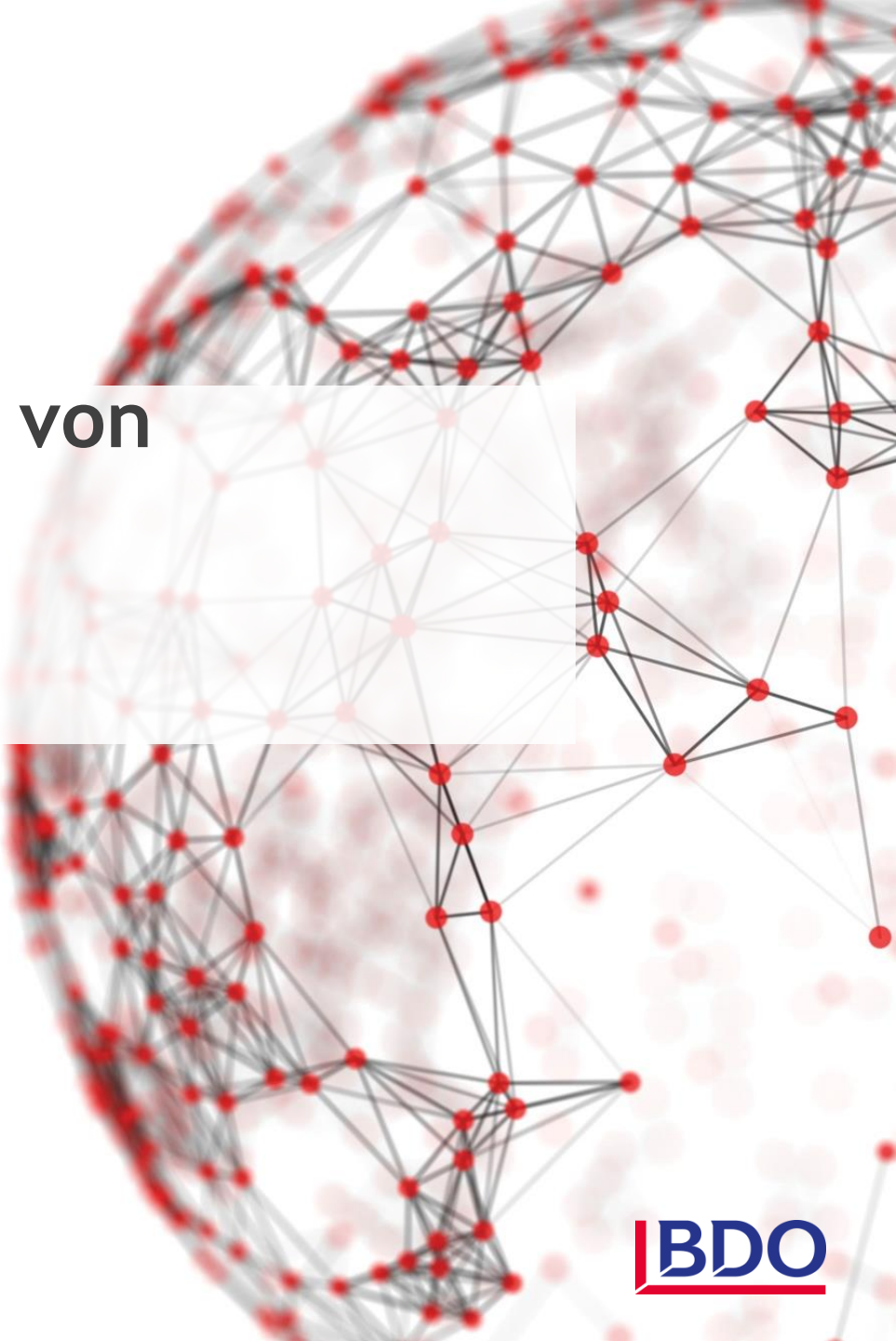
Missbrauchspotential von Kryptowährungen

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 →

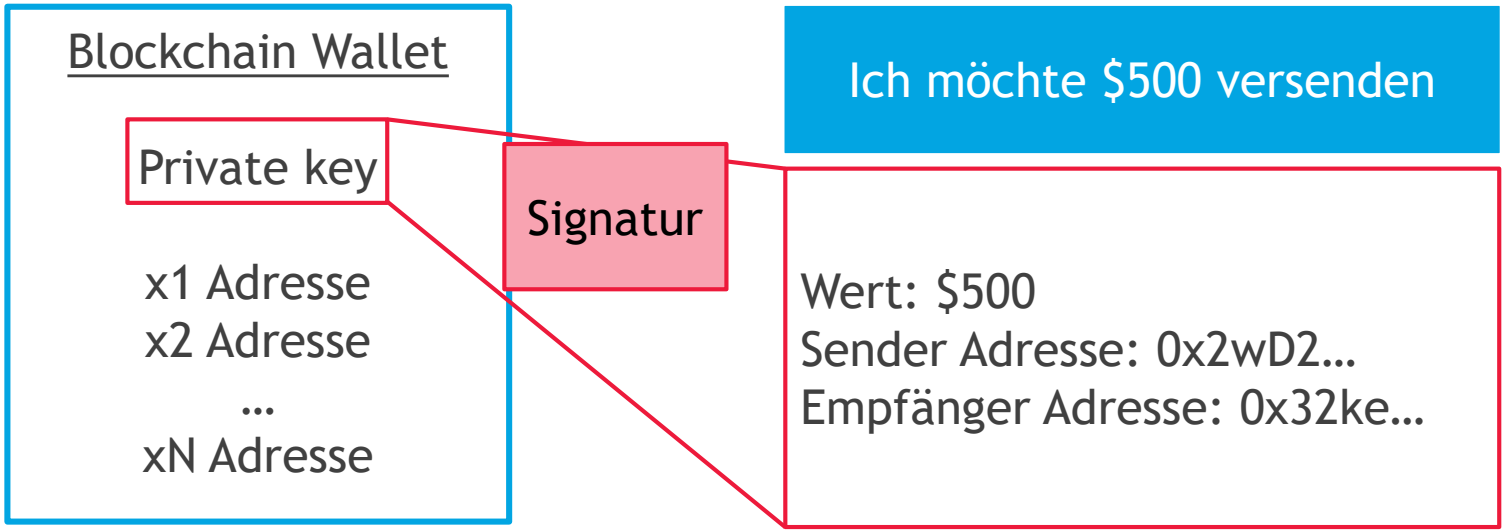
Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
544859	7 minutes	2563	8,023.79 BTC	F2Pool	1,266.17	3,997.83
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
544857	57 minutes	617	2,384.16 BTC	AntPool	241.83	815.45
544856	1 hour 6 minutes	2038	10,905.90 BTC	ViaBTC	1,193.54	3,992.97

Update no. 544859 with 2563 new transactions, with a volume of 8,023.79 BTC

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

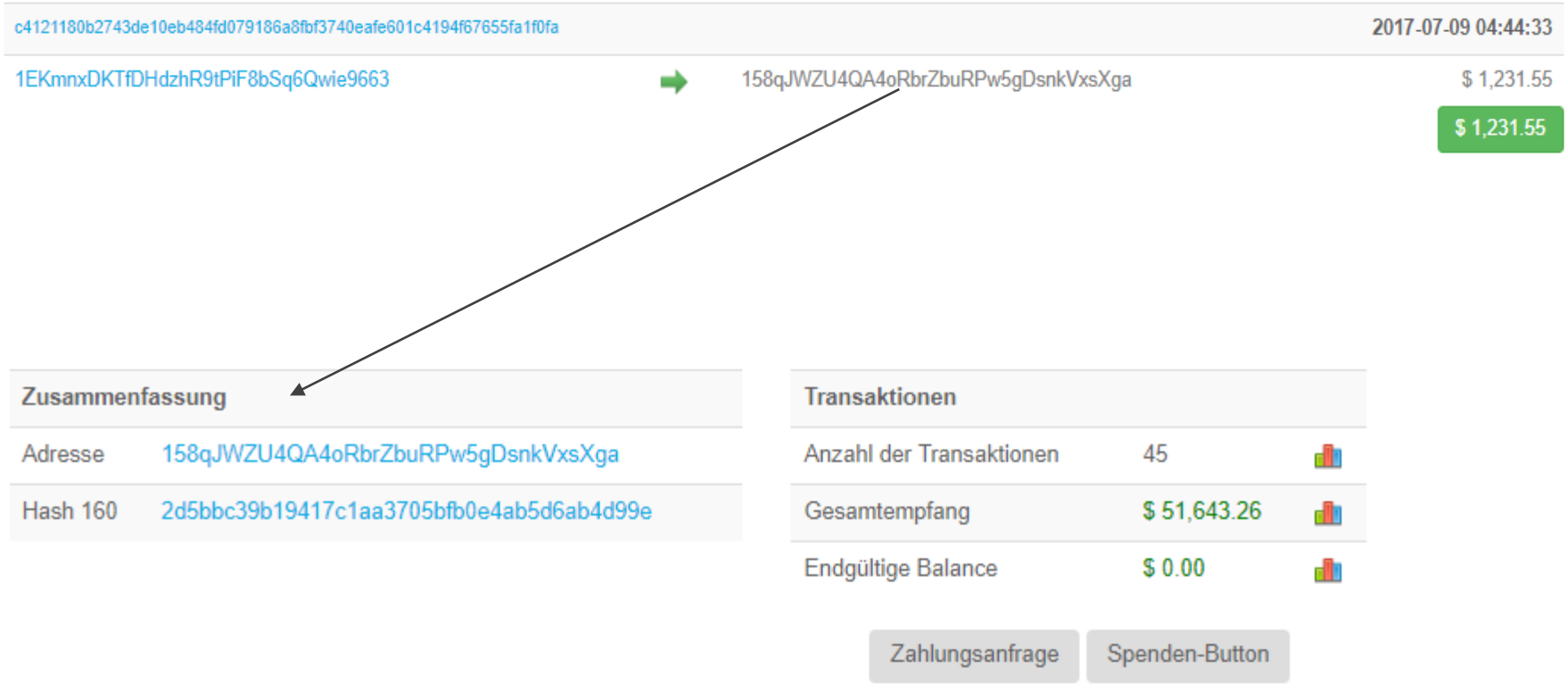
HINTERGRUND

Transaktionen versenden



HINTERGRUND

Aufbau einer Transaktion



HINTERGRUND

Pseudoanonyme und anonyme Transaktionen

Public Coins

BTC

ETH

Privacy Coins

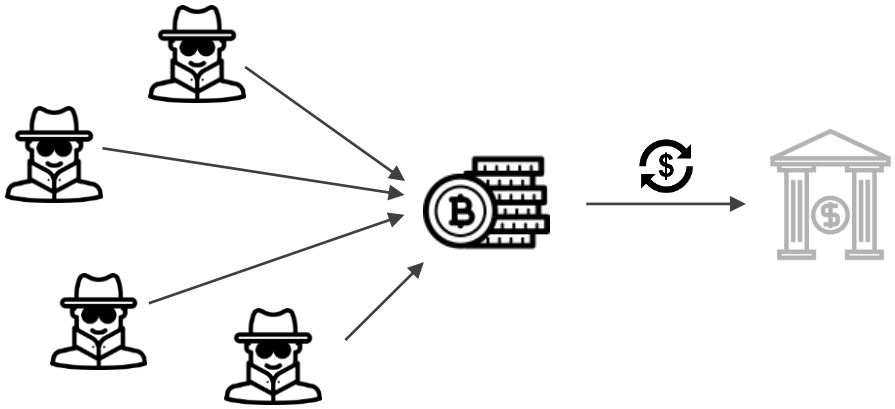
Monero (XMR)

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 -> Empfehlungscodes auf Social Media beschleunigten Anmeldung.
- FBI ermittelt, Gründer in Dubai verhaftet

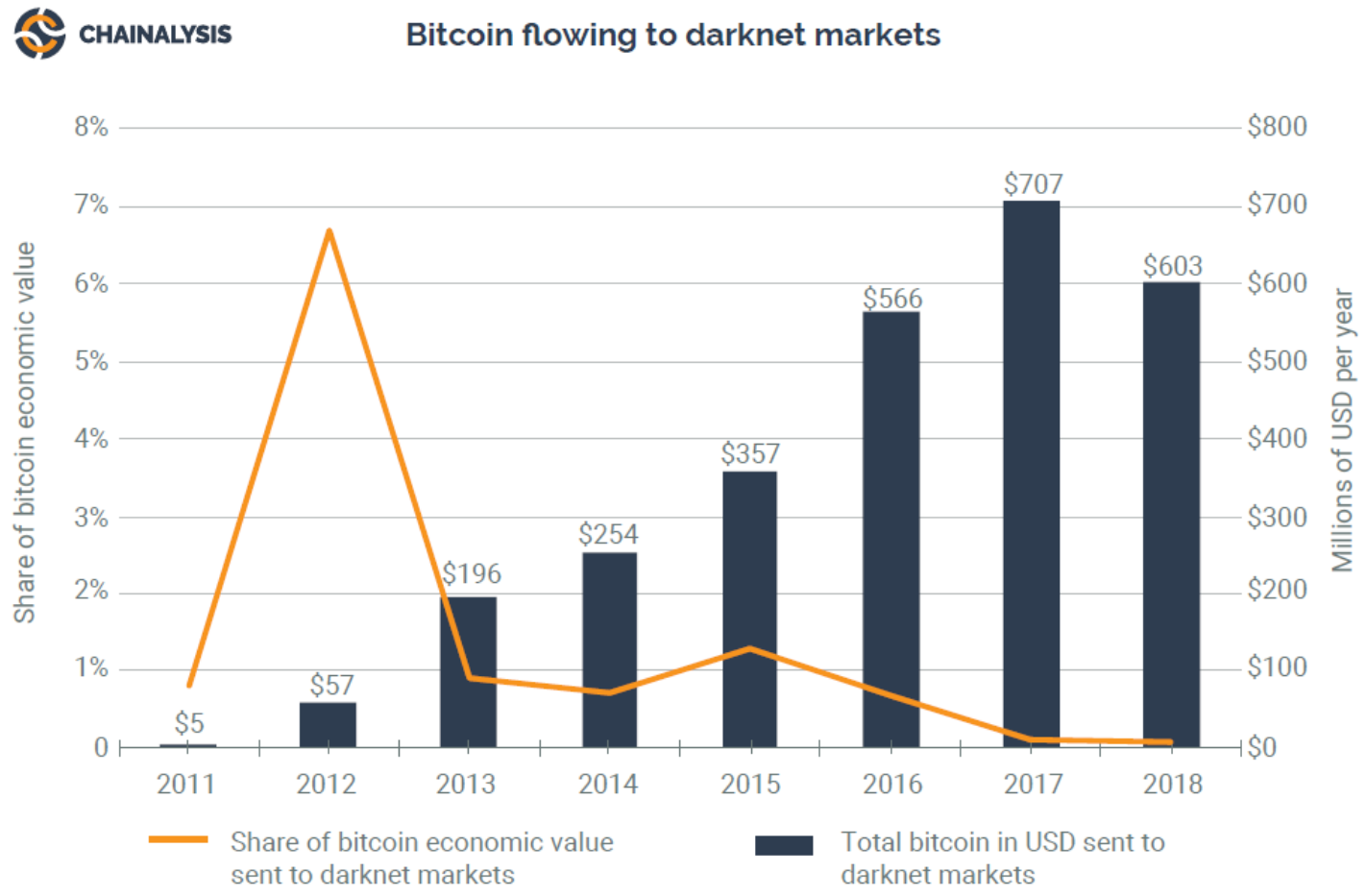
ETHEREUM SCAM

Ponzi Games – FOMO3D

Sources: exitscam.me

DARKMARKETS

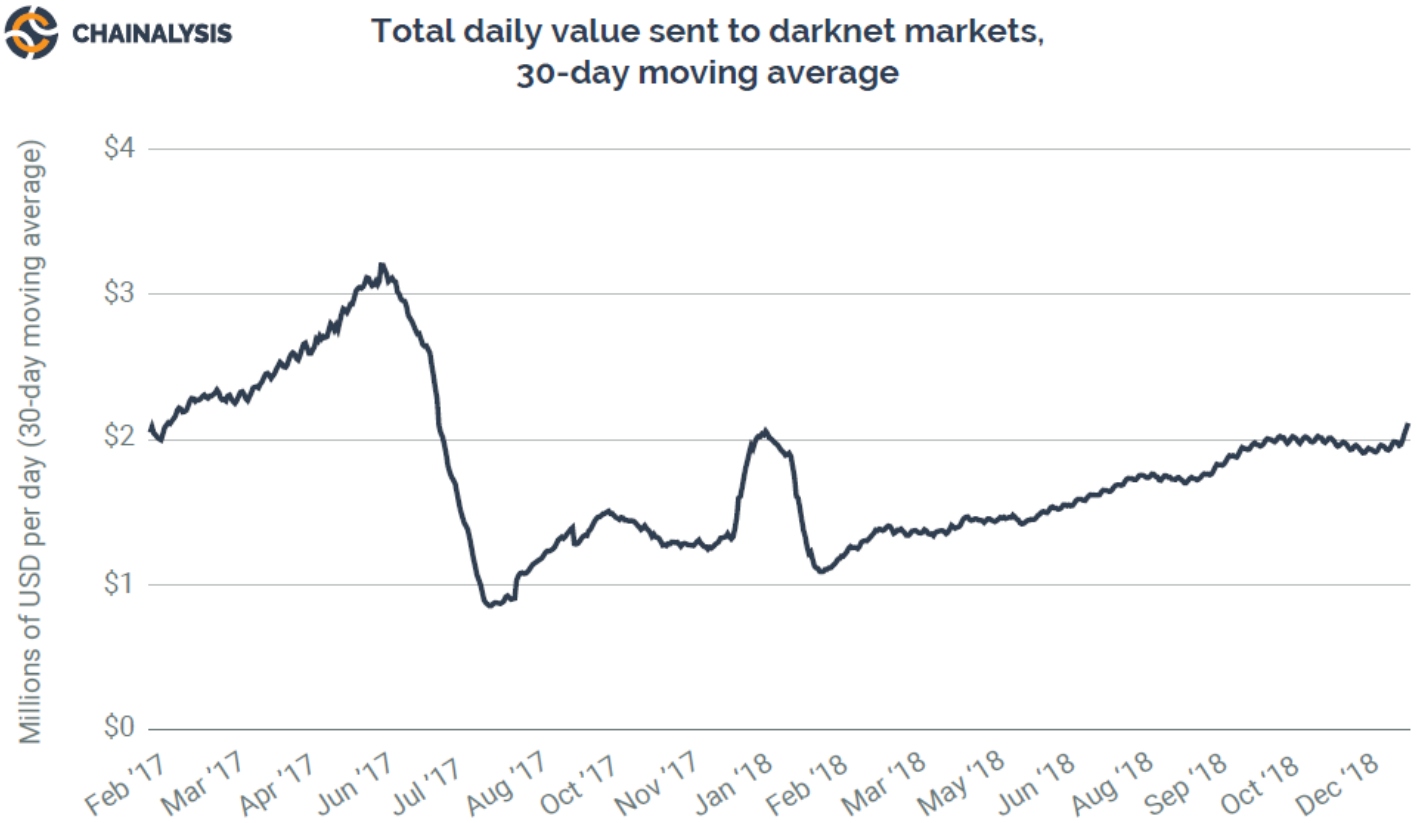
Zahlungsmittel auf illegalen Marktplätzen



Quelle: Crypto Crime Report, Januar 2019

DARKMARKETS

Zahlungsmittel auf illegalen Marktplätzen



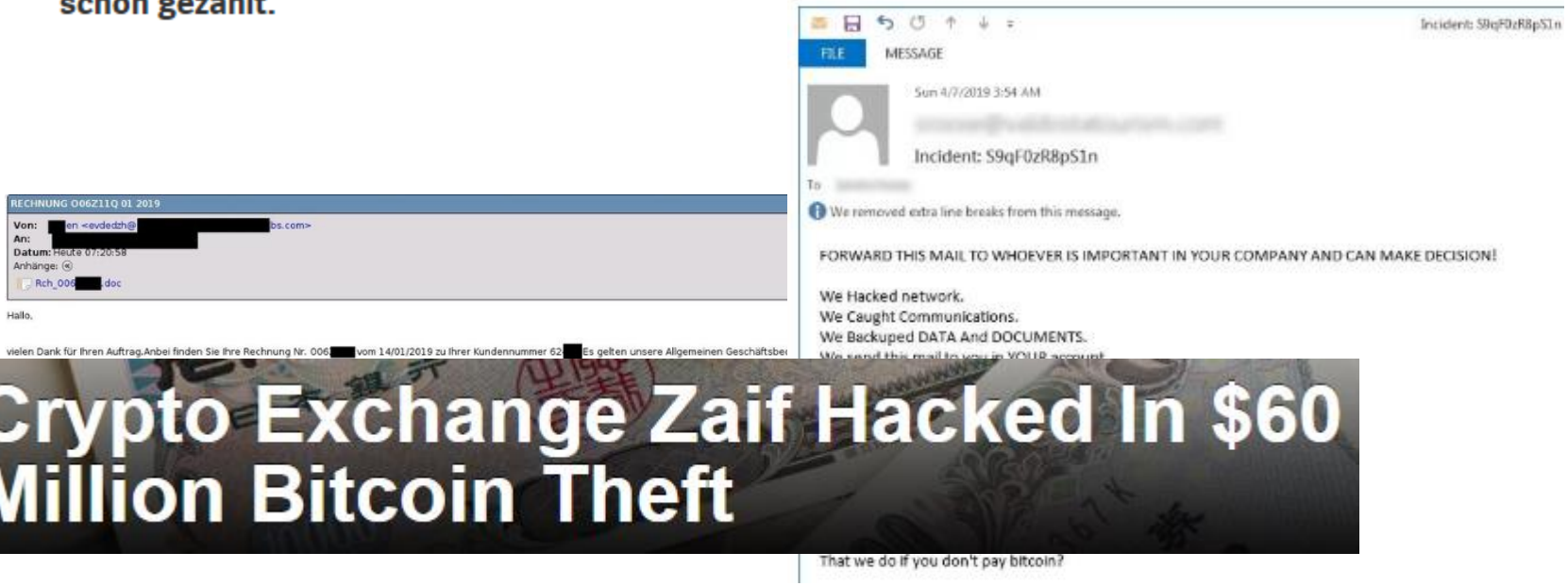
Quelle: Crypto Crime Report, Januar 2019

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.



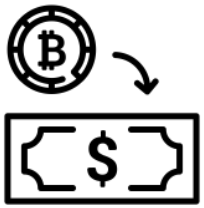
ASSET RECOVERY

Allocate

- Wo wurden Bitcoins hingeschickt?

Track

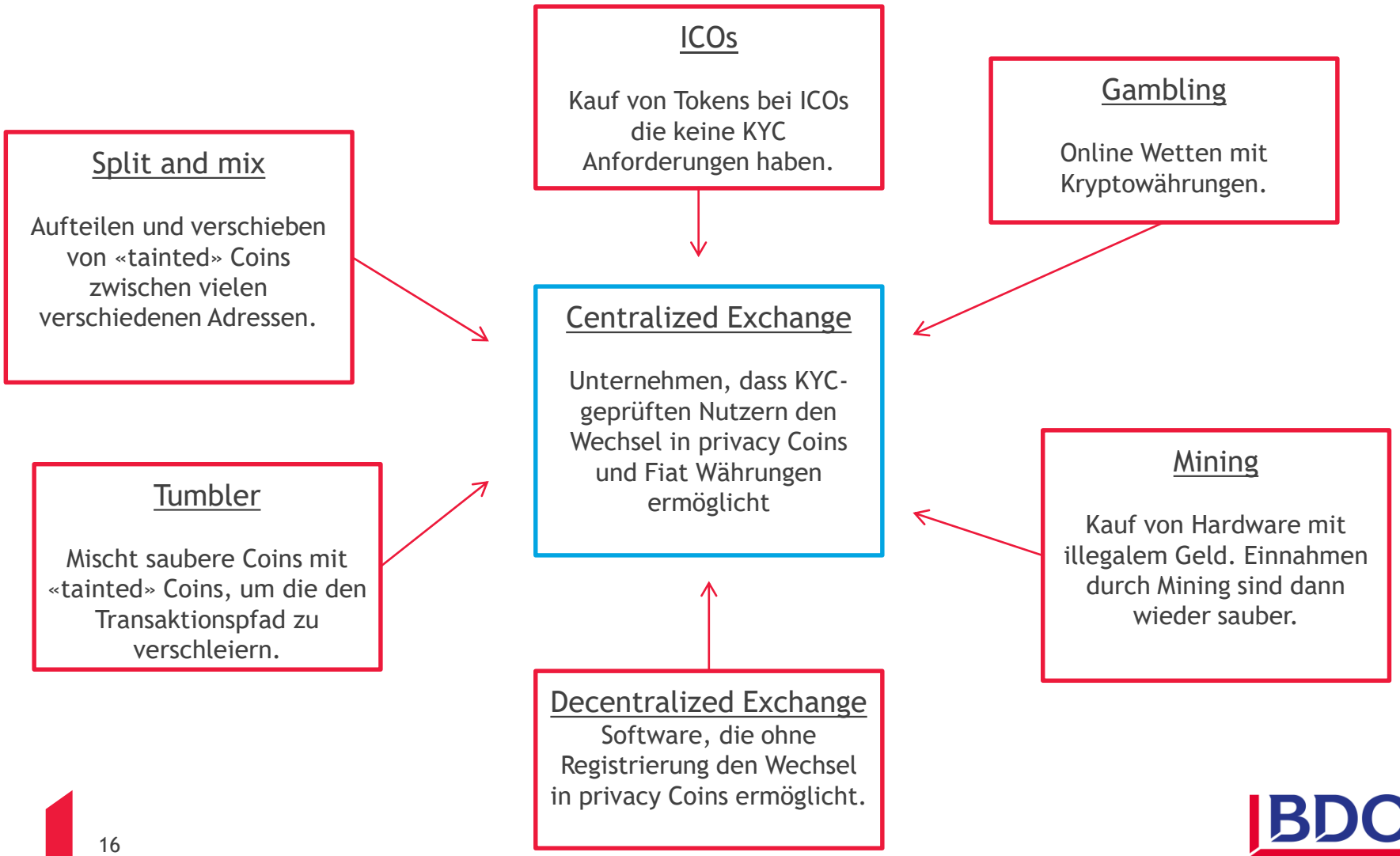
- Wie werden Bitcoins weiter versendet?



Identify

- Identifizieren der Täterschaft dort wo Bitcoins eingetauscht werden

TYPOLOGIEN VON GELDWÄSCHEREI



WANNA CRY

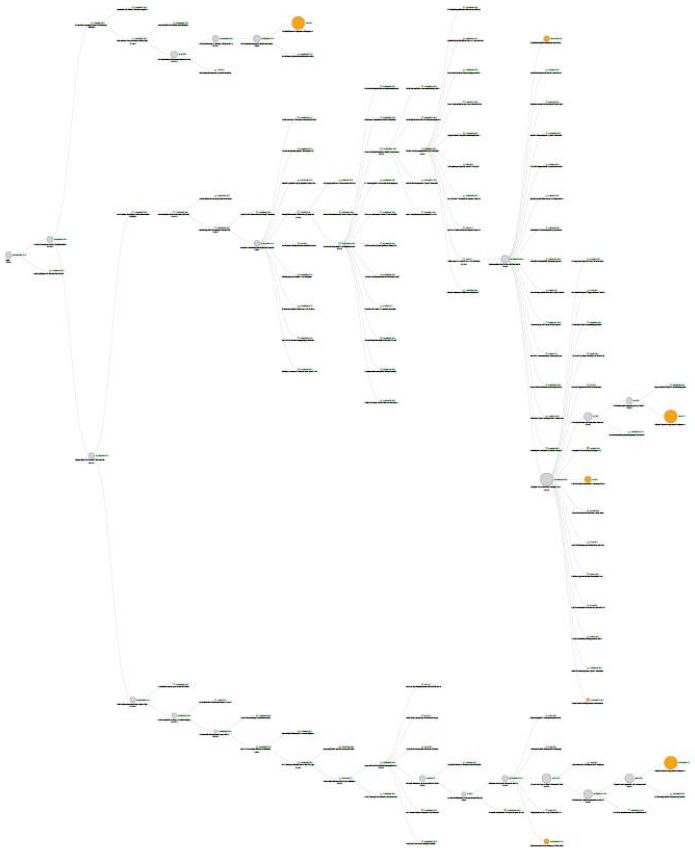
Sources: The SSL Store

WANNA CRY

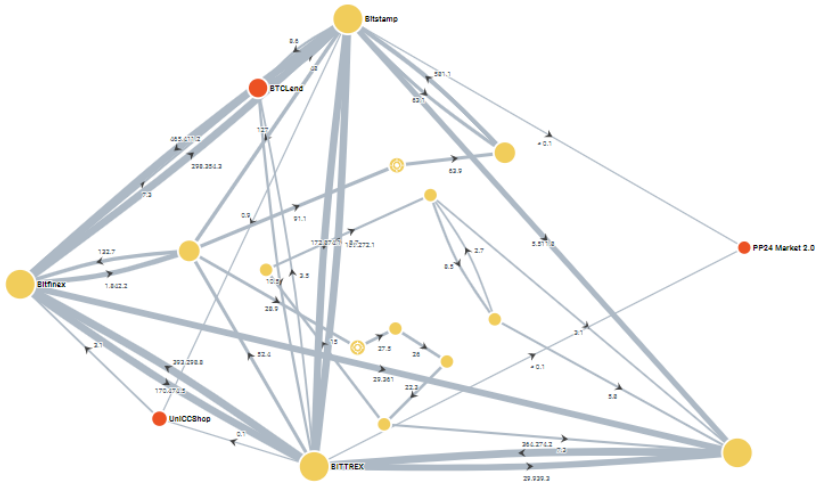
Allocate

TRACK

Transaktionsbaum

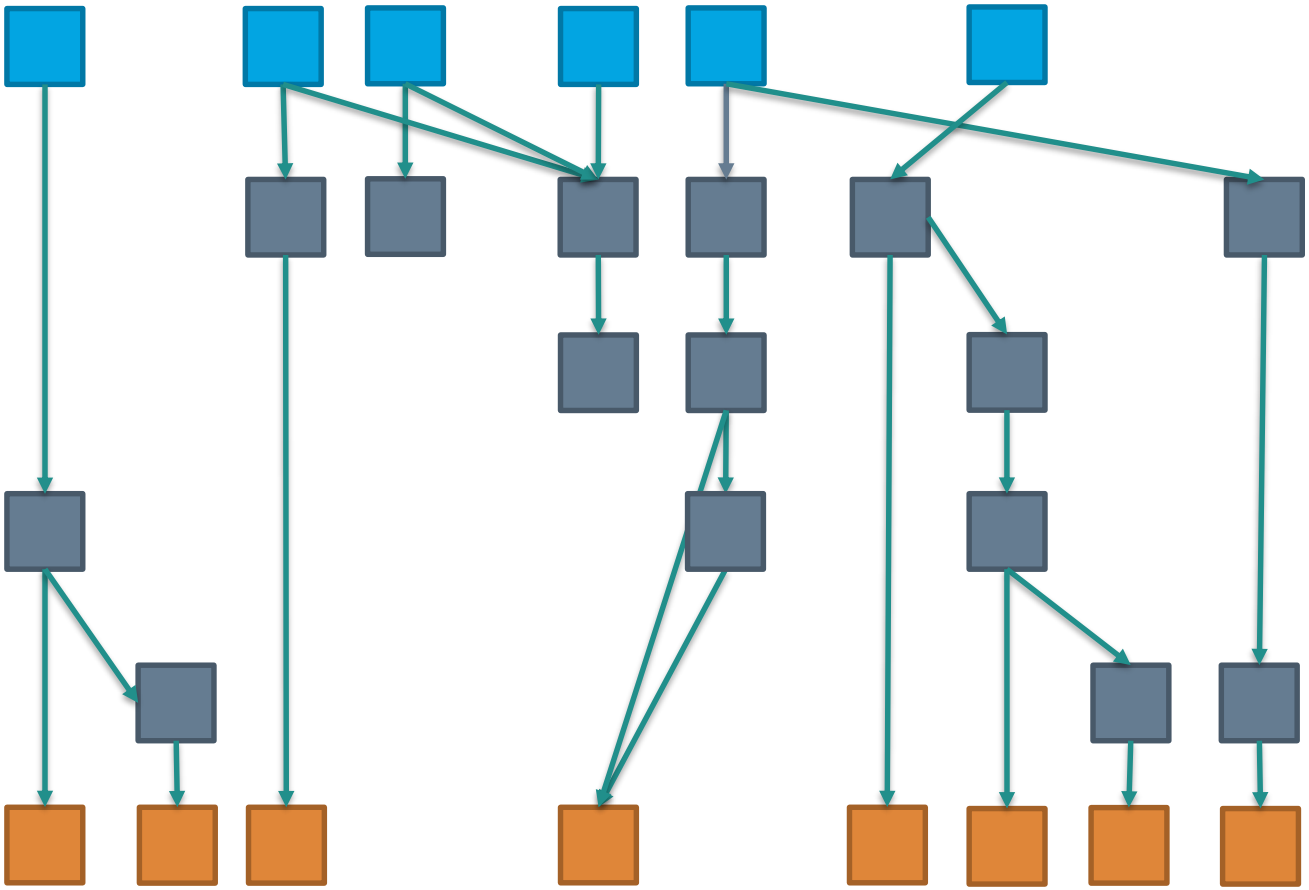


High-Potential Link



TRACK WANNA CRY

Split and mix – Exchange to privacy cryptocurrency



WannaCry main Addresses

Split and mix

Wechsel in Monero

BDO

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?