



# Bitcoin & Co-Kryptowährung

Fachhochschule Güstrow

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



# Agenda

## 1 Ausgangssituation

1.1 klassische Zahlungsarten

1.2 Topologie klass. Zahlungsarten

1.3 Anwendbarkeit

## 2 Lösung Kryptoware

2.1 Kryptowährungen

2.2 Topologie der Kryptowährung

2.3 - 2.6 Bestandteile von Kryptowährungen

2.7 - 2.9 Beschreibungen

## 3 Bitcoins näher betrachtet

3.1 Vor- und Nachteile von Bitcoins

3.2 Welchen Fehler macht der Autor?

3.3 Bitcoin – erste Schritte

3.4 Bitcoinadresse anlegen

3.5 Ansicht in der Blockchain

3.6 Kontrollfragen

## 4 Kryptoware im Kontext Polizei

## 5 Schlussbetrachtung

## 6 weiterführende Quellen

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



# 1.2 Topologie klass. Zahlungsarten

IBAN:DO28BAGR00000001212453611324

IBAN:LV80BANK0000435195001



IBAN:FO6264600001631634



IBAN:BH67BMAG00001299123456

IBAN:CZ6508000000192000145399



IBAN:KZ86125KZT5004100100

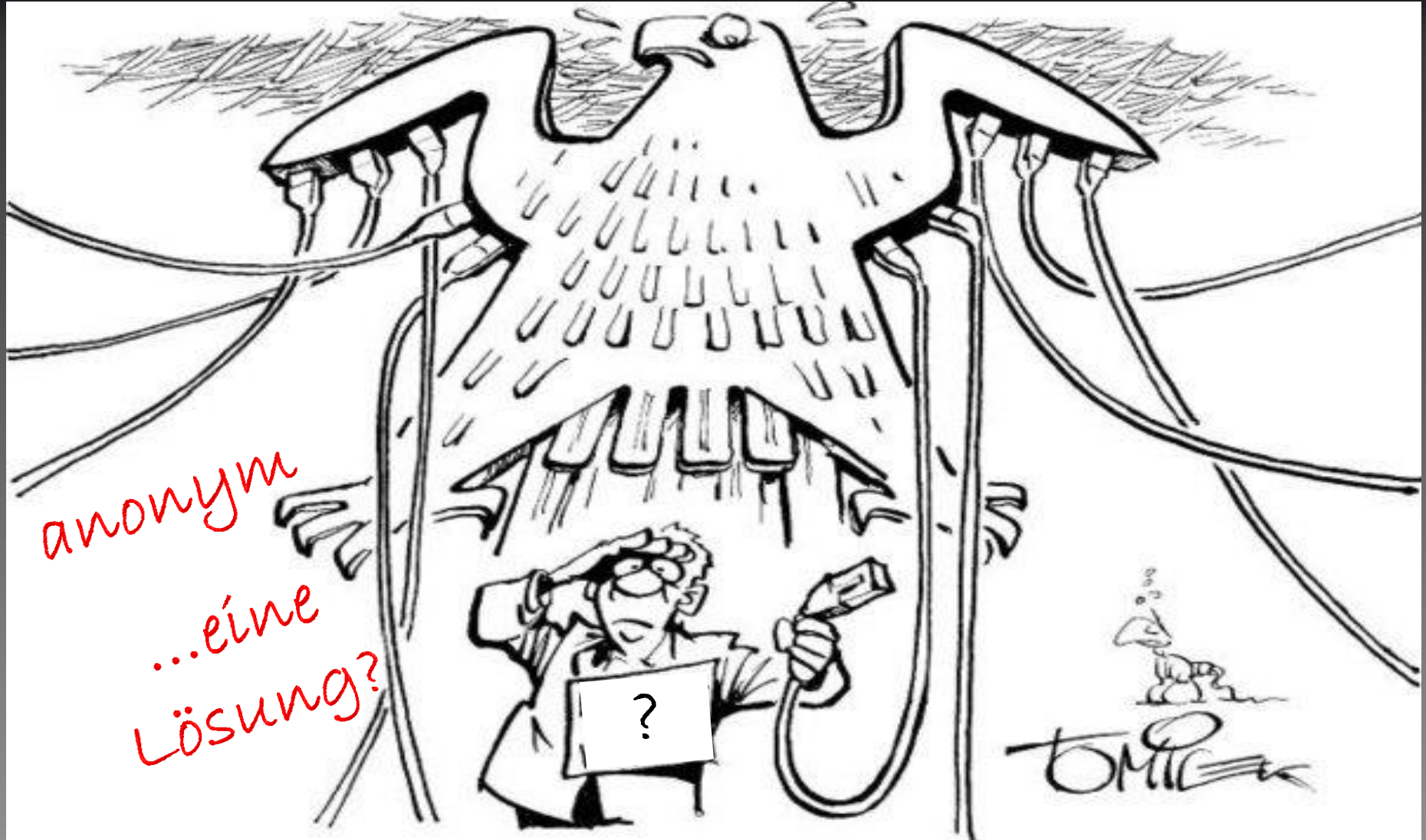
IBAN:FI2112345600000785:



IBAN:BE68539007547034



# 1.3 Anwendbarkeit



## 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](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.



# 2.2 Topologie der Kryptowährung



1MFMix923qnLbA8qPazb1uzFPJEEEn1jxXk

16ghzkw1KyPGX63cQ9Fj6EHd1qCEW2d8Fg

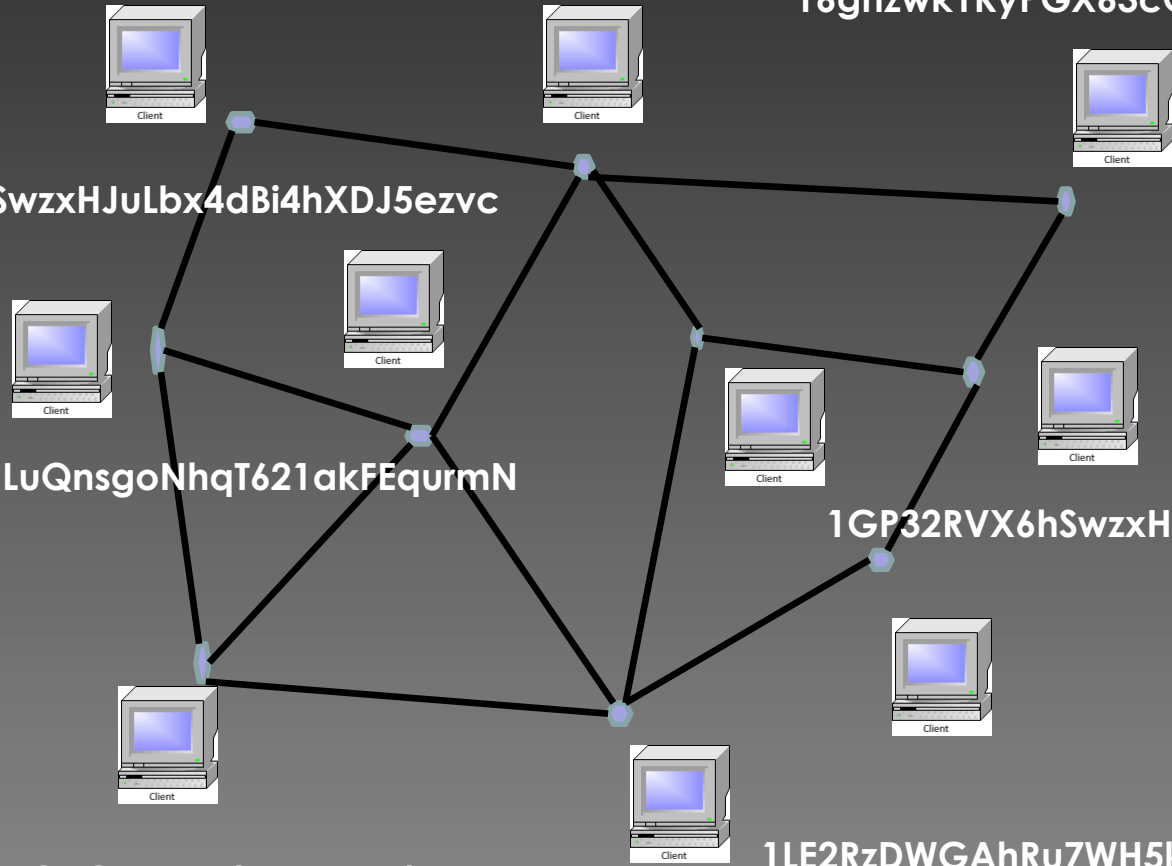
1GP32RVX6hSwzxHJuLbx4dBi4hXDJ5ezvc

1AGuEXQsfcULuQnsgoNhqT621akFEqurmN

1GP32RVX6hSwzxHJuLbx4dBi4hXDJ5ezvc

16EJLS1m6apTQcCAxxUNT5epvgRntTqnmK

1LE2RzDWGAhRu7WH5kRyTKpNqbWrgfEL7Q





## 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
- \* persistent



## 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.

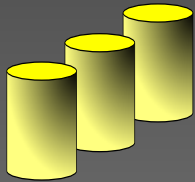
Ein Wallet ist **nicht Voraussetzung** für eine **Transaktion**.  
Der private Schlüssel und die bitcoin-Adresse kann auch  
auf Papier festgehalten werden.

(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?



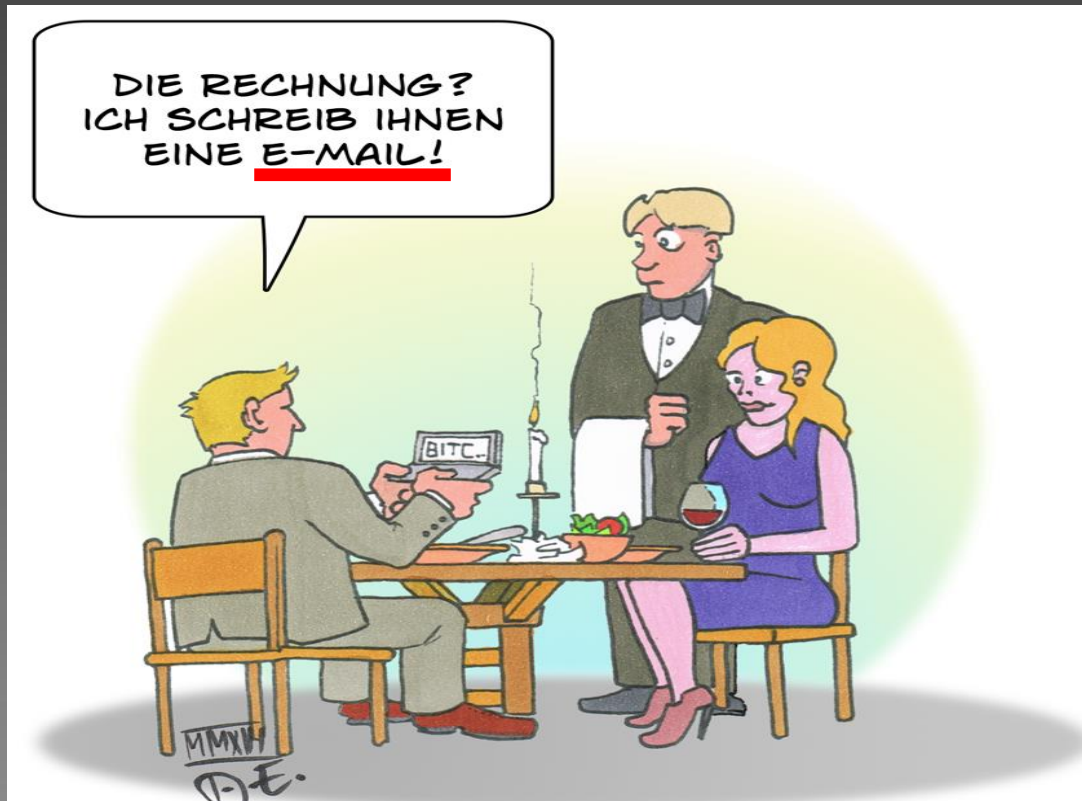
*Video*

## 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?





## 3.3 Bitcoin – erste Schritte

<https://www.bitaddress.org>

**bitaddress.org**  
Offener, client-seitiger Bitcoin-Wallet-Generator in JavaScript

10% 10% 10% Kopf-Wallet  
10% 10% Walletdetails

Erstelle Bitcoin-Wallet...  
Bewege deine Maus umher, um die Zufälligkeit zu erhöhen... 10%  
OR type some random characters into this textbox

**Bitcoinadresse**

```
163b54227e8dc06ab55e6d25c8799c7f3e42586a98219f151533  
d3ac0823d9ed46004ccb9da57ca096dc509d402b  
40989a3449fda529bd075b1e9c998  
9616f4edd4a1c1d59fcb4cc55d9fe  
307a50e6ba8e1402e46e5bde1455bb6a3107c285e  
a9f285174e2e29905a215a120523ca0c615f2f0c38da64dac5f  
71b1744084013d36199bde707b5fa3820232322b04fa06ae70da  
fa3a16c07ff66d2f4883c038815c1ba530f5a8937060721da031a  
af4165016fc9d5bba22df56b69d24b6c65150821464ebdf1ba25f  
40ea3710e443e40cb4d95654f59b051a254
```

<https://blockchain.info/>

**BLOCKCHAIN** WALLET CHARTS STATISTIKEN MÄRKTE API

NEUESTE BLOCKS [WEITERE →](#)

Höhe	Alter	Transaktionen	Insgesamt generiert	Wahrgenötigt von	Größe (KB)
475419	1 minute	1444	17.172,28 BTC	BitFury	294,38
475418	11 minutes	2086	26.148,89 BTC	BitFury	305,57
475417	28 minutes	1777	22.877,77 BTC	BitFury	308,82
475416	45 minutes	1777	2.833,38 BTC	BTCC-Pool	274,1

NEW TO BITCOIN?  
Like paper money and gold before it, bitcoin is a currency that allows parties to exchange value. Unlike it predecessors, bitcoin is digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.  
[BUY BITCOIN →](#) [LEARN MORE →](#) [GET A FREE WALLET →](#)

SUCHEN  
Hier können Sie nach Blockchain, Adresse, Blockchain, Transaktions-Hash, hash160 oder IPV4-Adresse suchen.



# 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**

1JEdLgLw4iyfYBngVo28DV5mo3nYbatBK4



**SECRET**

KyTGBxPcXk5N73NT6tCNXXcf4sh2NBLtfbWYNcmtJ6VXFuZY8YZ2



## 3.5 Ansicht in der Blockchain

bbd000705696ddcd1d958c95c258aae510a929b912a1e6b3a367fbdac0c741fa

2017-06-20 02:19:55

1DuV2BgUviBtXVnoY7stZC86VynGpRi4r7  
16EJLS1m6apTQcCAxxUNT5epvgRntTqnmK  
1NiuwAjavPu4QGk6GBB8hsmeHns5YzcJRe  
17rJvXwTkGafcNY8Yj7wNBez4QEeiSocj  
1BKePTZf76JUdp3ws9NCwLrsvnBVmf2Mxa  
1EyhS23sAWGywuFtidxYjuyLojxu5ihmt1  
1LE2RzDWGAhRu7WH5kRyTKpNqbWrgfEL7Q

Silkroad Seized Coins [🔗](#)

0.00031626 BTC



0.00031626 BTC

bbd000705696ddcd1d958c95c258aae510a929b912a1e6b3a367fbdac0c741fa

2017-06-20 02:19:55

1DuV2BgUviBtXVnoY7stZC86VynGpRi4r7



1F1tAaz5x1HUXr... (Silkroad Seized Coins [🔗](#))  
1P1yGCU3k5ydfsEwVN97F6PENMq7B4PH8N

0.00031626 BTC

0.00007885 BTC

-0.00067339 BTC

<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



# 5 Schlussbetrachtung

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



# 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](mailto:heiko.franke@educationcamp.de)**

**Hornshagen 8**

**17348 Woldegk**