Cryptocurrencies and their impact on crime

A Brief History of Bitcoin/Crypto

- 2008 Satoshi Nakamoto publishes the Bitcoin whitepaper
- 2009 First Bitcoin transaction
- 2010 Lazlo Hanyecz paid 10,000 bitcoins for two delivered pizzas
- 2011 Bitcoin reached parity with the U.S. dollar for the first time (1 USD = 1 BTC)
- 2012 First Bitcoin Halving Day observed
- 2013 Total bitcoin market capitalization exceeded $1billion USD for the first time

A Brief History of Bitcoin/Crypto

- 2014 Tokyo-based bitcoin exchange Mt. Gox begins to collapse
- 2015 European Union issued its first ever ruling on bitcoin
- 2016 Bitfinex was hacked
- 2017 Japan categorized bitcoin as legal tender
- 2018 Bitcoin the price dropped 60%
- 2019 Hackers stole $41 million in BTC from Binance
- 2020 The third bitcoin halving occurred

Characteristics of Bitcoin and other Cryptocurrencies

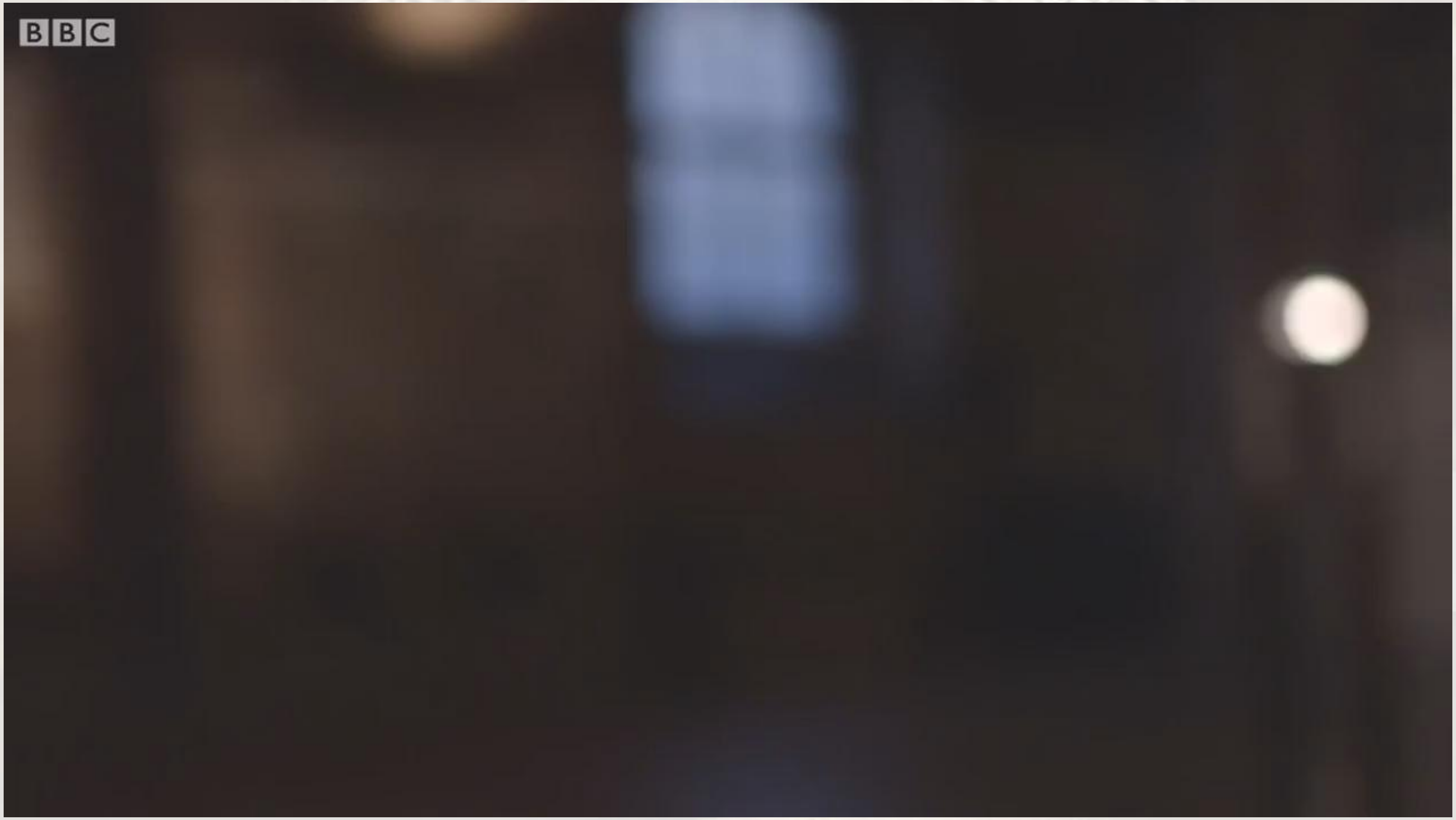
- **Private**

- **Decentralized**

- **Digital**

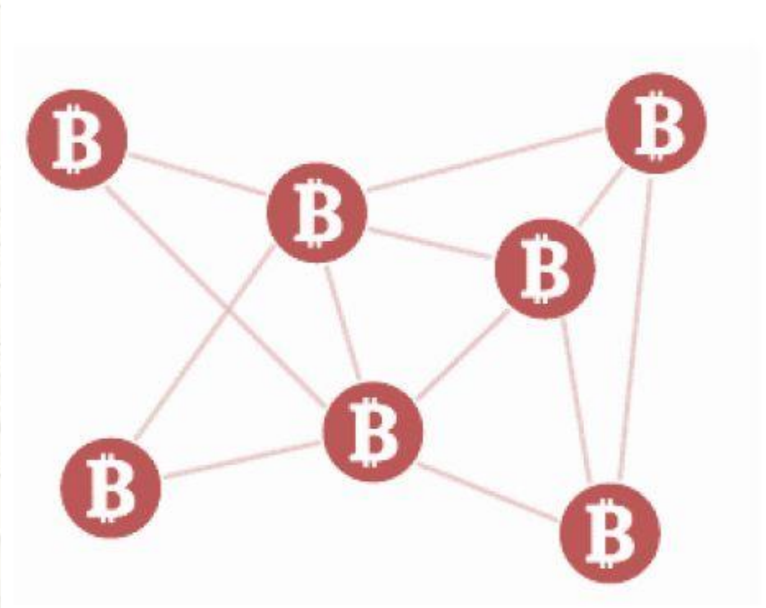
- **Cryptocurrency**

Classic bank payment / BTC payment



Bitcoin Blockchain

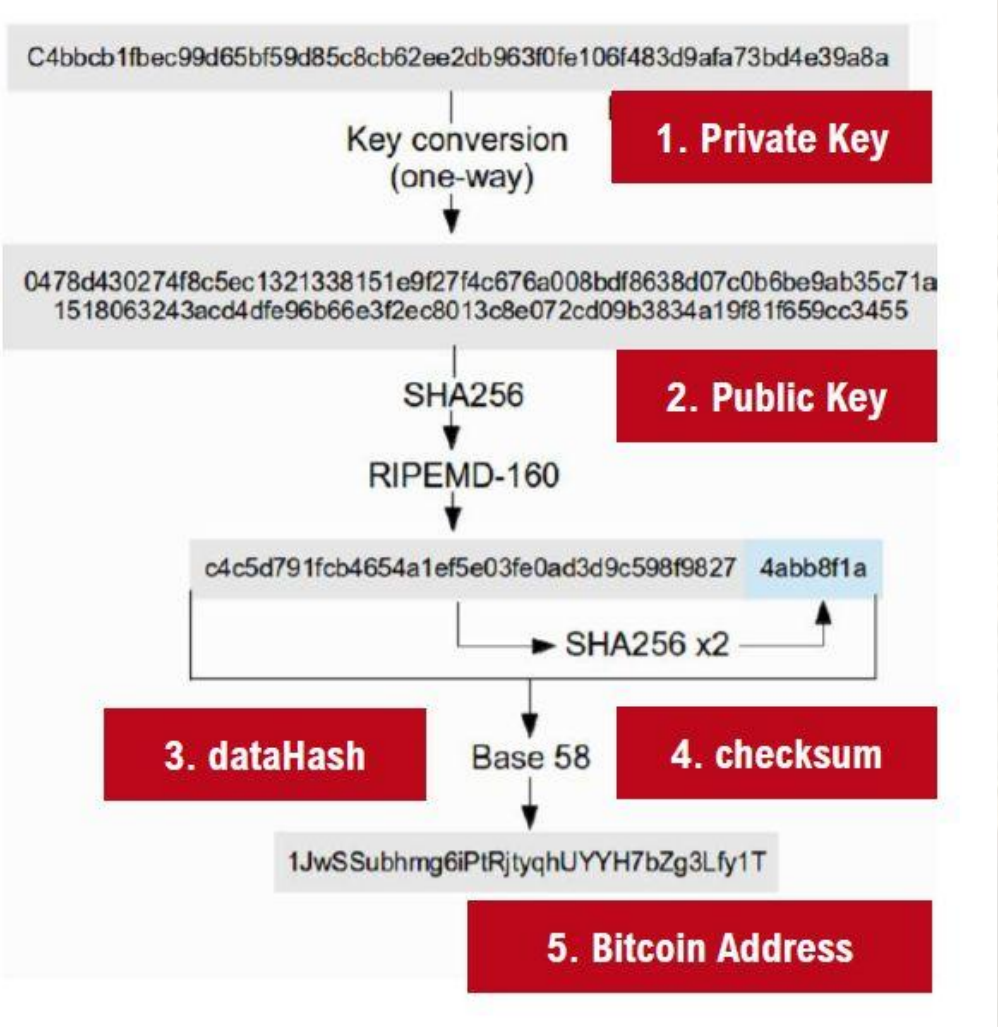
- **Highly durable**
- **Highly portable**
- **Highly fungible**
- **Highly divisible**
- **Highly resistant to counterfeiting**



Bitcoin and Cryptography

- A decentralized peer-to-peer network
- A public transaction ledger (the blockchain)
- Distributed mining and the “Proof-of-Work” consensus algorithm
- A decentralized transaction verification system
- Cryptographic hash functions
- Public Key Cryptography (i.e. ECDSA)

Generating a Bitcoin Address



C4bbcb1fbec99d65bf59d85c8cb62ee2db963f0fe106f483d9afa73bd4e39a8a

Key conversion
(one-way)

1. Private Key

0478d430274f8c5ec1321338151e9f27f4c676a008bdf8638d07c0b6be9ab35c71a
1518063243acd4dfe96b66e3f2ec8013c8e072cd09b3834a19f81f659cc3455

SHA256

2. Public Key

RIPEMD-160

c4c5d791fcb4654a1ef5e03fe0ad3d9c598f9827 4abb8f1a

SHA256 x2

3. dataHash

Base 58

4. checksum

1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T

5. Bitcoin Address

https://bitcoinpaperwallet.com

Cryptocurrencies

- Bitcoin
- Bitcoin Cash
- Litecoin
- Privacy Coins (Monero, Zcash, Dash, Grin)
- Ethereum (Platform)

Bitcoin (BTC)

- First Block: 3 January 2009
- Consensus Mechanism: Proof-of-Work
- Average Block Time: 10 minutes
- Total Supply Limit: 21 million bitcoin
- Current Circulating Supply: 18.57 million
- Market Capitalization #1: $430 billion (24 December 2020)

Source: https://coinmarketcap.com

Bitcoin Cash (BCH)

- 1 Aug 2017: Bitcoin Cash (BCH), also referred to as Bcash, emerged out of a hard fork of Bitcoin (BTC) prior to SegWit activation, due to a disagreement
- Consensus Mechanism: Proof-of-Work
- Average Block Time: 10 minutes
- Total Supply Limit: 21 million BCH
- Current Circulating Supply: 18.6 million
- Market Capitalization #6: $5,2 billion (24 December 2020)

Source: https://coinmarketcap.com

Litecoin

- 13 Oct 2011: Litecoin(LTC) went live as a Bitcoin fork.
- Rank: #5 with total market capitalization of $6,9 billion(24 Dec 2020).
- Total supply: 84 million.
- Average blocktime: 2.5 minutes.
- Consensus Mechanism: Proof-of-Work utilizing the ‘Scrypt’ algorithm which is an alternative to SHA-256usedinBitcoin.
- Litecoin was often referred to as the 'silver‘ to Bitcoin's digital 'gold.'

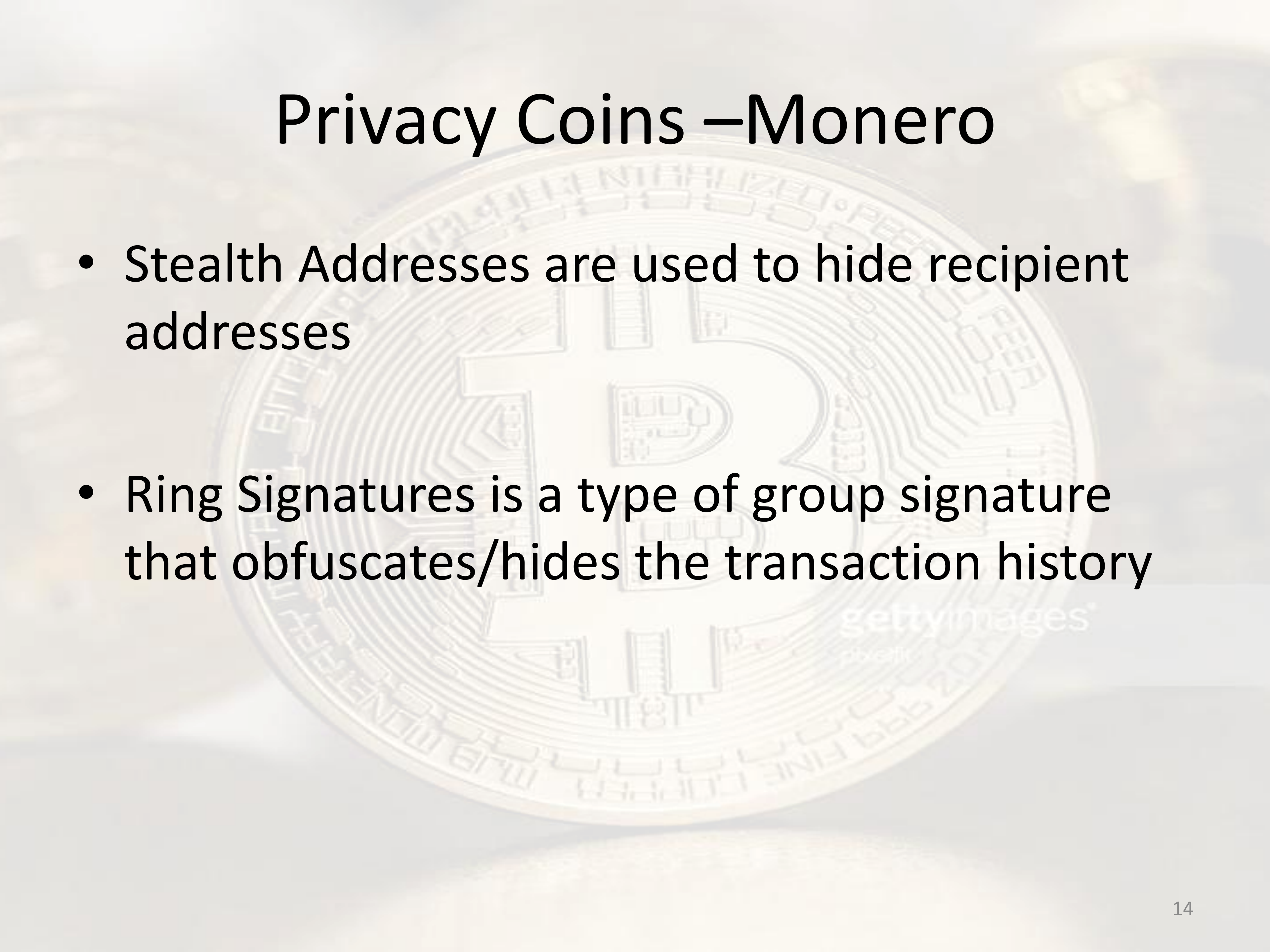
Source: https://coinmarketcap.com

Privacy Coins –Monero

- One of the most well-known privacy coins
- Rank: #14 with a total market capitalization of $2.8 billion (30 Dec 2020)
- Total supply: 17,788 million.
- Average blocktime: 2 minutes.
- Consensus Mechanism: Proof-of-Work
- Monero uses two techniques to make tracing difficult: Ring signatures and Stealth Addresses.

Source: https://coinmarketcap.com

Privacy Coins –Monero



- Stealth Addresses are used to hide recipient addresses

- Ring Signatures is a type of group signature that obfuscates/hides the transaction history

Privacy Coins –Dash

- First blocked mined on 18 Jan 2014.
- Rank: #31 with total market capitalization of $976 million (30 Dec 2020)

- Total supply: 18,9 million.
- Average blocktime: 2,6 minutes.
- Consensus Mechanism: Proof-of-Work
- Dash features: **InstantSend** and **PrivateSend**

Source: https://coinmarketcap.com

Privacy Coins –Zerocoin/Zerocash

- Rank: #38 with total market capitalization of $683 million (30 Dec 2020)
- Total supply: 21 million
- Average blocktime: 75 seconds.
- Consensus Mechanism: Zero-Knowledge-Proof
- Zerocash features: zk-SNARKs

Source: https://coinmarketcap.com

Ethereum

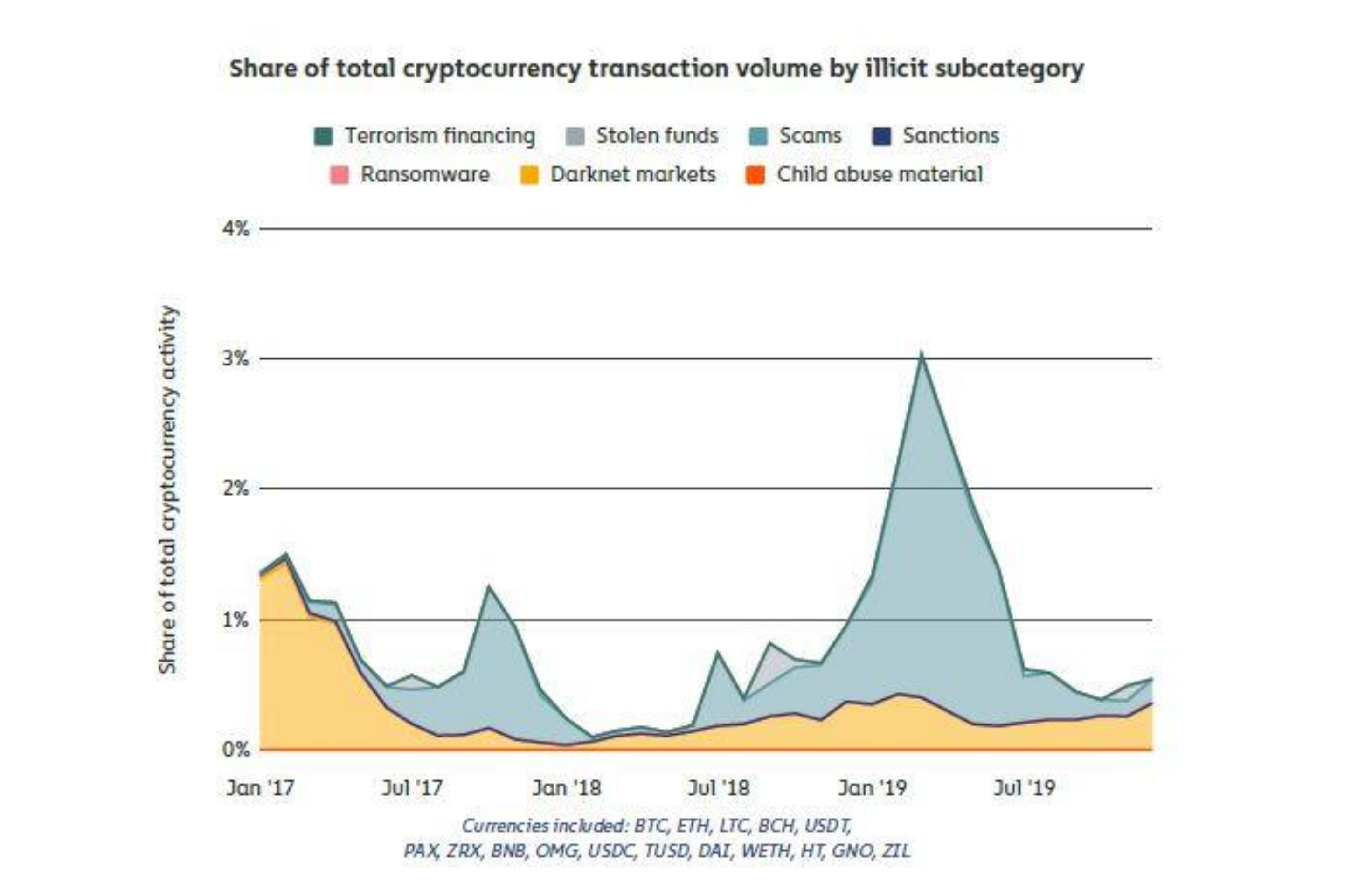
- Platform tokens – consumer tokens
- Genesis Block: 30 July 2015
- Rank #2 with total market capitalization: $111.2 billion (04 January 2021)
- Average Block Time: 13 seconds
- Total Supply Limit: None
- Current Circulating Supply: 114 million ether
- Consensus Mechanism: Proof-of-Work; shifted to Proof-of-Stake

Source: https://coinmarketcap.com

Criminal use of Cryptocurrencies*

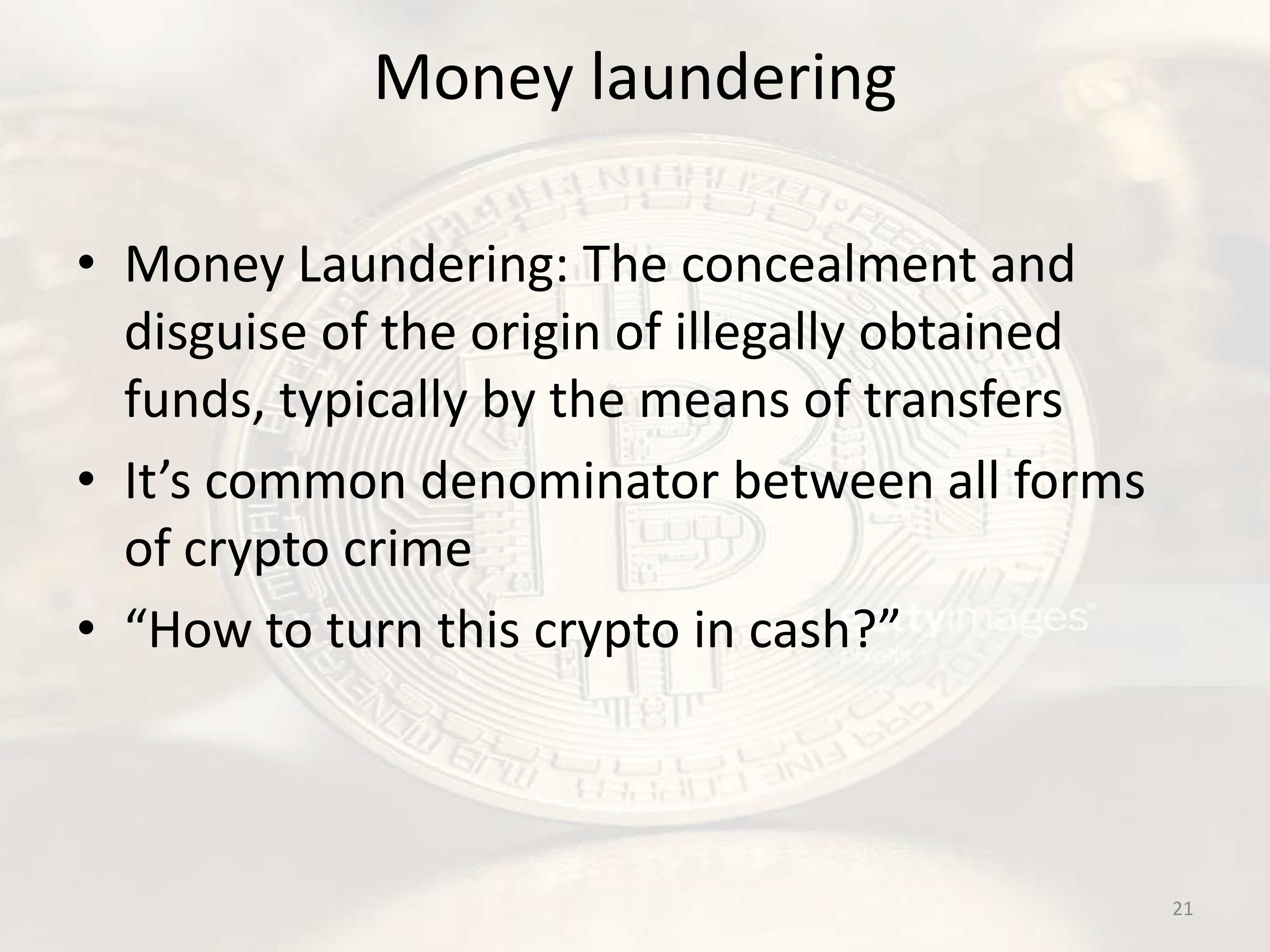
- Money laundering
- Scams
- Ransomware
- Hacks (cryptocurrency theft)
- Darknet Markets
- Terrorism Financing

*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html



*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html

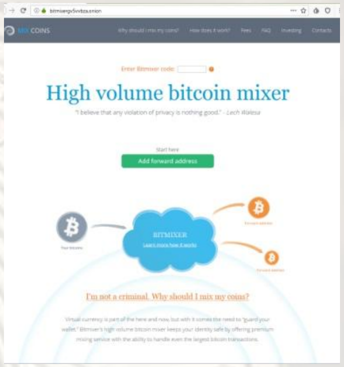
Money laundering



- Money Laundering: The concealment and disguise of the origin of illegally obtained funds, typically by the means of transfers
- It’s common denominator between all forms of crypto crime
- “How to turn this crypto in cash?”

Money laundering

- Mixers and Coin Join services



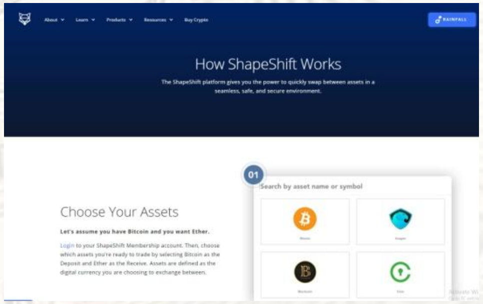
High volume bitcoin mixer

"I believe that any violation of privacy is nothing good." - *Lech Wałęsa*

I'm not a criminal. Why should I mix my coins?

Virtual currency is part of the here and now, but with it comes the need to "guard your wallet." Bitmixer's high volume bitcoin mixer keeps your identity safe by offering premium mixing service with the ability to handle even the largest bitcoin transactions.

- Shift BTC-Altcoins-BTC



How ShapeShift Works

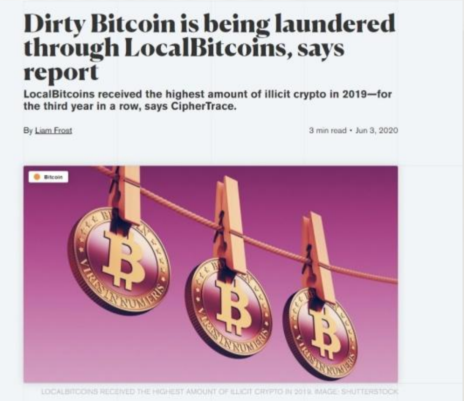
The ShapeShift platform gives you the power to quickly swap between assets in a seamless, safe, and secure environment.

Choose Your Assets

Let's assume you have Bitcoin and you want Ether.

Login to your ShapeShift Membership account. Then, choose which assets you're ready to trade by selecting Bitcoin as the Deposit and Ether as the Receive. Assets are defined as the digital currency you are choosing to exchange between.

- Using Local Bitcoin exchange



Dirty Bitcoin is being laundered through LocalBitcoins, says report

LocalBitcoins received the highest amount of illicit crypto in 2019—for the third year in a row, says CipherTrace.

By Liam Frost

3 min read • Jun 3, 2020

LOCALBITCOINS RECEIVED THE HIGHEST AMOUNT OF ILLICIT CRYPTO IN 2019. IMAGE: SHUTTERSTOCK

Scams

- Biggest treat in crypto crime
- Reason is because crypto world sent message: “get rich quick”
- Ponzi schemes – 92% in 2019*
- Sextortion (Blackmail) scam

*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html

Ponzi schemes

- A **Ponzi scheme** (also a **Ponzi game**) is a form of fraud that lures investors and pays profits to earlier investors with funds from more recent investors

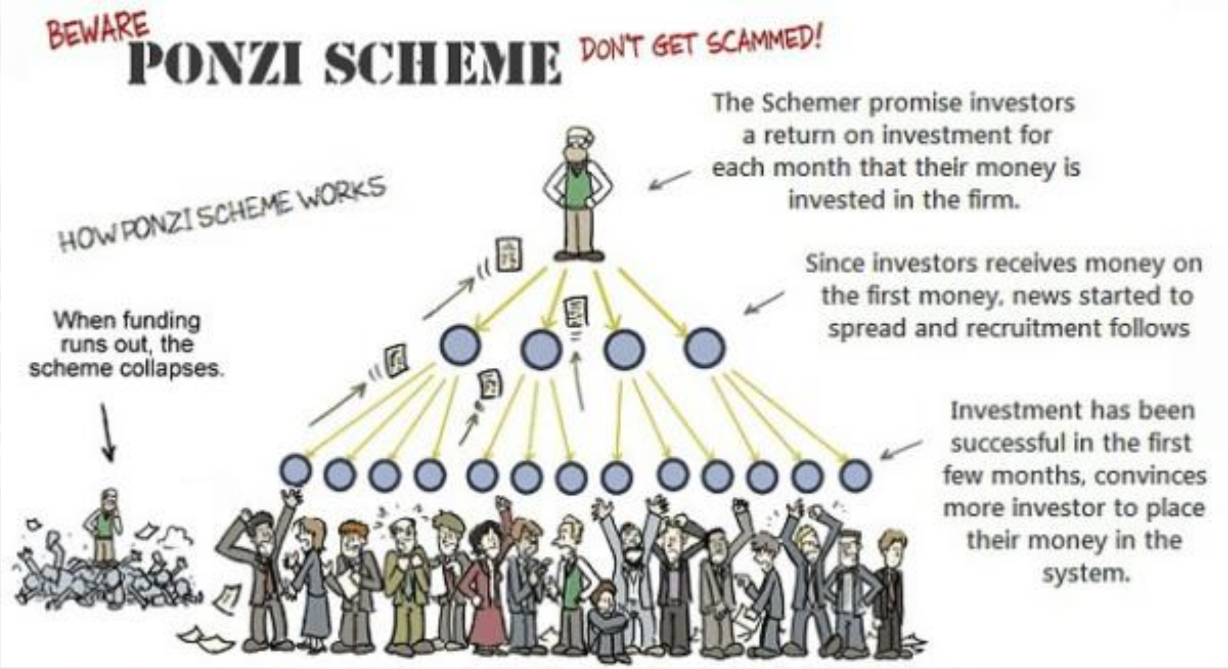
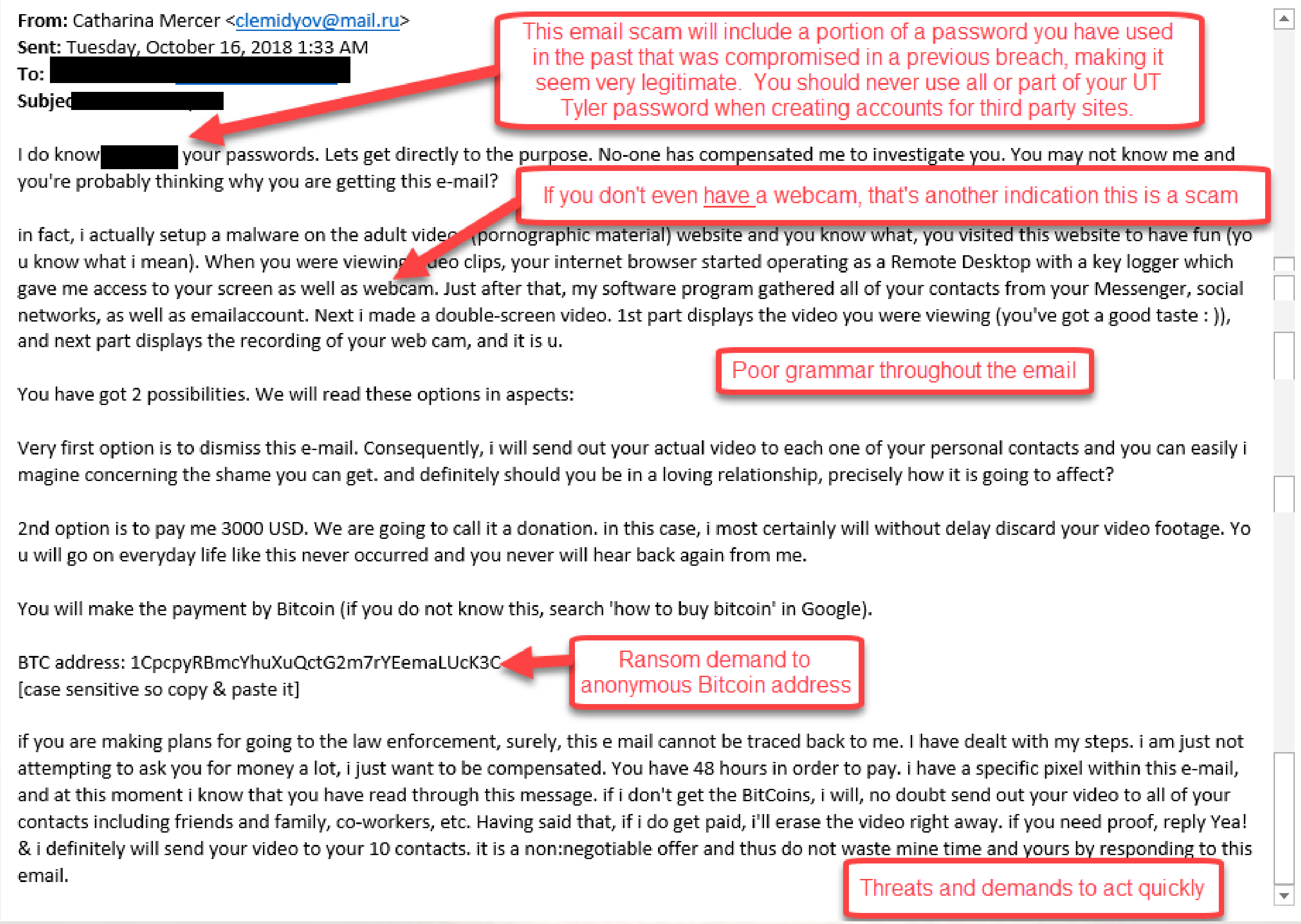

BEWARE
PONZI SCHEME
DON'T GET SCAMMED!
HOW PONZI SCHEME WORKS
The Schemer promise investors a return on investment for each month that their money is invested in the firm.
Since investors receives money on the first money, news started to spread and recruitment follows
Investment has been successful in the first few months, convinces more investor to place their money in the system.
When funding runs out, the scheme collapses.

Image Source: https://coinclarity.com/thursday-checkup-4-5-18/

Sextortion scam



From: Catharina Mercer <clemidyov@mail.ru>
Sent: Tuesday, October 16, 2018 1:33 AM
To: [redacted]
Subjec [redacted]

This email scam will include a portion of a password you have used in the past that was compromised in a previous breach, making it seem very legitimate. You should never use all or part of your UT Tyler password when creating accounts for third party sites.

I do know [redacted] your passwords. Lets get directly to the purpose. No-one has compensated me to investigate you. You may not know me and you're probably thinking why you are getting this e-mail?

If you don't even have a webcam, that's another indication this is a scam

in fact, i actually setup a malware on the adult video (pornographic material) website and you know what, you visited this website to have fun (you know what i mean). When you were viewing video clips, your internet browser started operating as a Remote Desktop with a key logger which gave me access to your screen as well as webcam. Just after that, my software program gathered all of your contacts from your Messenger, social networks, as well as emailaccount. Next i made a double-screen video. 1st part displays the video you were viewing (you've got a good taste :)), and next part displays the recording of your web cam, and it is u.

Poor grammar throughout the email

You have got 2 possibilities. We will read these options in aspects:

Very first option is to dismiss this e-mail. Consequently, i will send out your actual video to each one of your personal contacts and you can easily imagine concerning the shame you can get. and definitely should you be in a loving relationship, precisely how it is going to affect?

2nd option is to pay me 3000 USD. We are going to call it a donation. in this case, i most certainly will without delay discard your video footage. You will go on everyday life like this never occurred and you never will hear back again from me.

You will make the payment by Bitcoin (if you do not know this, search 'how to buy bitcoin' in Google).

BTC address: 1CpcpyRBmcYhuXuQctG2m7rYEemaLUcK3C
[case sensitive so copy & paste it]

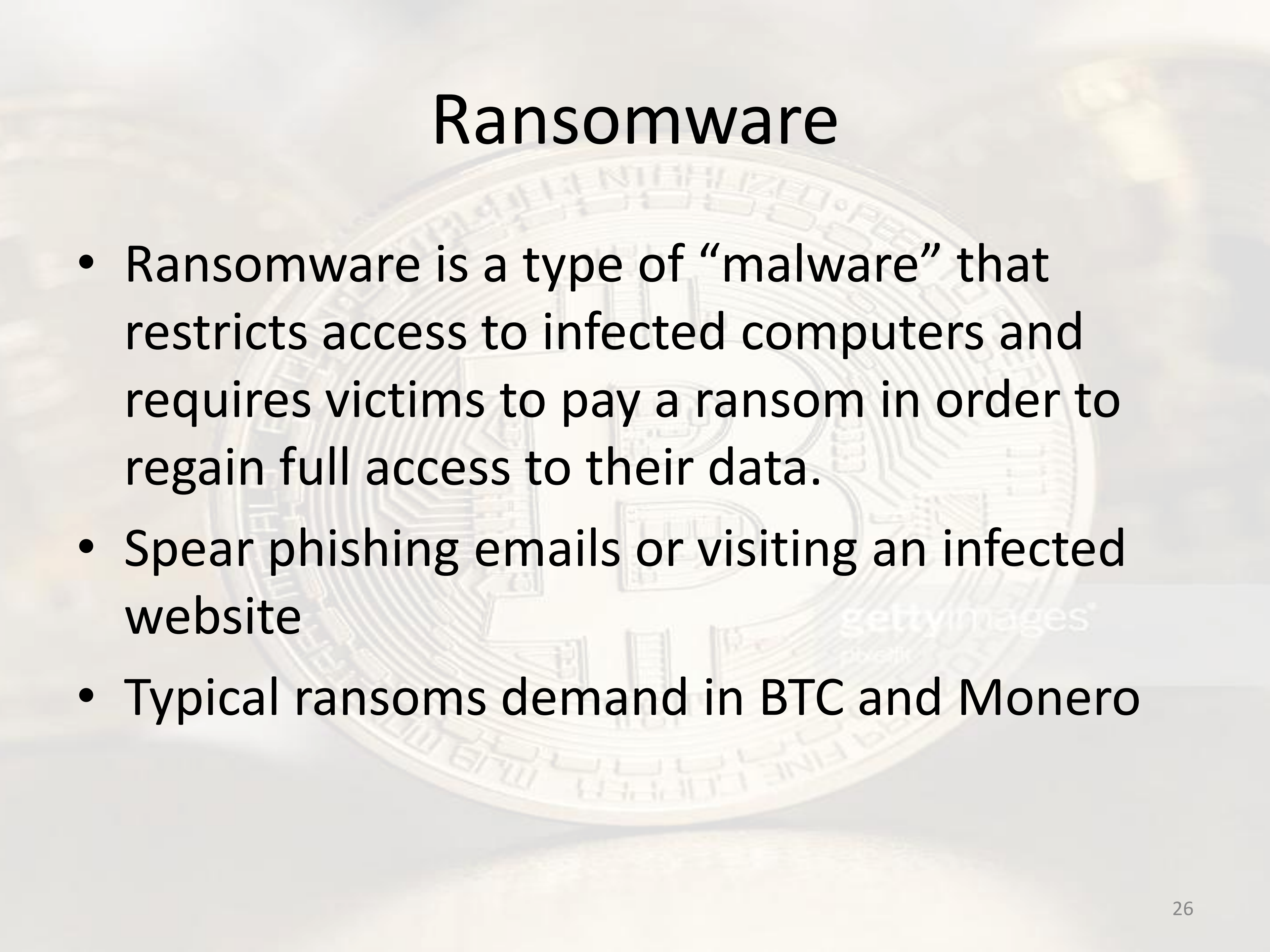
Ransom demand to anonymous Bitcoin address

if you are making plans for going to the law enforcement, surely, this e mail cannot be traced back to me. I have dealt with my steps. i am just not attempting to ask you for money a lot, i just want to be compensated. You have 48 hours in order to pay. i have a specific pixel within this e-mail, and at this moment i know that you have read through this message. if i don't get the BitCoins, i will, no doubt send out your video to all of your contacts including friends and family, co-workers, etc. Having said that, if i do get paid, i'll erase the video right away. if you need proof, reply Yea! & i definitely will send your video to your 10 contacts. it is a non:negotiable offer and thus do not waste mine time and yours by responding to this email.

Threats and demands to act quickly

Image Source: https://www.uttyler.edu/iso/phishwebcamvideo.php

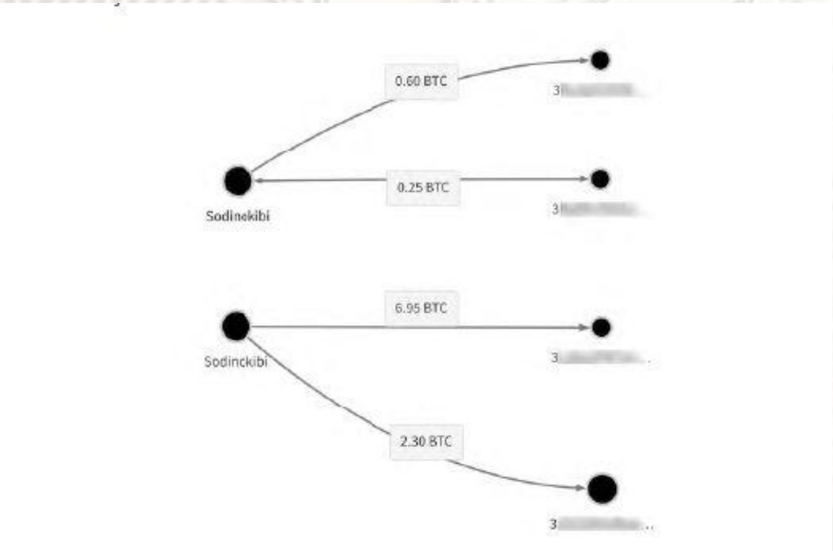
Ransomware



- Ransomware is a type of “malware” that restricts access to infected computers and requires victims to pay a ransom in order to regain full access to their data.
- Spear phishing emails or visiting an infected website
- Typical ransoms demand in BTC and Monero

RaaS

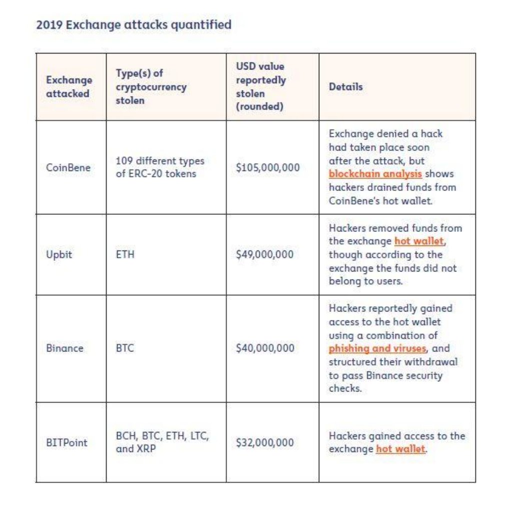
- Hackers who develop ransomware technology now allow less sophisticated hackers to rent access to it-Ransomware as a service (RaaS)*



*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html

Hacks (cryptocurrency theft)

- **Exchange Hack- Mt Gox, KuCoin***



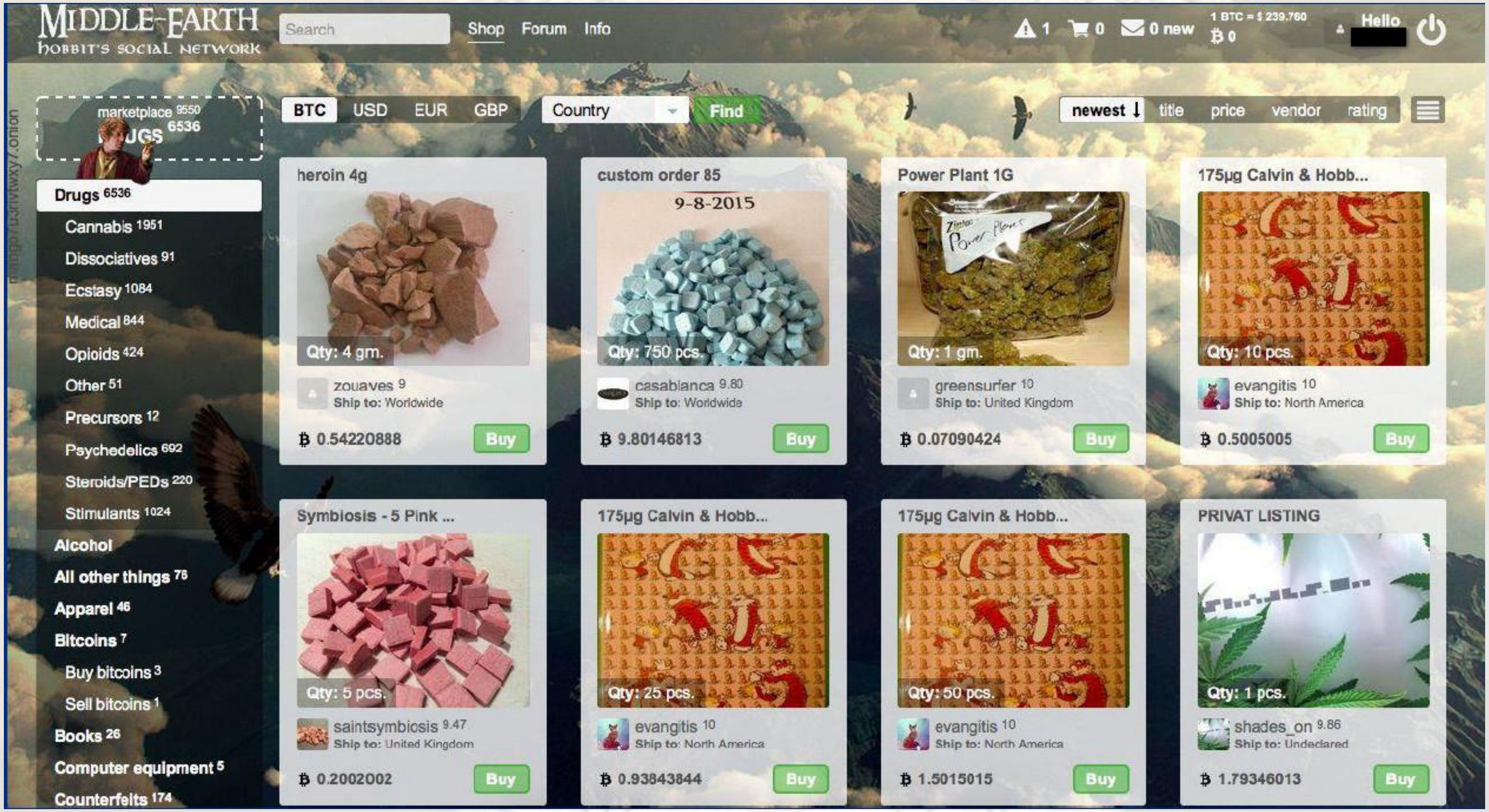
2019 Exchange attacks quantified

Exchange attacked	Type(s) of cryptocurrency stolen	USD value reportedly stolen (rounded)	Details
CoinBene	109 different types of ERC-20 tokens	$105,000,000	Exchange denied a hack had taken place soon after the attack, but blockchain analysis shows hackers drained funds from CoinBene's hot wallet.
Upbit	ETH	$49,000,000	Hackers removed funds from the exchange hot wallet, though according to the exchange the funds did not belong to users.
Binance	BTC	$40,000,000	Hackers reportedly gained access to the hot wallet using a combination of phishing and viruses, and structured their withdrawal to pass Binance security checks.
BITPoint	BCH, BTC, ETH, LTC, and XRP	$32,000,000	Hackers gained access to the exchange hot wallet.

- **Personal Hack – Trojans, Social Engineering**

*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html

Darknet Markets



MIDDLE-EARTH
HOBBIT'S SOCIAL NETWORK

Search · Shop · Forum · Info

⚠ 1 · 🛒 0 · ✉ 0 new · 1 BTC = $ 239.760 · ฿ 0 · Hello [redacted]

BTC · USD · EUR · GBP · Country · Find

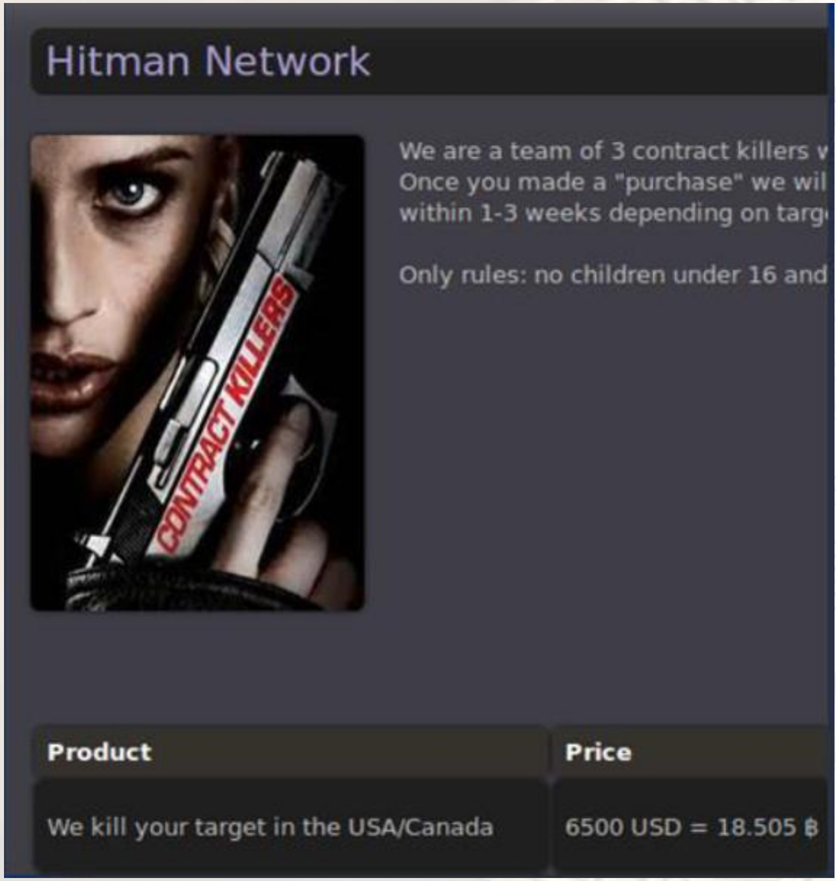
newest ↓ · title · price · vendor · rating

marketplace 9550
DRUGS 6536

- Drugs 6536
  - Cannabis 1951
  - Dissociatives 91
  - Ecstasy 1084
  - Medical 844
  - Opioids 424
  - Other 51
  - Precursors 12
  - Psychedelics 692
  - Steroids/PEDs 220
  - Stimulants 1024
- Alcohol
- All other things 75
- Apparel 46
- Bitcoins 7
  - Buy bitcoins 3
  - Sell bitcoins 1
- Books 26
- Computer equipment 5
- Counterfeits 174

Listing	Qty	Vendor	Ship to	Price
heroin 4g	Qty: 4 gm.	zouaves 9	Worldwide	฿ 0.54220888
custom order 85	Qty: 750 pcs.	casablanca 9.80	Worldwide	฿ 9.80146813
Power Plant 1G	Qty: 1 gm.	greensurfer 10	United Kingdom	฿ 0.07090424
175µg Calvin & Hobb...	Qty: 10 pcs.	evangitis 10	North America	฿ 0.5005005
Symbiosis - 5 Pink ...	Qty: 5 pcs.	saintsymbiosis 9.47	United Kingdom	฿ 0.2002002
175µg Calvin & Hobb...	Qty: 25 pcs.	evangitis 10	North America	฿ 0.93843844
175µg Calvin & Hobb...	Qty: 50 pcs.	evangitis 10	North America	฿ 1.5015015
PRIVAT LISTING	Qty: 1 pcs.	shades_on 9.86	Undeclared	฿ 1.79346013

Darknet Markets

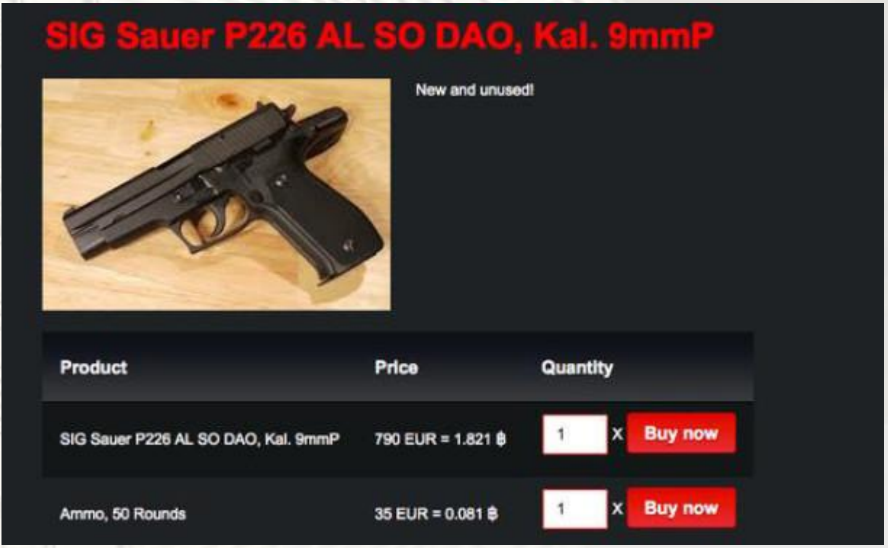


Hitman Network

We are a team of 3 contract killers v
Once you made a "purchase" we wil
within 1-3 weeks depending on targ

Only rules: no children under 16 and

Product	Price
We kill your target in the USA/Canada	6500 USD = 18.505 ฿

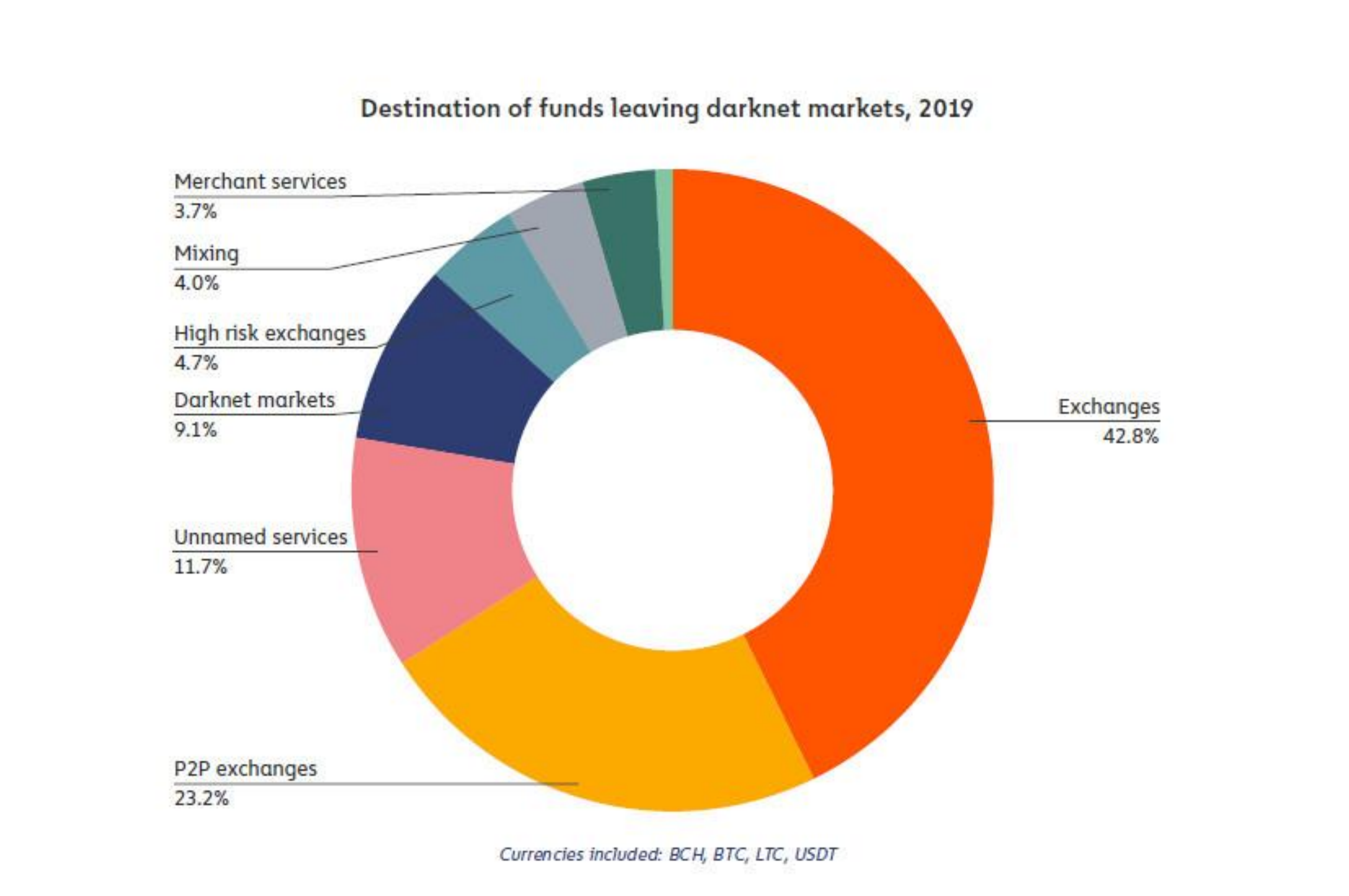


SIG Sauer P226 AL SO DAO, Kal. 9mmP

New and unused!

Product	Price	Quantity
SIG Sauer P226 AL SO DAO, Kal. 9mmP	790 EUR = 1.821 ฿	1 x Buy now
Ammo, 50 Rounds	35 EUR = 0.081 ฿	1 x Buy now

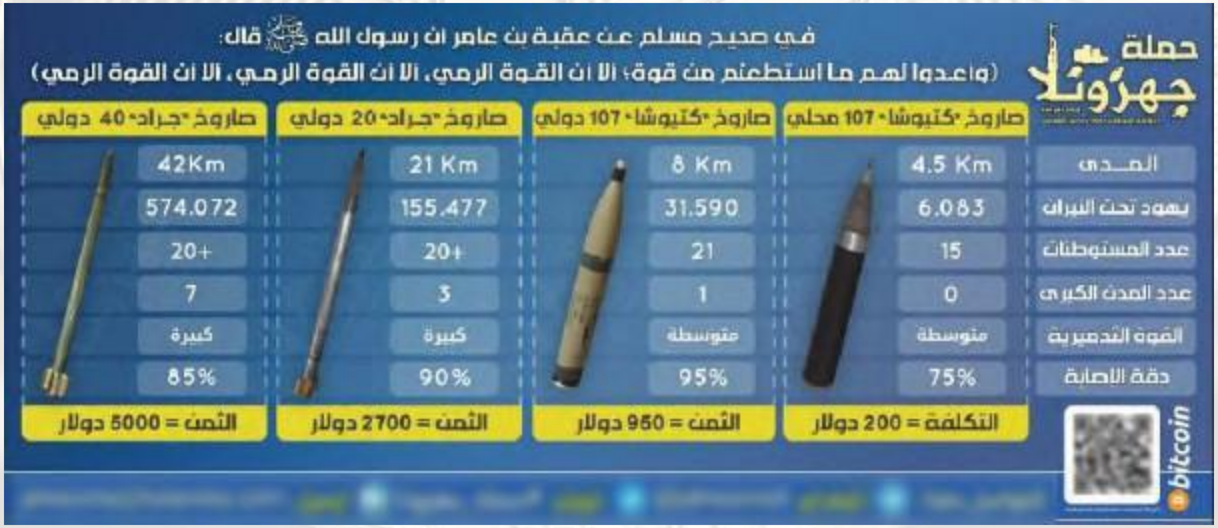
Darknet Markets



*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html

Terrorism Financing

- Terrorists have found in cryptocurrencies a great way for their hidden financing



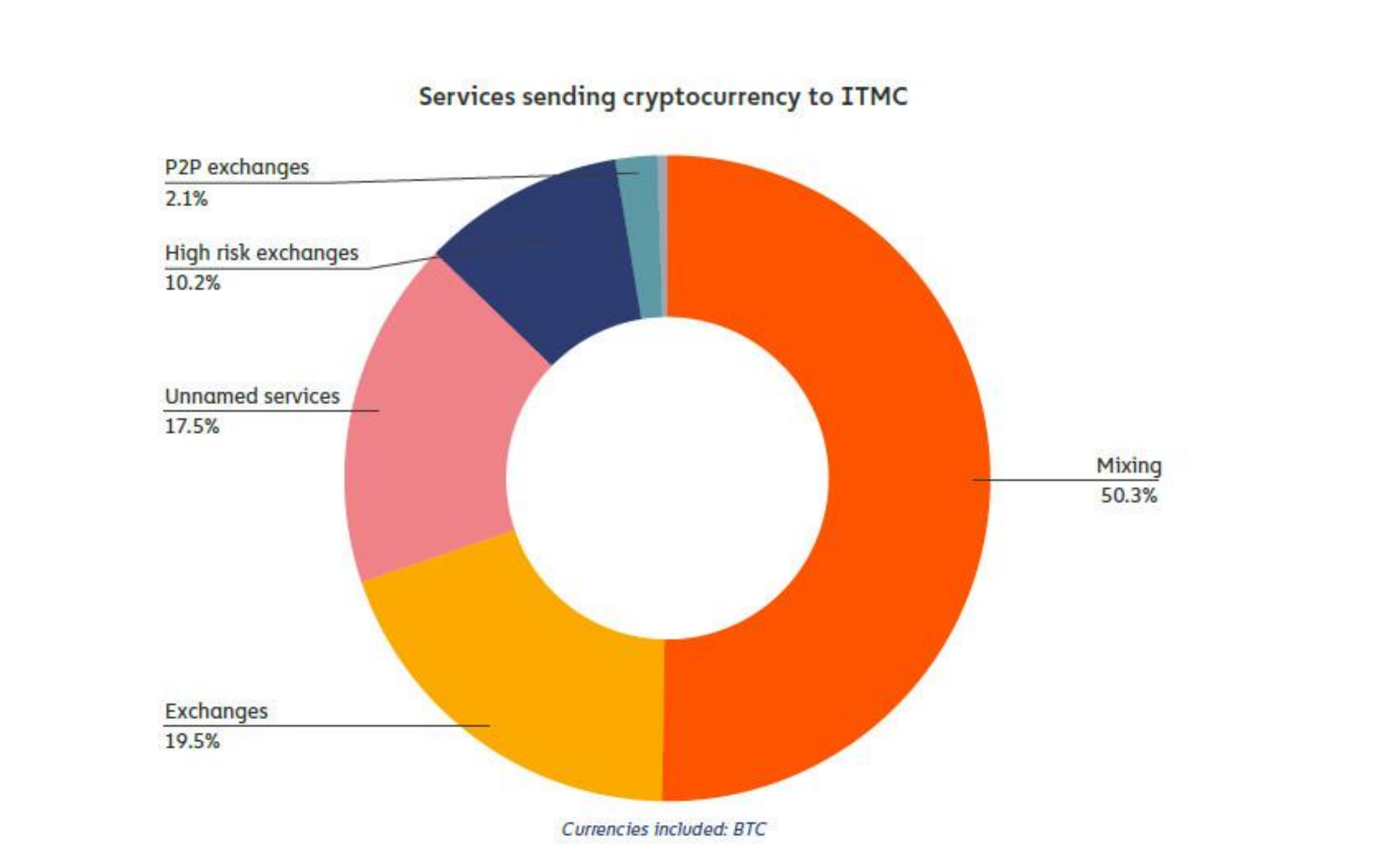
حملة جهزونا

في صحيح مسلم عن عقبة بن عامر ان رسول الله ﷺ قال:

(واعدوا لهم ما استطعتم من قوة؛ الا ان القوة الرمي، الا ان القوة الرمي، الا ان القوة الرمي)

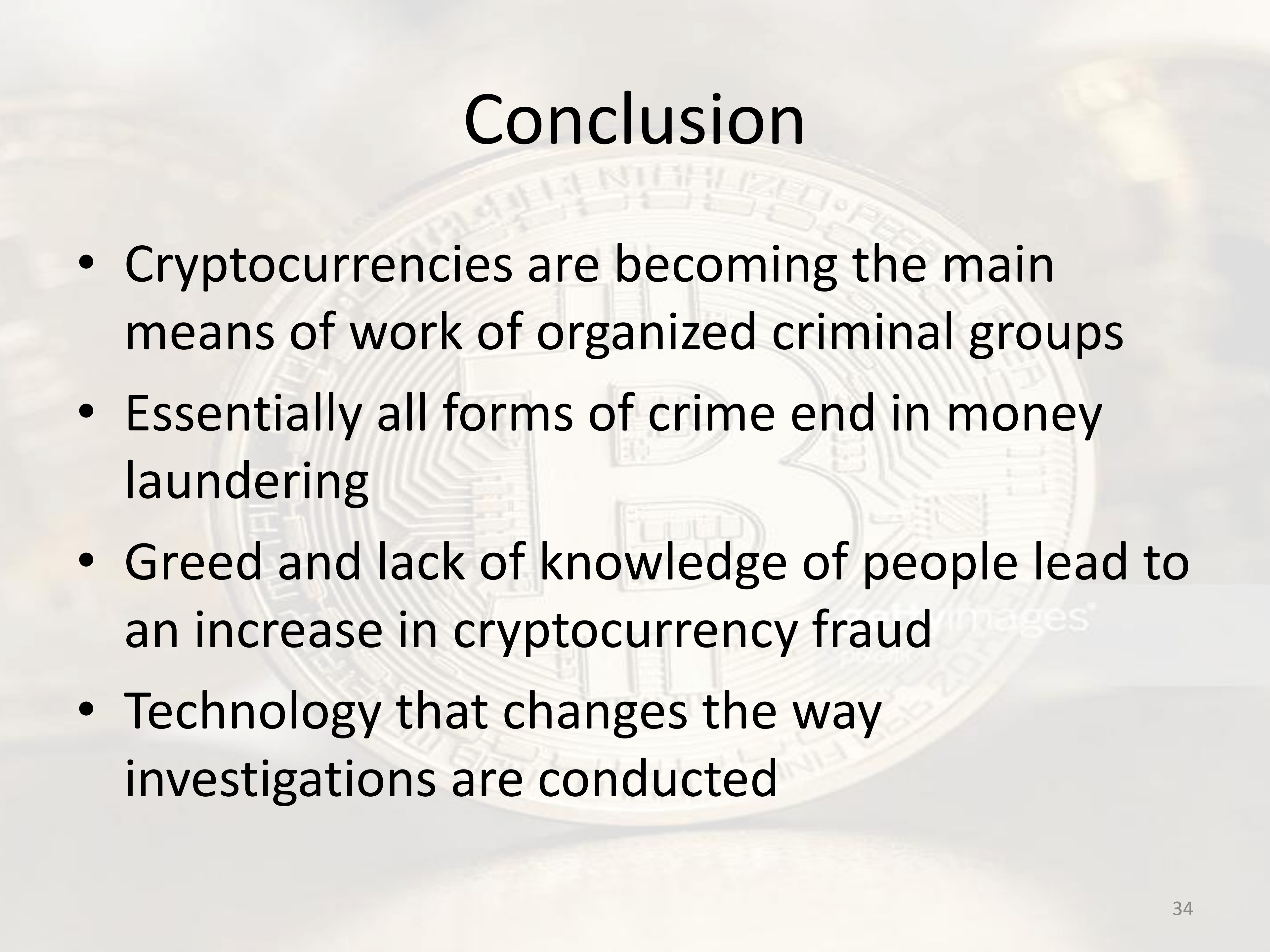
	صاروخ "كتيوشا" 107 محلي	صاروخ "كتيوشا" 107 دولي	صاروخ "جراد" 20 دولي	صاروخ "جراد" 40 دولي
المدى	4.5 Km	8 Km	21 Km	42Km
يهود تحت النيران	6.083	31.590	155.477	574.072
عدد المستوطنات	15	21	20+	20+
عدد المدن الكبرى	0	1	3	7
القوة التدميرية	متوسطة	متوسطة	كبيرة	كبيرة
دقة الاصابة	75%	95%	90%	85%
	التكلفة = 200 دولار	الثمن = 950 دولار	الثمن = 2700 دولار	الثمن = 5000 دولار

Ibn Taymiyyah Media Center’s



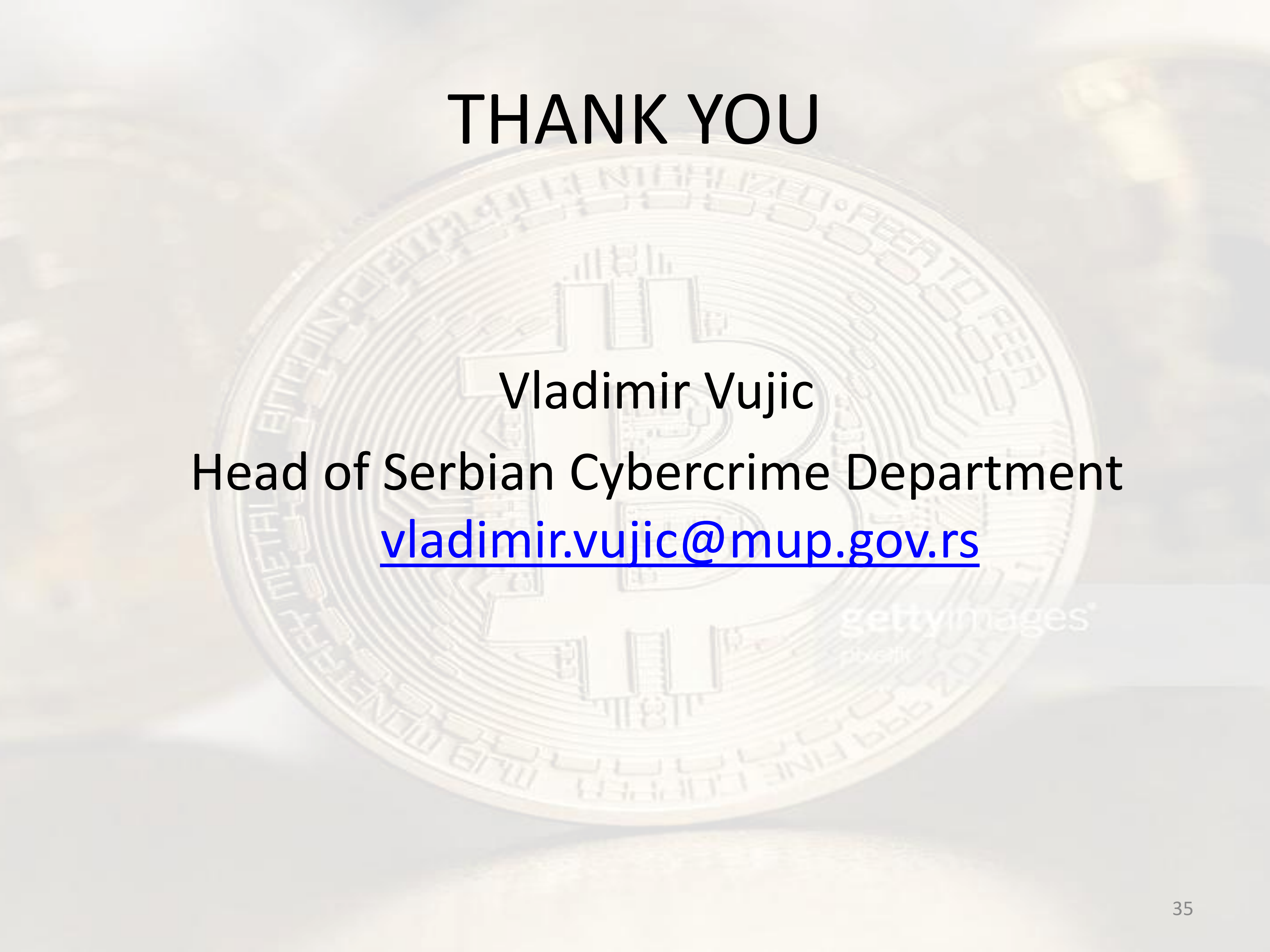
*Source: https://go.chainalysis.com/2020-Crypto-Crime-Report.html

Conclusion



- Cryptocurrencies are becoming the main means of work of organized criminal groups
- Essentially all forms of crime end in money laundering
- Greed and lack of knowledge of people lead to an increase in cryptocurrency fraud
- Technology that changes the way investigations are conducted

THANK YOU



Vladimir Vujic

Head of Serbian Cybercrime Department

vladimir.vujic@mup.gov.rs