



# Missbrauchspotential von Kryptowährungen

LAW DAYS HSG

Roman Andermatt

23. APRIL 2019

©17CREATORS.COM

WANNACRY  
Demands we pay  
\$300 RANSOM  
IN BITCOIN.



Bokbluster.com

WHAT'S  
WANNACRY?

WHAT'S A  
BITCOIN?



# HINTERGRUND

Transaktionen werden in Blöcken zusammengefasst

## LATEST BLOCKS

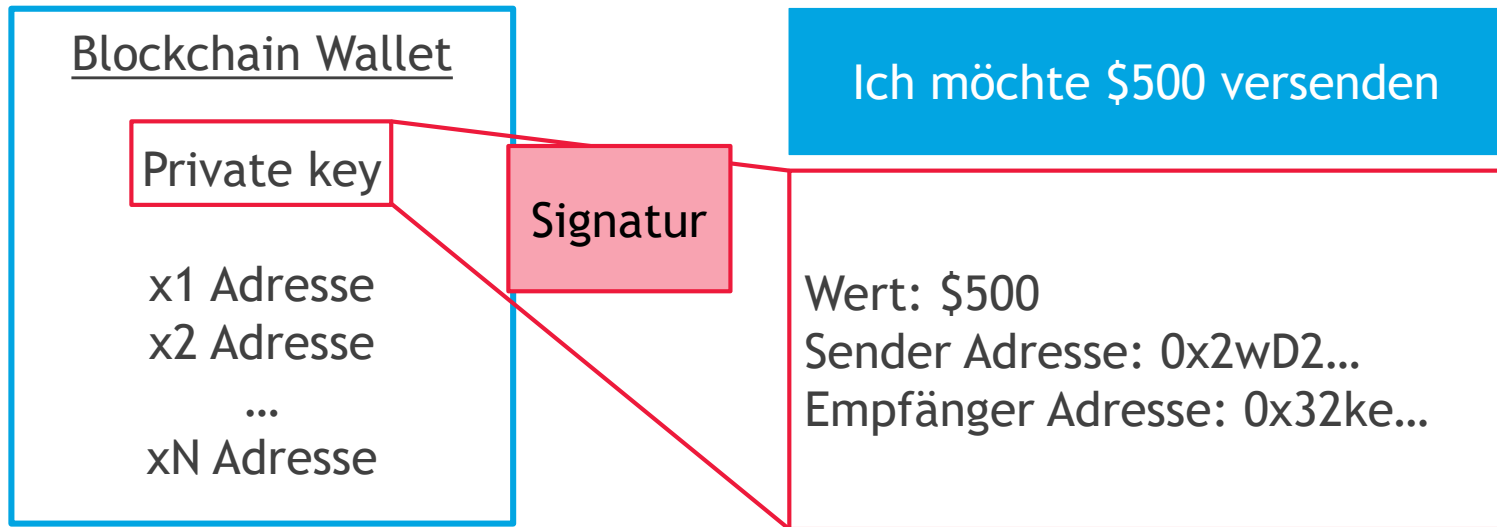
[SEE MORE →](#)

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
<a href="#">544859</a>	7 minutes	2563	8,023.79 BTC	<a href="#">F2Pool</a>	1,266.17	3,997.83
Update no. 544859 with 2563 new transactions, with a volume of 8,023.79 BTC						
<a href="#">544857</a>	57 minutes	617	2,384.16 BTC	<a href="#">AntPool</a>	241.83	815.45
<a href="#">544856</a>	1 hour 6 minutes	2038	10,905.90 BTC	<a href="#">ViaBTC</a>	1,193.54	3,992.97

1 Update schickt \$7,600,000 um die Welt - ohne eine Bank

# HINTERGRUND

## Transaktionen versenden



# HINTERGRUND

## Aufbau einer Transaktion

c4121180b2743de10eb484fd079186a8fbf3740eafe601c4194f67655fa1f0fa

2017-07-09 04:44:33

1EKmnxDKtFDHdzhR9tPiF8bSq6Qwie9663



158qJWZU4QA4oRbrZbuRPw5gDsnkVxsXga

\$ 1,231.55

\$ 1,231.55

### Zusammenfassung

Adresse [158qJWZU4QA4oRbrZbuRPw5gDsnkVxsXga](#)

Hash 160 [2d5bbc39b19417c1aa3705bfb0e4ab5d6ab4d99e](#)

### Transaktionen

Anzahl der Transaktionen 45

Gesamtempfang \$ 51,643.26

Endgültige Balance \$ 0.00

Zahlungsanfrage

Spenden-Button

# HINTERGRUND

Pseudoanonyme und anonyme Transaktionen

## Public Coins



BTC



ETH

## Privacy Coins



Monero (XMR)

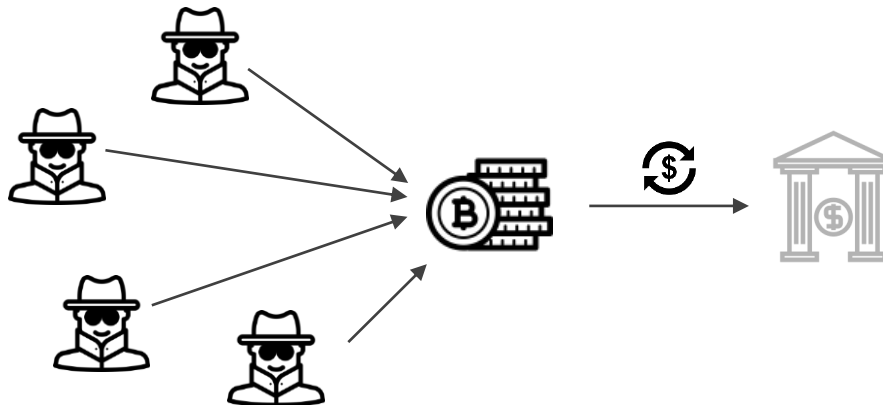


Zcash

# WHEN CYBERCRIME MEETS CRYPTOCURRENCIES

## Herausforderung

- ▶ Kryptowährungen erlauben den einfachen, weltweiten und schnellen Austausch von Vermögenswerten.
- ▶ Der Austausch erfolgt über pseudoanonyme / anonyme Transaktionen die automatisch generiert werden können.
- ▶ Die mit Abstand grösste Herausforderung für das heutige Ökosystem ist die Trennung von «guten» und «bösen» Coins.



# MISSBRAUCHSPOTENTIAL VON KRYPTOWÄHRUNGEN

Die meisten illegalen Aktivitäten fallen in eine von drei Kategorien

- ▶ Ethereum Scams - von ICO Exit Scams bis zu Ponzi Schemas  
Größenordnung: **Dutzende von Millionen** Dollar / Jahr
- ▶ Darkmarkets - Zahlungsmittel auf illegalen Marktplätzen  
Größenordnung: **Hunderte von Millionen** Dollar / Jahr
- ▶ Erpressung / Hacks  
Größenordnung: **Milliarden** Dollar / Jahr





# ETHEREUM SCAM

ICO Scam - Crowdfunding für nicht existente Unternehmen

## DEADCOINS.COM

ÜBER 1'572 KRYPTOWÄHRUNGEN

### ELECTRONIC DOLLAR

«Entwickler hatte 4% für sich vorgesehen, die sofort verkauft wurden, nachdem seine Kryptowährung handelbar wurde. Seit dem ist der Entwickler krank.»

### BITCOINCROWN

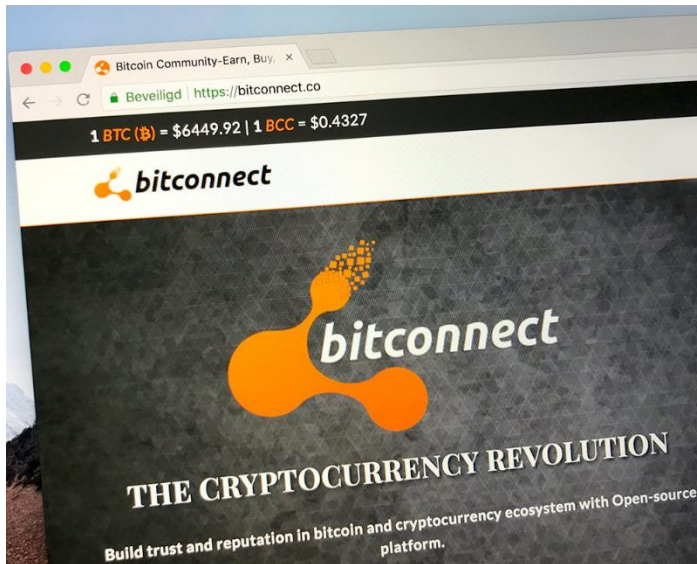
«Seit fast einem Jahr tot. Website seit sieben Monaten offline. Es gibt keine Möglichkeit, Kontakt aufzunehmen.»

### EMPOWER COIN

«Inflationäre Entwicklung. Die Entwickler schufen einen Vorrat von 12 Billionen Coins und haben Weiterentwicklung aufgegeben. Herausgegeben für 3'500 \$ pro Coin, heute weniger als 0.0000001 \$ pro Coin»

# ETHEREUM SCAM

## Ponzi Schema - Bitconnect



- ▶ Anonym betriebene Webseite
- ▶ Idee: Investoren geben Darlehen an Nutzer
- ▶ Z.B.: \$10'000 für 180 Tage, gibt 40% Rendite pro Monat und einen 20% Tagesbonus.
- ▶ Mehrstufige Empfehlungsfunktion -> Empfehlungscode auf Social Media beschleunigten Anmeldung.
- ▶ FBI ermittelt, Gründer in Dubai verhaftet

# ETHEREUM SCAM

Ponzi Games - FOM03D

*someone else is*

# EXIT SCAMMING

**1319.0884** 

+ Pre-Seed: 5452.9361 

= Total: 6772.0245 

22:38:39

1x  This key is a key, you know you want it

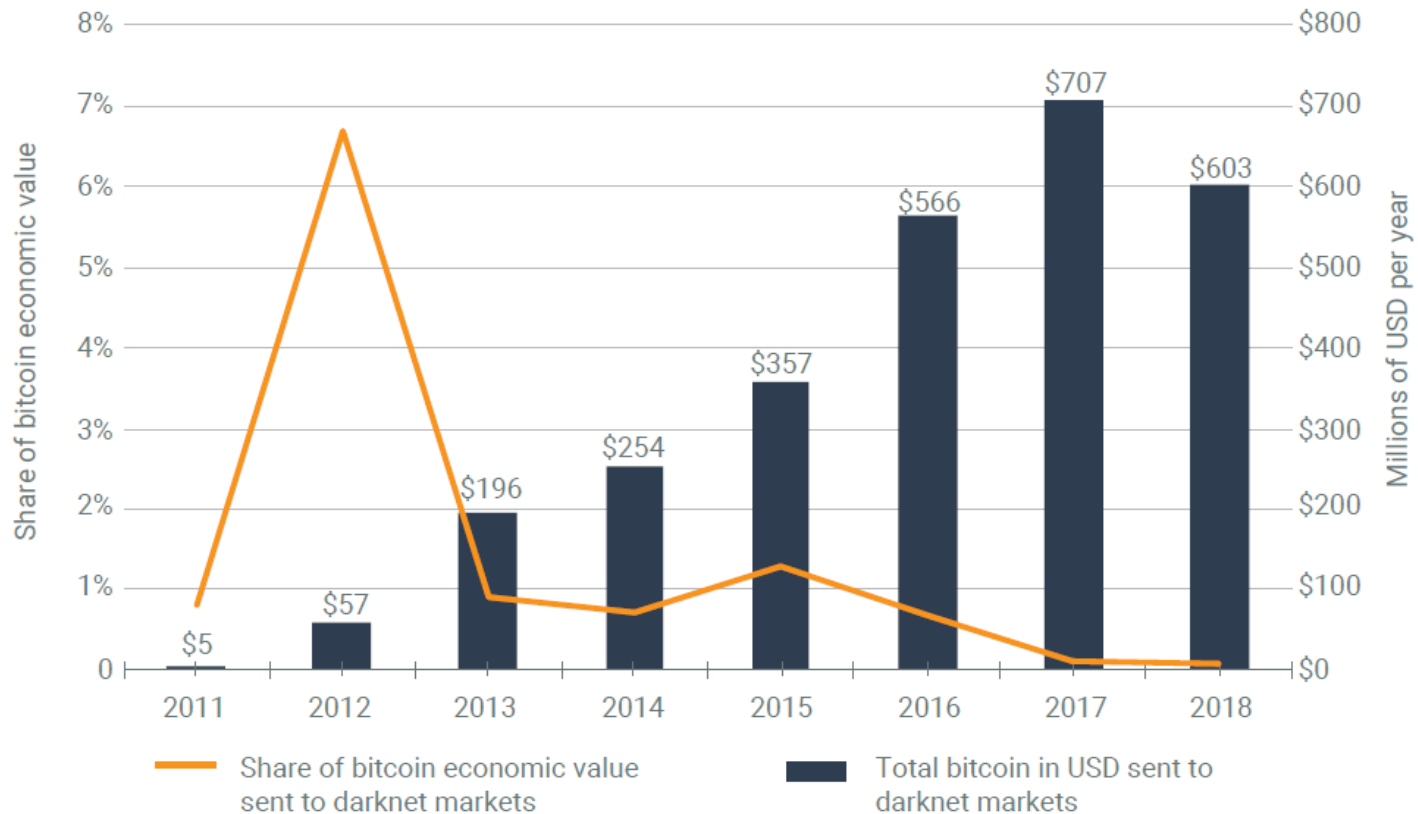
Sources: [exitscam.me](https://exitscam.me)

# DARKMARKETS

## Zahlungsmittel auf illegalen Marktplätzen



Bitcoin flowing to darknet markets



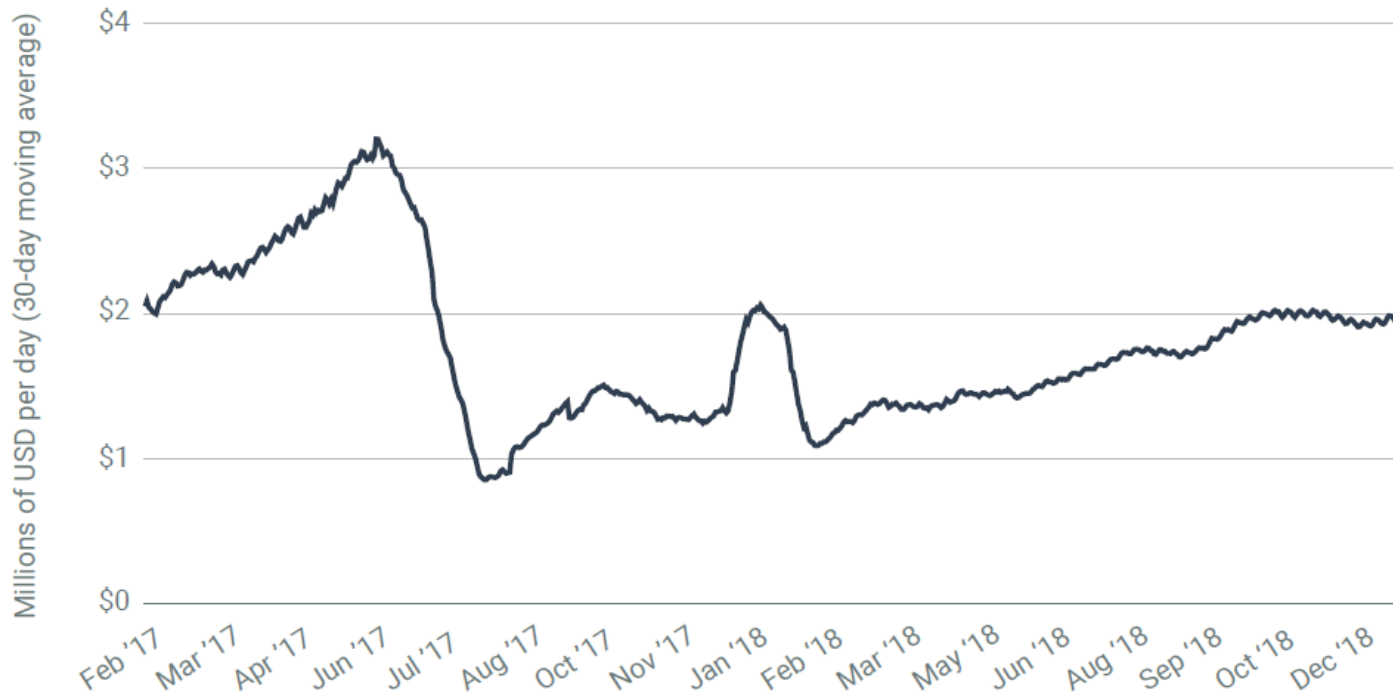
Quelle: Crypto Crime Report, Januar 2019

# DARKMARKETS

## Zahlungsmittel auf illegalen Marktplätzen



Total daily value sent to darknet markets,  
30-day moving average



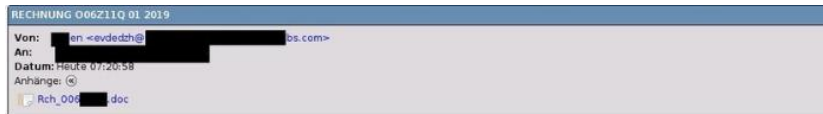
Quelle: Crypto Crime Report, Januar 2019

# ERPRESSUNG / HACKS

*Well, in my opinion, \$11000 is a fair price for our little hidden secret. You will make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" search engines like google).*

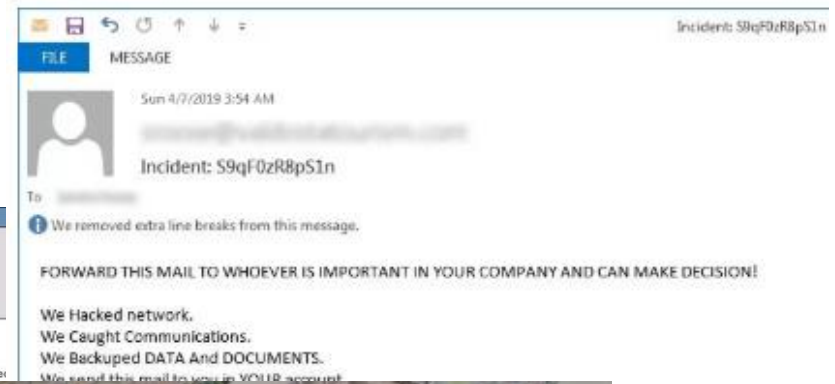
**"Zahle Bitcoins oder ich veröffentliche Videos von dir, auf denen du**

**Die Verschlüsselungssoftware Ryuk hat Deutschland erreicht. Kombiniert mit zwei älteren Trojanern ermöglicht sie Angreifern maßgeschneiderte Erpressungsversuche. Offenbar haben nicht wenige Firmen schon gezahlt.**



Hallo,

vielen Dank für Ihren Auftrag. Anbei finden Sie Ihre Rechnung Nr. 006 [redacted] vom 14/01/2019 zu Ihrer Kundennummer 62 [redacted]. Es gelten unsere Allgemeinen Geschäftsbedingungen.



## Crypto Exchange Zaif Hacked In \$60 Million Bitcoin Theft

That we do if you don't pay bitcoin?

# ASSET RECOVERY



## Allocate

- Wo wurden Bitcoins hingeschickt?



## Track

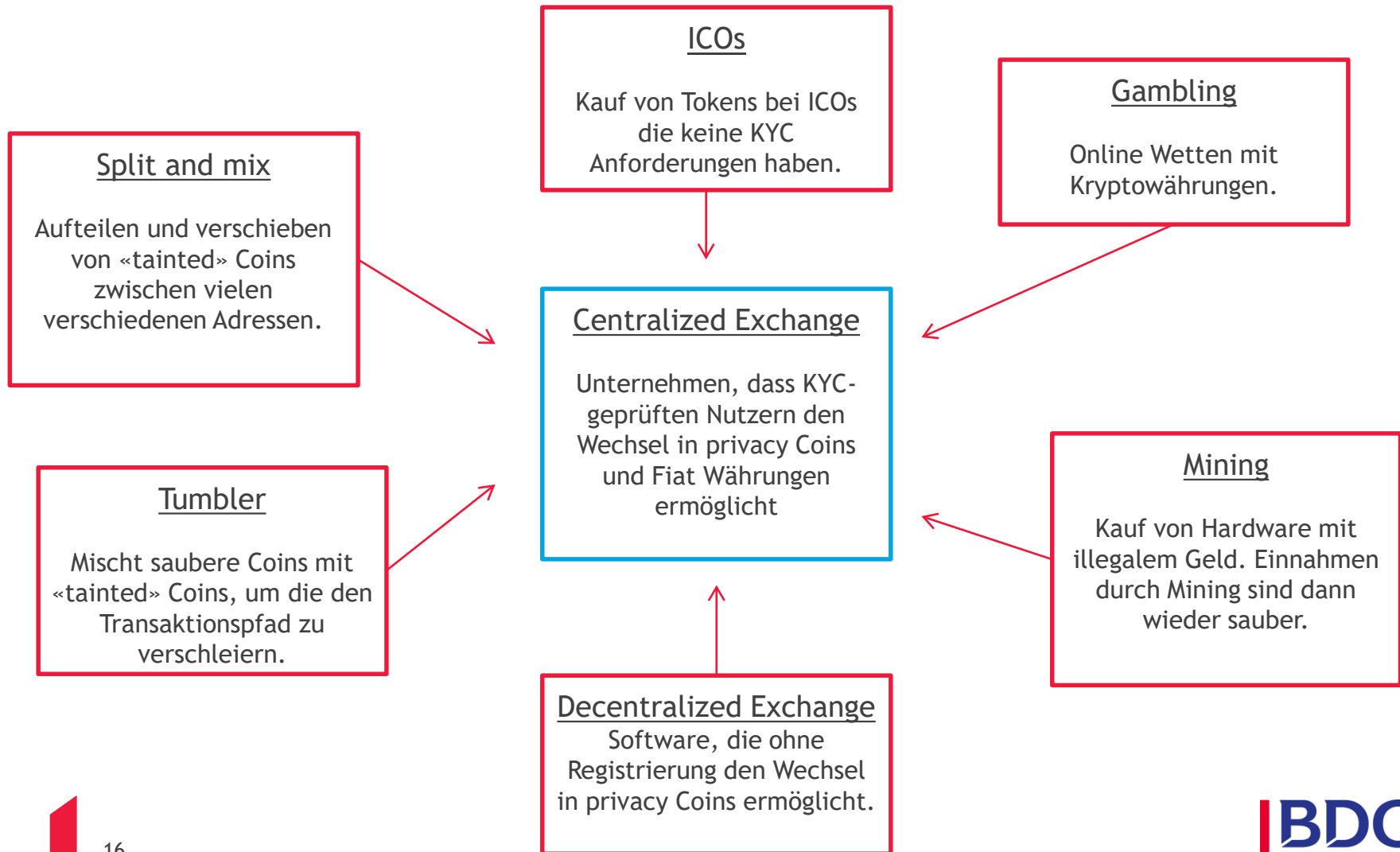
- Wie werden Bitcoins weiter versendet?



## Identify

- Identifizieren der Täterschaft dort wo Bitcoins eingetauscht werden

# TYOLOGIEN VON GELDWÄSCHEREI





# WANNA CRY



Sources: The SSL Store

# WANNA CRY

## Allocate

Address A  
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94  
Current Balance: 0.238 BTC  
Max Balance: 19.983BTC  
Number of Transactions in: 138

1ARirZgU4q61sSjVK2iB8BEYC5w2B8ZnE9	0.1028 BTC
1H68h8qsVkMUgY8khcdFpbHV22cCnC74dk	9.676 BTC
1M1CfXLynR6vqbjwTqSiiLRVDQZEXHHJbb	10.058 BTC

Address B  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw  
Current Balance: 1.502 BTC  
Max Balance: 19.273 BTC  
Number of Transactions in: 126

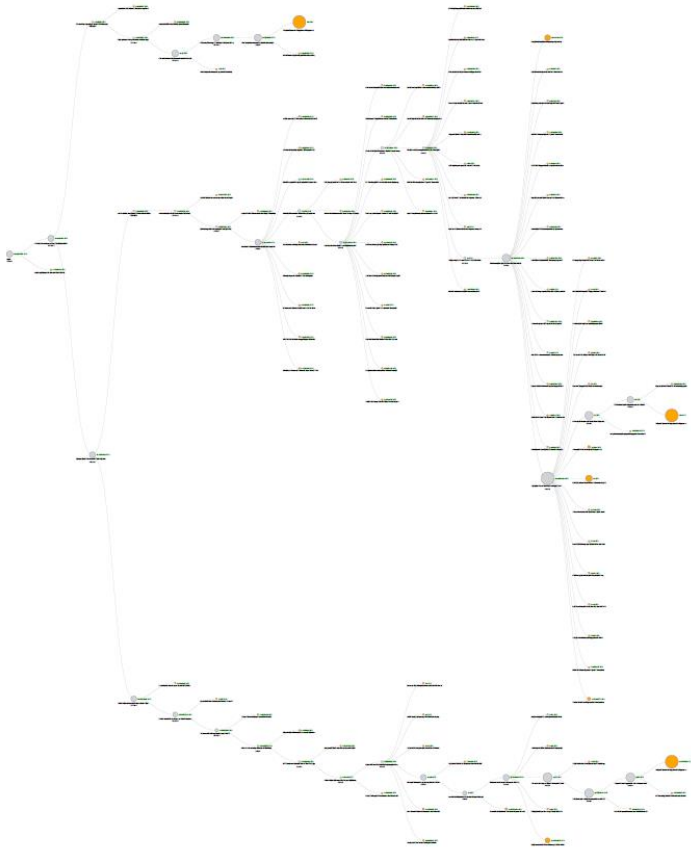
16dfTuSx4f78eQ81PzTgBtBDyZ7QhNZ8Vy	9.027 BTC
1JC41YHmjKEcW1rLH6pmMWEFHkoNwSmhnC	0.0122 BTC
1FQQ86tMuvhQ4Ruyggbb8j7iaNfUZ69gpY	8.7326 BTC

Address C  
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn  
Current Balance: 0.2698 BTC  
Max Balance: 14.680 BTC  
Number of Transactions in: 119

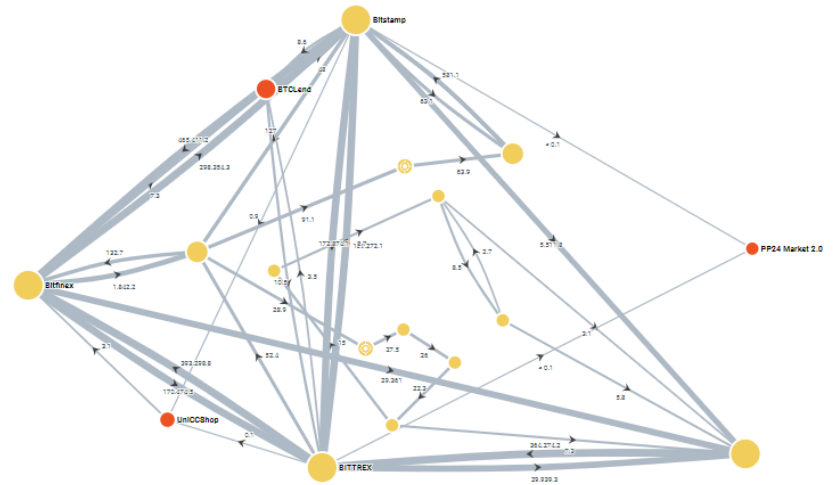
14Y8rfeRAcZkGqG451UGk1epq5zw3dVQif	7.069 BTC
18gsrbQsTY7HzYVZEbvtVBfhywpQk6No2Q	0.0151 BTC
1Q8maVpVNAZbPiavySQz9Jaiwsfht9vBz	7.320 BTC

# TRACK

## Transaktionsbaum

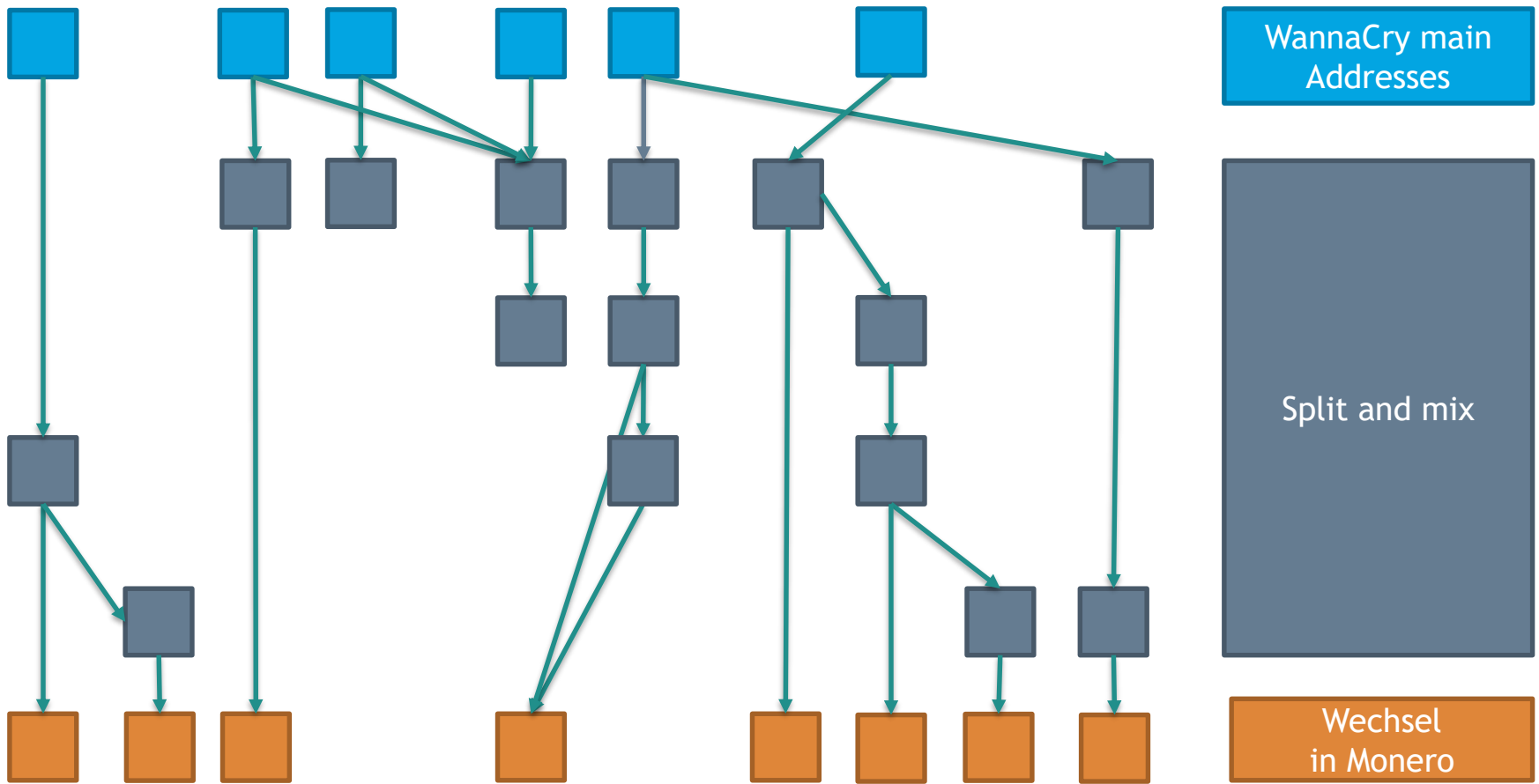


## High-Potential Link



# TRACK WANNA CRY

Split and mix - Exchange to privacy cryptocurrency





# AUSBLICK

Grosse Herausforderungen für globales Finanzsystem und Bekämpfung der Wirtschaftskriminalität.

- ▶ Anonymisierung der Transaktionen auf der Blockchain wird weiterentwickelt
- ▶ Darkmarkets werden dezentraler über mobile Apps wie Telegram oder Whatsapp organisiert.
- ▶ Sanktionen werden in Zukunft mithilfe von Kryptowährungen vermehrt umgangen.



**FRAGEN?**