



Federal Police (Belgium)
FEDERAL COMPUTER CRIME UNIT
Christophe Landries



Kennistest



Aantal cryptocurrencies?

Criminele toepassingen

- Darknet marketplaces (~~AlphaBay~~, ~~HANSA Market~~)
- Ransomware
- Ontvoering en afpersing
- Witwassen
- Cryptojacking
- Etc.

TOP MARKETS!

Dream market - 98.27%

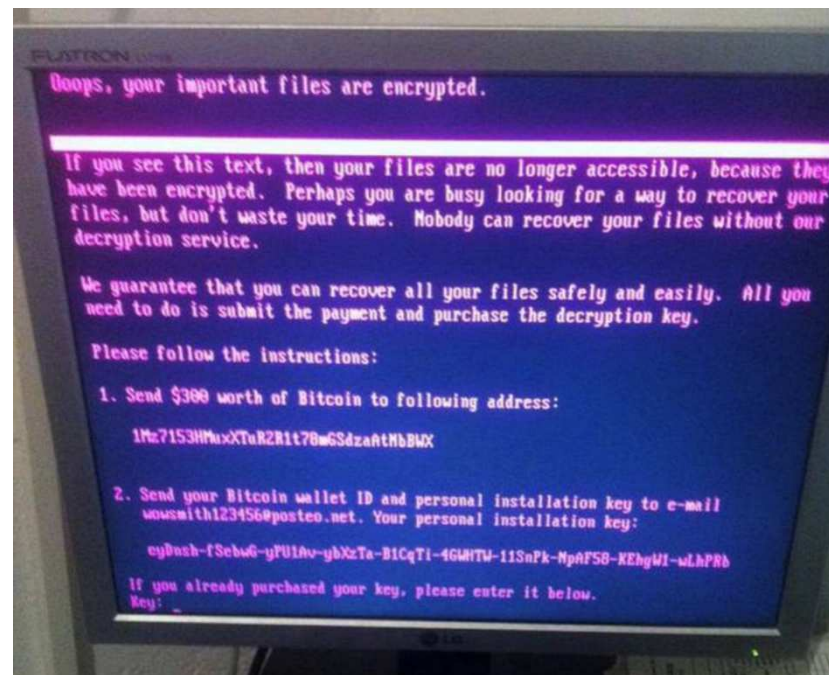
Wall Street Market - 97.72%

Point / T•chka Free Market - 92.98%

Bron: DeepDotWeb

Criminele toepassingen

- Voorbeeld NotPetya
 - Veel slachtoffers – grote schade



Bron: Wikipedia

Criminele toepassing

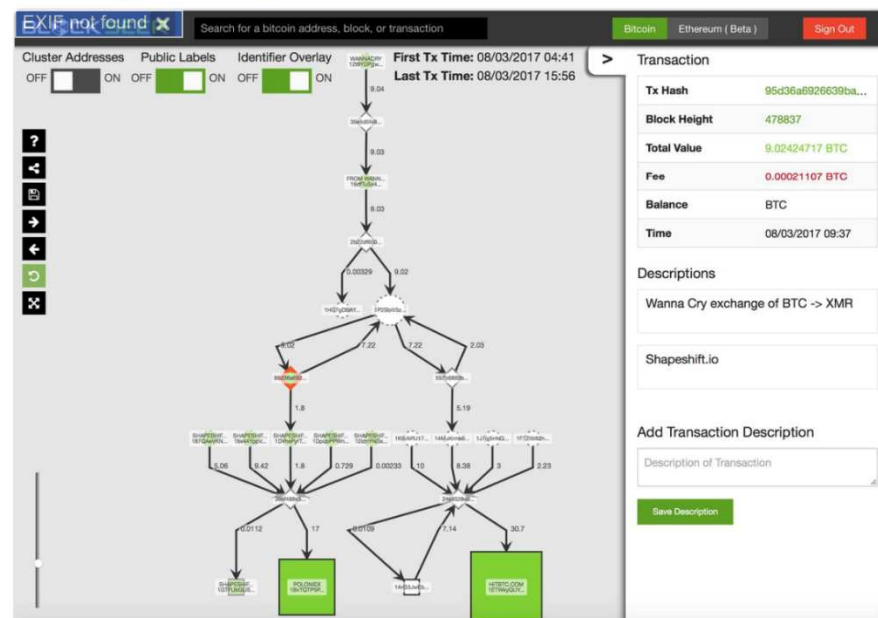
WannaCry



Bron: Wikipedia




Wanna Cry ransomware money laundering with Bitcoins in action. Graph shows Bitcoin being converted to Monero (XMR) via @ShapeShift_io











23:21 - 3 aug. 2017

Bron: BlockSeer

Cryptocurrencies

- Bitcoin 
 - Digitaal
 - Gedecentraliseerd
 - Niet gereguleerd
 - Pseudo-anoniem
 - Grenzeloos
 - Alle transacties in publiek grootboek (blockchain)
- Altcoins
 - Bv. privacy-focused  

Cryptocurrencies: 1926

- 1  Bitcoin
- 2  Ethereum
- 3  XRP
- 4  Bitcoin Cash
- 5  EOS
- 6  Stellar
- 7  Litecoin
- 8  Tether

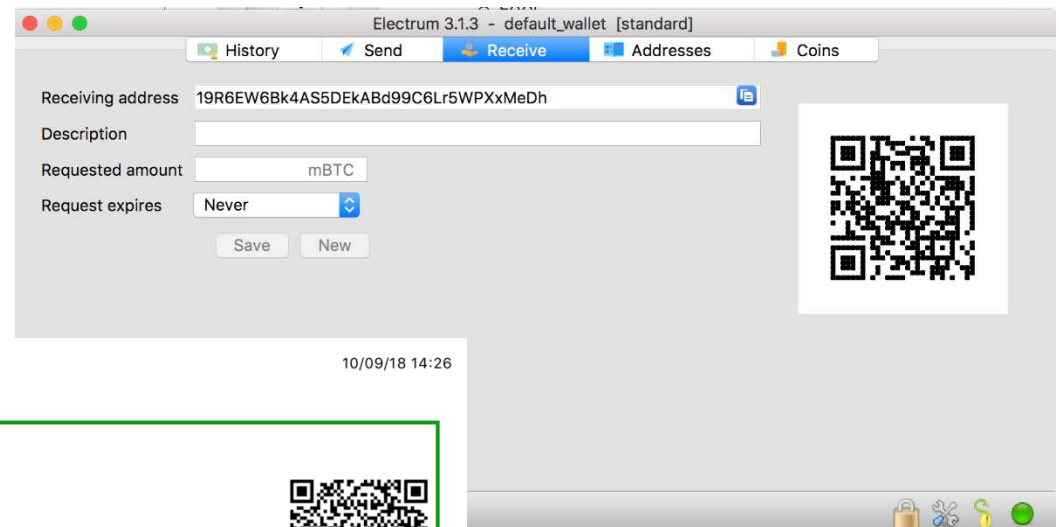
Bron: <https://coinmarketcap.com>

Bitcoin businesses

- Exchanges
- Payment processing
- Mining (pools)
- Darknet marketplaces
- Etc.

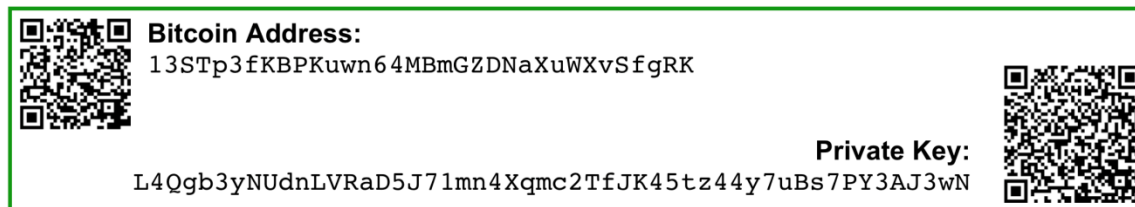
Wallet

- Verschillende soorten (paper, software, etc.)
 - Electrum
 - Paper
- Adressen



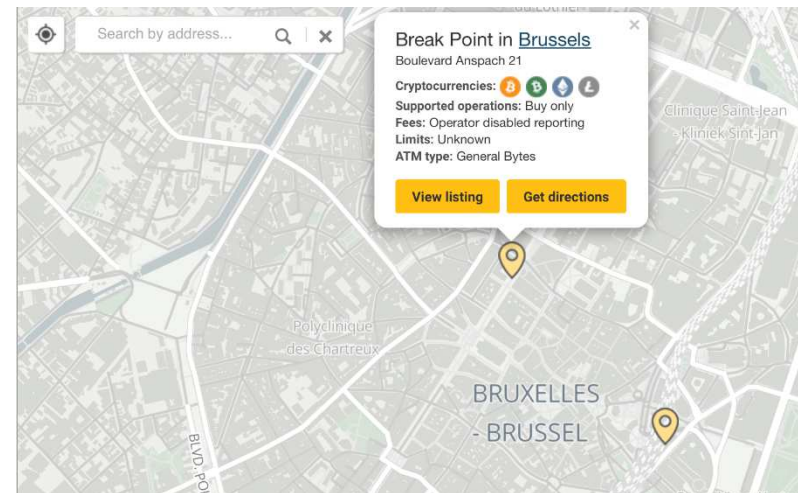
bitaddress.org

10/09/18 14:26



Transactie

- Aankoop/verkoop/betaling
 - Goederen en diensten
 - ATM
 - Exchanges (KYC)
 - Face-to-face



Bron: <https://coinatmradar.com>

Transactie

Transaction View information about a bitcoin transaction

[baf7908f77d577fc2596c94233b9af1e6e77e9b945e557d2d61c64648160170b](#)

[19afYX8D5G8nGVJte6z7png1gfeJaHdXid](#) (0.73989496 BTC - Output)



[1HL67PWtvZaQfDoxuGXivn8U5WJ76toceZ](#) - (Spent)
[19afYX8D5G8nGVJte6z7png1gfeJaHdXid](#) - (Unspent)

0.05 BTC
0.68986962 BTC

17 Confirmations

0.73986962 BTC

Summary

Size	225 (bytes)
Weight	900
Received Time	2018-05-03 08:26:01
Included In Blocks	521002 (2018-05-03 08:29:25 + 3 minutes)
Confirmations	17 Confirmations
Visualize	View Tree Chart

Inputs and Outputs

Total Input	0.73989496 BTC
Total Output	0.73986962 BTC
Fees	0.00002534 BTC
Fee per byte	11.262 sat/B
Fee per weight unit	2.816 sat/WU
Estimated BTC Transacted	0.05 BTC

Scripts

[Hide scripts & coinbase](#)

Bron: <https://www.blockchain.com/>

Blockchain

- Een blockchain bevat blokken
- Een blok bevat transacties

LAATSTE BLOCKS

Hoogte	Leeftijd	Transacties	Verzonden Totaal	Doorgegeven door
540949	8 minutes	2345	4,212.94 BTC	BTC.TOP
540948	13 minutes	2932	9,910.10 BTC	SlushPool
540947	19 minutes	2259	15,140.82 BTC	F2Pool
540946	54 minutes	370	1,183.36 BTC	BTC.TOP

Bron: <https://www.blockchain.com/>

Opsporingsmogelijkheden (kansen)

- Vooral onderzoek naar Bitcoin (BTC)
- Verschuiving naar privacy-focused cryptocurrencies? (Monero, Verge, Zcash, etc.) – shape-shifting
- Blockchain biedt kansen (blockchain explorers)
 - Publiek en doorzoekbaar <> Monero
 - Alle transacties worden geregistreerd

Opsporingsmogelijkheden (kansen)

- Follow the money
- OSINT (voorbeeld)
- Blockchain analyse
 - Open source tools
 - Commerciële tools
- Technieken (voorbeeld)
 - Clustering
 - Linking/attribution
- Potentiële identificatie (KYC)

Opsporingsmogelijkheden (kansen)

OSINT

WikiLeaks

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

[36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo](#)  

Monero is an open-source cryptocurrency that focuses on privacy, decentralisation and scalability. Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNote protocol and possesses significant algorithmic differences relating to blockchain obfuscation.

Monero users may choose to donate to us at:

[453VWT5GEkXGc2J9asRpXpRkjoCGKCJr96rndm2VMe5yECiAcUB3h8p](#) 

Bron: WikiLeaks

Opsporingsmogelijkheden (kansen)

Clustering (change adres)

Transactie Bekijk informatie over een bitcoin transactie

[aaa76683d8795fcfac068eb8e9d547bf3f5eb5cbfd96d030276797f493b72a89](#)

[1D2ajYcwJUwdD1BPM1rGNWhpbAsvPGFDjc](#)



[12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw](#)
[1DNpSvv8kmtKRitgBaJrxWWazCWvTd3NrM](#)

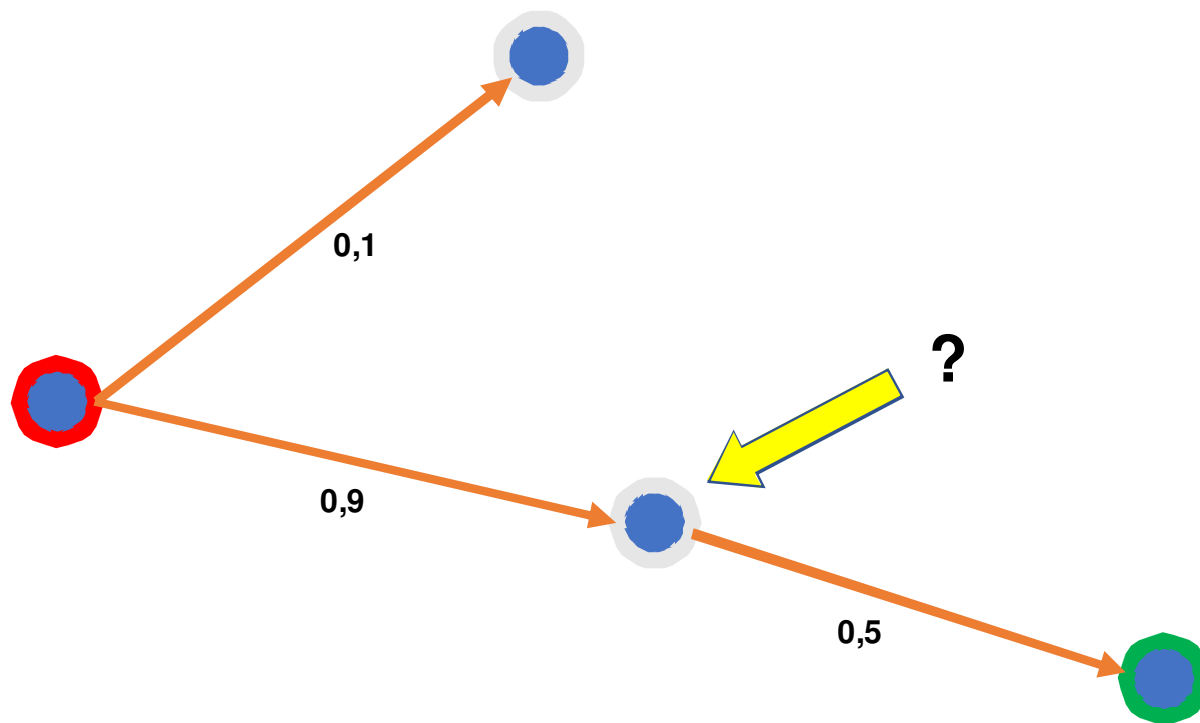
0.16321544 BTC
4.88899673 BTC

Bron: <https://www.blockchain.com/>

5.05221217 BTC

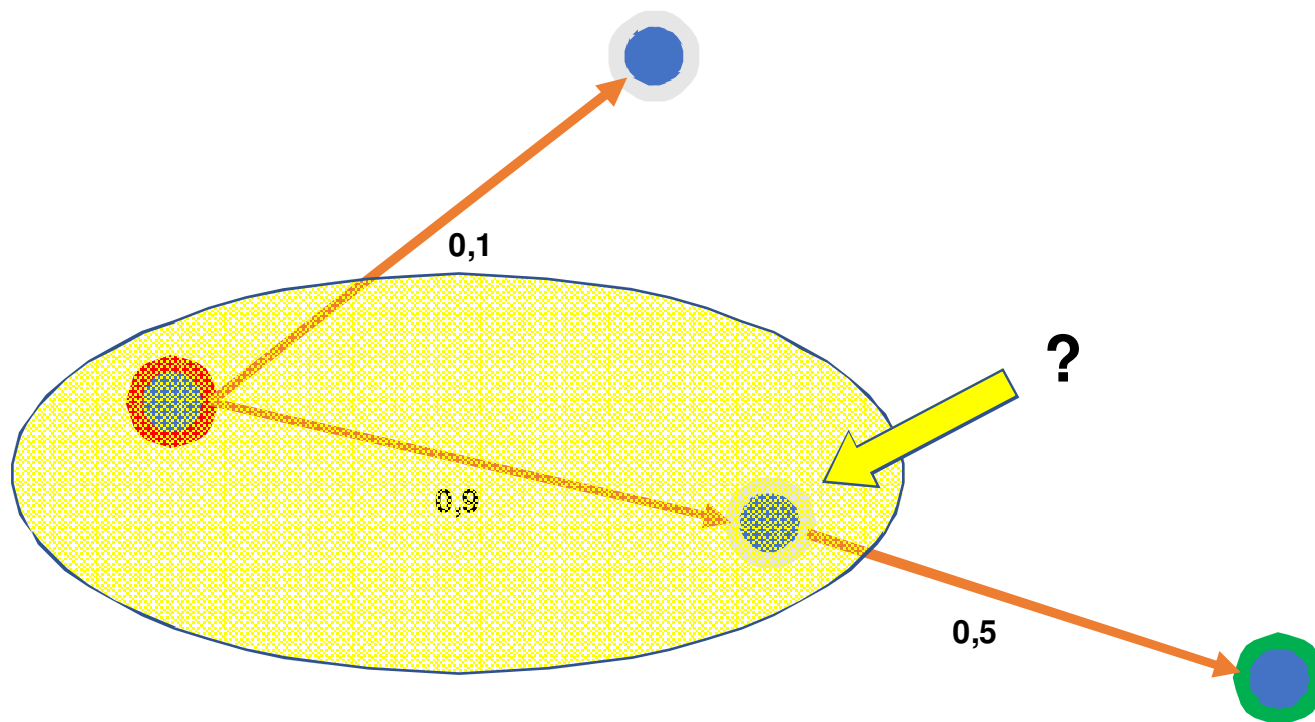
Opsporingsmogelijkheden (kansen)

Clustering & linking



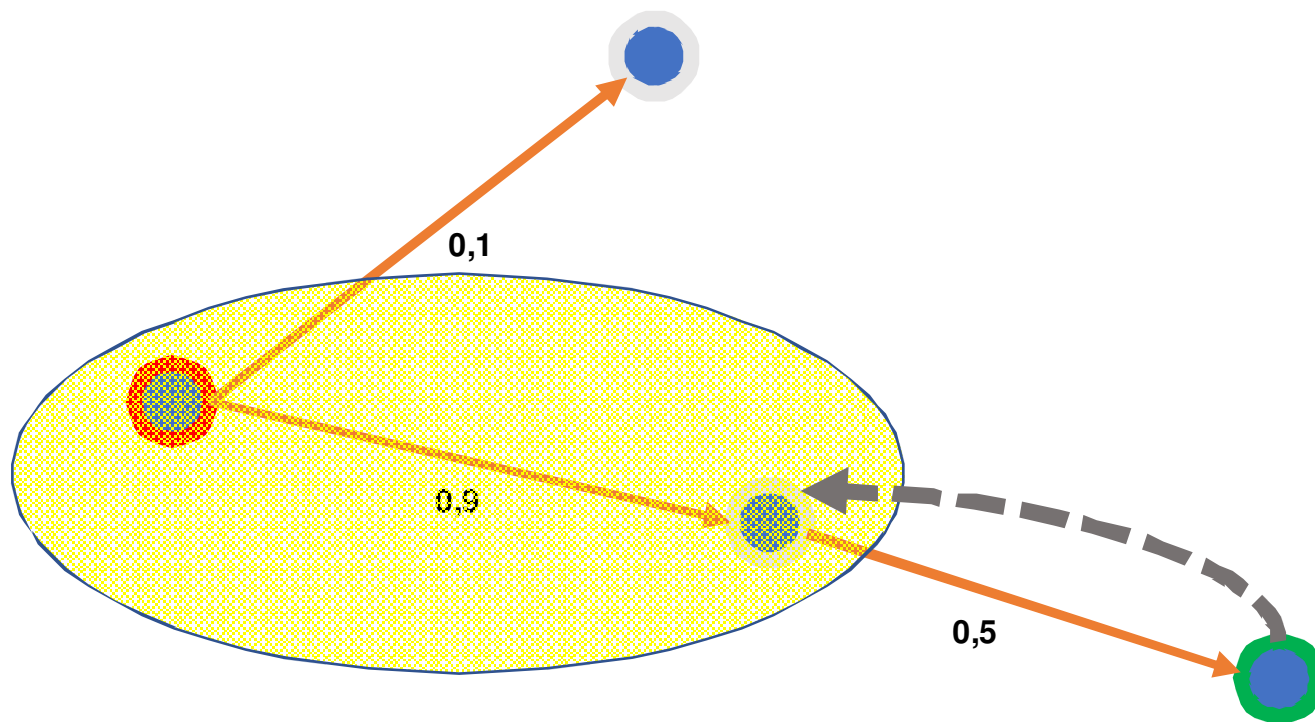
Opsporingsmogelijkheden (kansen)

Clustering & linking



Opsporingsmogelijkheden (kansen)

Clustering & linking



Opsporingsmogelijkheden (uitdagingen)

- Privacy-focused cryptocurrencies
- Mixers/tumblers/laundering (versluieren)
- Cryptojacking

