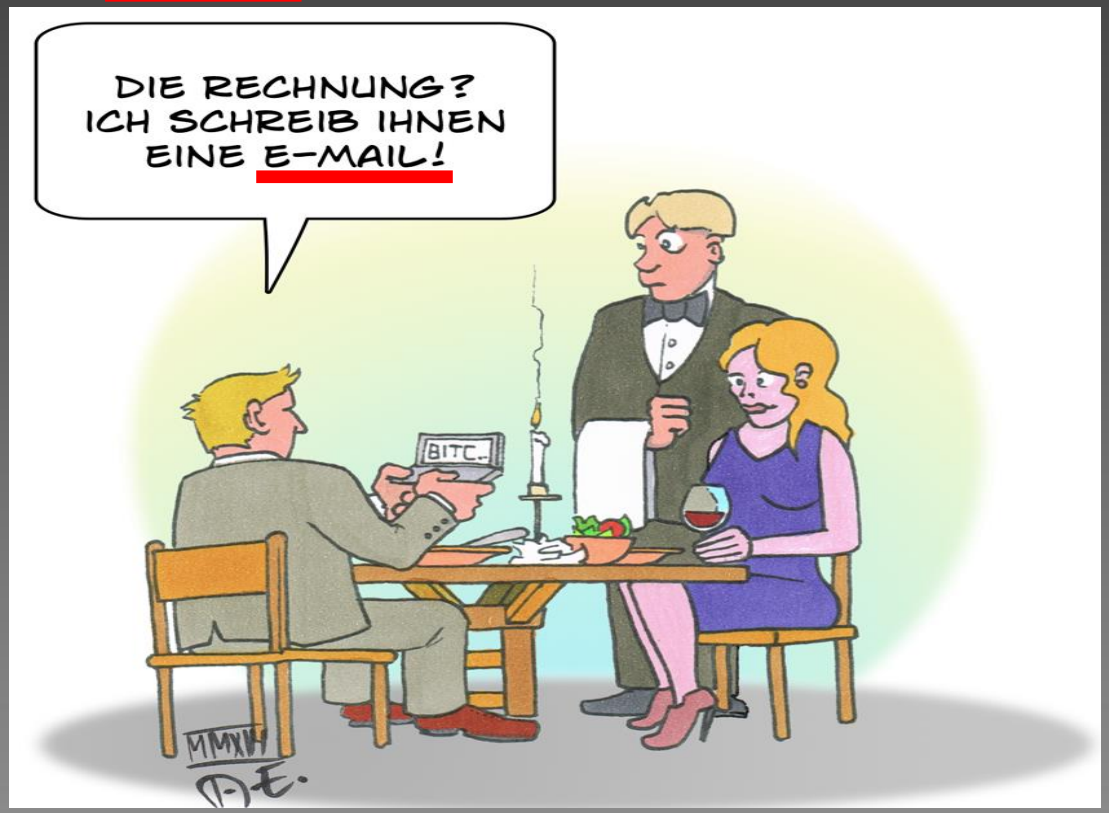
6. **Bekanntgabe eines neuen Blocks im Netzwerk Katrin sieht, dass die Bitcoins jetzt auf Ihrem Konto sind?**

3.1 Vor- und Nachteile v. Bitcoins

Welche „Vorteile“ und Nachteile gibt es für die „Handelspartner“ des Heroins?

3.2 Welchen Fehler macht d. Autor?

28.03.2014 16:53 Age: 3 yrs
Autor: Martin Brosy Category: Top Story
Die Bitcoins in der Vertrauenskrise?

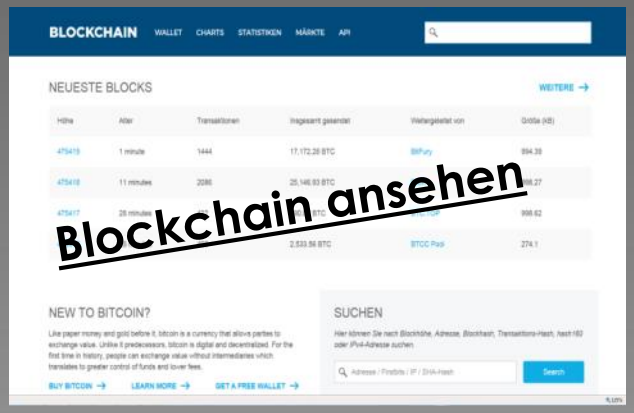


http://www.boersenpoint.de/boersenblog/blog/die-bitcoins-in-der-vertrauenskrise-1001701/

3.3 Bitcoin – erste Schritte

https://www.bitaddress.org

https://blockchain.info/



3.4 Bitcoinadresse anlegen

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address | **Private Key**

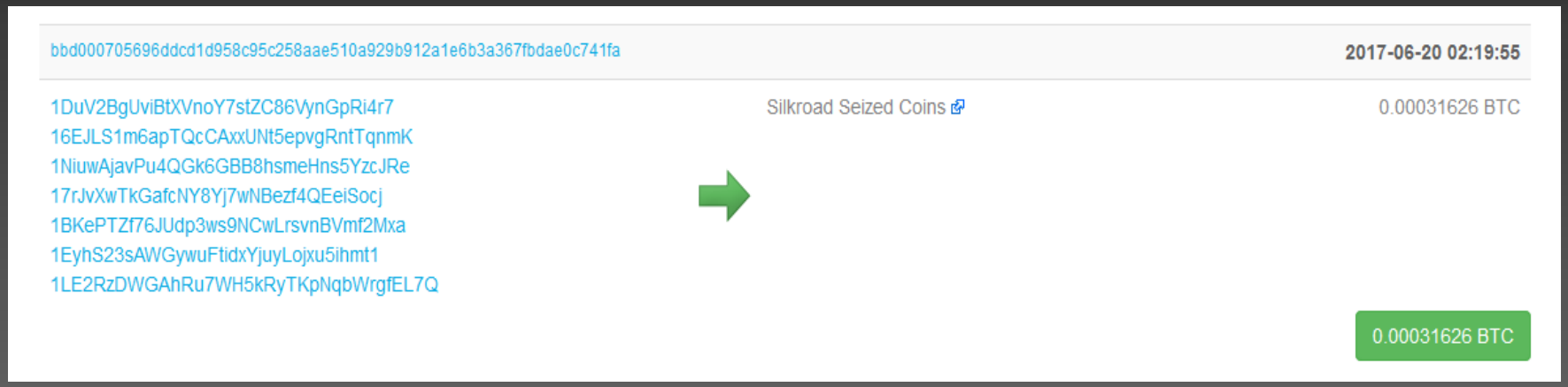
SHARE

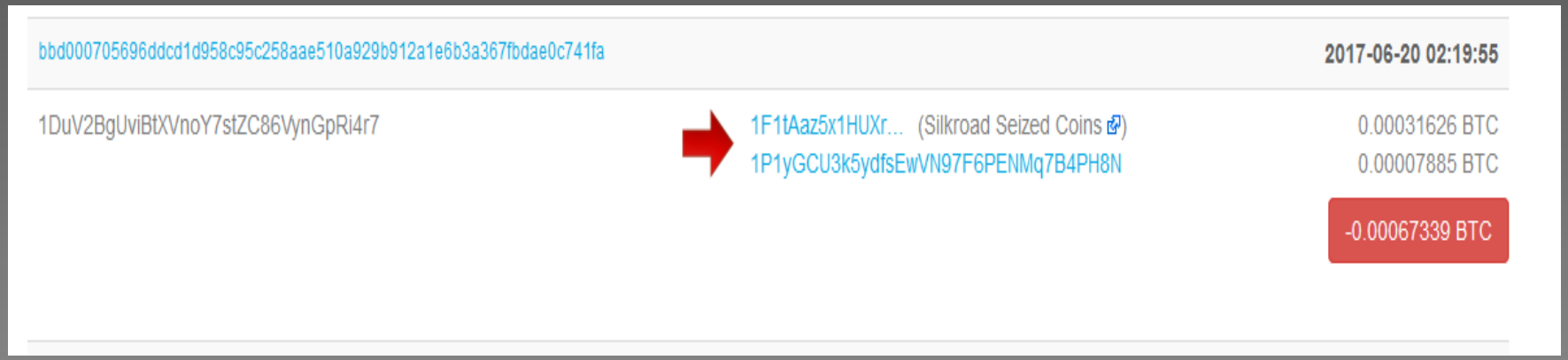
SECRET

1JEdLgLw4iyfYBngVo28DV5mo3nYbatBK4

KyTGBxPcXk5N73NT6tCNXXcf4sh2NBLtfbWYNcmtJ6VXFuZY8YZ2

3.5 Ansicht in der Blockchain





https://blockchain.info/de/address/1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

3.6 Kontrollfragen

Was ist ein Bitcoin?

Warum sind in der Blockchain keine Personen zu sehen?

Was ist eine Wallet?

Was passiert, wenn die Wallet mit allen Daten gelöscht wird? …und die Daten auf Papier stehen?

4 Kryptoware im Kontext Polizei

http://schwarwel-karikatur.com/ngg_tag/bahnhof/

5 Schlussbetrachtung

Haben der Käufer und der Verkäufer das Ziel durch die Anwendung von Kryptowährung erreicht?

https://www.w-t-w.org/de/bitcoin-bitcoin/bitcoin-miner/

6 weiterführende Quellen

Joerg Platzer, Bitcoin – kurz & gut

Elfriede Sixt, Bitcoins und andere dezentrale Transaktionssysteme

Sourcecode für Entwickler

https://github.com/lithander/Minimal-Bitcoin-Miner/tree/master/MiniMiner

https://aois.blob.core.windows.net/public/Blockchain%20Programming%20in%20CSharp.pdf

Vielen Dank für Ihre Aufmerksamkeit ☺

Heiko Franke
Telefon: 01627364880
E-Mail: heiko.franke@educationcamp.de
Hornshagen 8
17348 Woldegk