Cryptocurrency and the Trade of Online Child Sexual Abuse Material

The International Centre for Missing & Exploited Children and Standard Chartered | February 2021

International Centre™
FOR MISSING & EXPLOITED CHILDREN

LETTER FROM THE CEO OF THE INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN

At the International Centre for Missing & Exploited Children (ICMEC), we are dedicated to building a global community of caring adults and institutions all working together to bring about a world where children can grow up free from going missing, from being abducted, sexually abused or exploited. ICMEC works in more than 120 countries to identify gaps in the international community's ability to protect its children and bring together the people, the resources, and the tools needed to fill those gaps. For more than two decades, ICMEC has led the way in offering support to governments, policymakers, law enforcement, prosecutors, industries, civil society, and others around the world – because we believe safeguarding children is a responsibility every one of us shares.

ICMEC's Financial Coalitions Against Child Sexual Exploitation (FCACSEs) (U.S. and Asia Pacific) bring leaders in the financial and payments industries together to disrupt the economics of commercial child sexual exploitation and prevent the misuse of financial services technologies and platforms. As a result of the combined efforts of Coalition partners and law enforcement, the use of credit cards to purchase child sexual exploitation material (CSEM) online has been virtually eliminated globally and websites offering CSEM have had to find alternative payment schemes for their illicit businesses.

In 2017, ICMEC and the U.S. FCACSE turned their attention to emerging payment methods and published *Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation*. That report suggested cryptocurrency was likely to have broad and far-reaching implications for a wide range of industries (legitimate and illegitimate), including the commercial trade of CSEM. It also argued that while cryptocurrency may seem on the surface to be anonymous and untraceable, those who use it as a payment method for CSEM are not beyond identification by law enforcement — or successful prosecution. Indeed, two recent major takedowns of commercial CSEM sites demonstrate while cryptocurrency users may believe they are invisible from law enforcement, they can and will be found and held accountable for their illicit activities.

ICMEC is pleased to provide this addendum to our 2017 report on cryptocurrency. In the pages that follow, we:

- Highlight the most recent global data and research on usage of cryptocurrency to trade in CSEM;
- Examine two recent case studies of law enforcement takedowns of websites trading in CSEM — both of which relied almost exclusively on cryptocurrency;
- Provide an overview of the most recent understandings of the mechanics and typologies of CSEM cryptocurrency transactions.

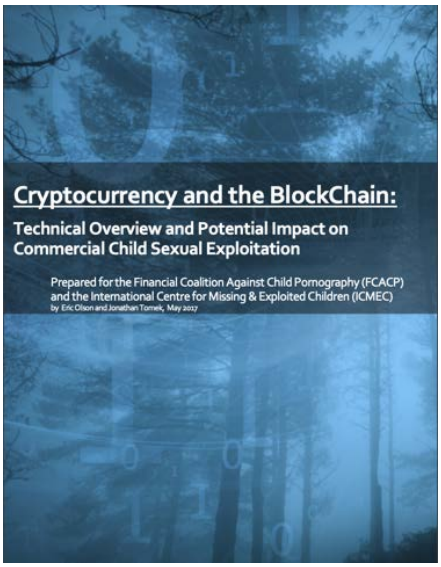
"Perpetrators who use Bitcoin to buy or sell child sexual exploitation material are on borrowed time, these case studies demonstrate law enforcement can and will find you and prosecute you."

- Bob Cunningham, ICMEC CEO

We are grateful to our colleagues at Standard Chartered Bank, who provided research for this paper as well as overall support for its publication. We hope that all stakeholders in the fight against child sexual exploitation will benefit from this study of emerging trends in commercial CSEM and use the lessons learned in their own efforts to keep children safe.

Bob Cunningham
Chief Executive Officer, International Centre for Missing & Exploited Children (ICMEC)

Introduction



Since the publication of *Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation* in 2017, the role of cryptocurrencies in the commercial sale of child sexual exploitation material (CSEM) has, predictably, expanded significantly. Combined with an increase in CSEM on the dark web, the dynamics around this issue have changed in several important ways that affect those investigating and prosecuting these horrific crimes, as well as the financial and technology firms that have joined in the fight.

In 2019, 132,676 URLs or web pages were confirmed by the Internet Watch Foundation (IWF), the national reporting hotline for the UK, to contain, link to, or advertise child sexual abuse imagery across 4,956 domains traced to 58 countries, representing a 27% increase since 2018.[1] In addition, in 2019 IWF identified 288 new dark web sites selling CSEM – an increase of 238% from 85 dark web sites identified by IWF in 2018. 197 of these 288 sites were assessed by IWF to be commercial and only accept payment in virtual currencies.[2] According to IWF, the last several years have seen the greatest overall rise of darknet markets engaged in the sale of CSEM.[3]

Because these markets almost always exclusively accept cryptocurrencies for payment rather than traditional payment methods, the last several years have also seen a dramatic increase in the use of cryptocurrencies to purchase CSEM, including the world's most prominent and most widely traded cryptocurrency, Bitcoin (BTC). In 2019, Chainalysis was able to track just under $930,000 worth of payments to addresses associated with CSEM providers via Bitcoin and another cryptocurrency, Ethereum (ETH). This represented a 32% increase over 2018, which in turn was a 212% increase over 2017.[4]

---

1 Internet Watch Foundation, *Annual Report 2019 – Zero Tolerance, at* https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance.

2 *Id.*

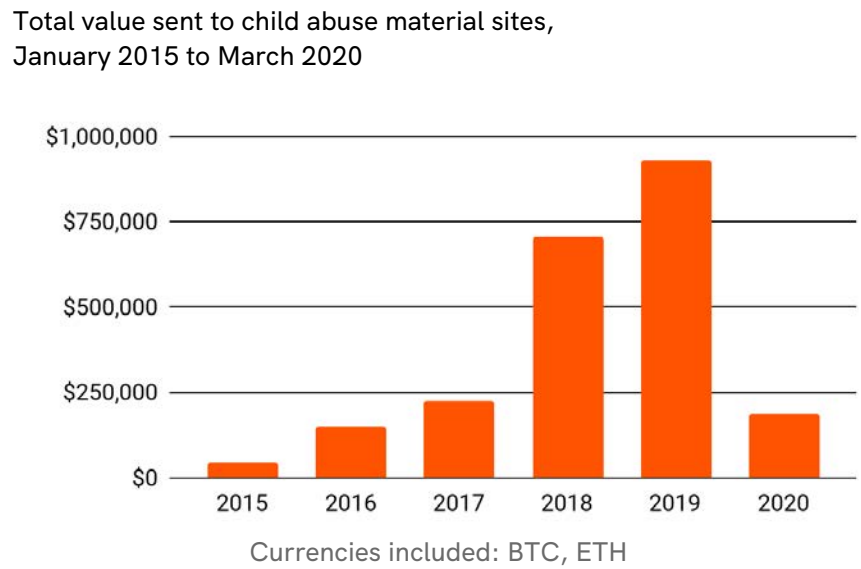
3 *Id.*

4 Chainalysis, *Making Cryptocurrency Part Of The Solution To Human Trafficking,* Apr. 21, 2020, *at* https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020.

While there are significantly more domains on the surface web hosting and using cryptocurrency to trade in CSEM, two notable recent cases of commercial CSEM market takedowns described in this paper illustrate both the proliferation of CSEM and the rise of Bitcoin as a major payment method for CSEM. In fact, in announcing the takedown of one of these markets, Welcome to Video (WTV), the U.S. Department of Justice said it was the largest ever seizure of CSEM content by volume; over 250,000 unique videos were seized. The Department of Justice further reported that users purchased these videos using Bitcoin.[5]

Many users believe they are anonymous and therefore beyond detection from law enforcement when using cryptocurrencies,[6] but as these cases will demonstrate, users can be detected and prosecuted. Indeed, the use of cryptocurrencies often provides the very pathway for law enforcement to trace perpetrators to illicit activities.

Figure 1: Cryptocurrency Payments to CSEM Sites



Source: https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020

The following case studies outline the mechanics of how customers of these markets sent cryptocurrency, as well as how the administrators of the markets then consolidated the cryptocurrency. Additional typologies associated with CSEM cryptocurrency transactions will also be reviewed.

[5] U.S. Department of Justice, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin,* Oct. 16, 2019, *at* https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.

[6] Chainalysis, *supra* note 4.

"Financial institutions need to ensure they understand how cryptocurrencies can be used by criminals in the trade of illicit material. Maintaining robust KYC & CDD expectations on Exchanges or other Virtual Asset Service Providers that financial institutions engage with plays an important part in helping to narrow the opportunities for these criminals."

- Nick Lewis, Standard Chartered,
Head of Financial Crime Compliance Investigations and Intelligence

Case Studies

Welcome to Video

In October 2019, the U.S. Department of Justice indicted 23-year-old South Korean national Jong Woo Son, who operated a dark website exclusively devoted to CSEM. Welcome to Video, commonly referred to as "WTV," began operating in the summer of 2015 and as of around March 2018 had over 200,000 unique video files on its server.[7] WTV customers created free accounts on the site and downloaded videos by redeeming points. Customers could purchase points with Bitcoin, or earn them through new customer referrals or by uploading their own videos depicting CSEM. Users that created an account with the website received a unique Bitcoin address. From the site's inception in mid-2015 through around March 2018, WTV received at least 420 BTC through at least 7,300 transactions, worth over $370,000 at the time of the respective transactions.[8]

By the time the site was taken down in March 2018, there were over one million Bitcoin addresses hosted on the website's server, indicating that the site had the capacity for at least one million users.[9]

7 United States v. Jong Woo Son, 1:18-cr-00243 (D.D.C. Aug. 9, 2018), *at* https://www.justice.gov/opa/press-release/file/1210441/download.

8 *Id.*

9 U.S. Department of Justice, *supra* note 5.

Investigators were able to arrest and charge 337 of those site users residing in the United States and in 11 other countries. Over 250,000 unique videos were removed from the site, making it one of the largest ever seizures of CSEM by volume.[10]

WTV established approximately 1.3 million unique BTC addresses to receive payments from WTV customer accounts.[11] Moreover, WTV directed its customers to particular BTC exchanges in order to make payments to WTV, including an exchange located in the United States.

Cryptocurrency Overview

The predominant cryptocurrency globally is Bitcoin (BTC), which has a market capitalization of over $650 billion as of January 2021.[12] Bitcoin is considered a pseudonymous cryptocurrency. While addresses that are used to send and receive Bitcoin are made up of random strings of letters and numbers not linked to real-world individuals, all Bitcoin transactions including the sending and receiving address as well as the date and time of transactions are publicly broadcast on the blockchain. Bitcoin relies on asymmetric cryptography that utilizes public/private key pairs to allow users to securely send and receive transactions. A user's Bitcoin address is known as a public key, that has a corresponding private key, which in turn allows a user to spend the cryptocurrency. In order to send and receive Bitcoin, users need to have access to a "wallet," which holds the private key that allows a user to access their Bitcoin address.[13]

Ethereum (ETH) is the second largest cryptocurrency by market capitalization after Bitcoin. However, while Bitcoin is exclusively a cryptocurrency, the primary purpose of Ethereum is to use blockchain technology for additional applications by enabling the deployment of smart contracts and decentralized applications.[14]

In order to exchange virtual currencies for real currency, users can open accounts at virtual currency exchanges allowing them to convert virtual currency into either fiat currency or other types of virtual currency.[15] Exchanges located in the United States are required to register as a money service business and establish an anti-money laundering (AML) program. As part of an AML program, exchanges are required to verify the identity of their customers and comply with recordkeeping and monitoring requirements for customer transactions.[16]

---

10 *Id.*

11 United States v. Jong Woo Son, *supra* note 7.

12 TradingView, *Cryptocurrency Market – Bitcoin, at* https://www.tradingview.com/markets/cryptocurrencies/prices-bitcoin/.

13 Coindesk, *How to Store your Bitcoin,* Aug. 20, 2013, *at* https://www.coindesk.com/learn/bitcoin-101/how-to-store-your-bitcoins.

14 Nathan Reiff, *Bitcoin vs. Ethereum: What's the Difference?,* Investopedia, Jun. 16, 2020, *at* https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp.

15 Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks,* Jun. 2014, *at* https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

16 FinCEN Guidance, *Application of FinCEN's Regulations to Certain Business Models involving Convertible Virtual Currencies*, May 9, 2019, *at* https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

U.S. law enforcement linked customers of WTV to specific BTC payments by analyzing a forensic image of WTV's server, which was seized by South Korean law enforcement in March 2018. By gaining access to WTV's server, law enforcement was able to link BTC addresses that sent Bitcoin to WTV BTC addresses to specific user accounts at WTV. Moreover, blockchain analysis revealed that BTC addresses that sent Bitcoin to WTV were linked to accounts hosted at three BTC exchanges. Law enforcement identified 24 accounts held at these three exchanges.[18] BTC transactions sent from five BTC addresses linked to accounts at the various exchanges contained the username of a WTV customer in the memo of the BTC transaction. In addition, five BTC addresses linked to accounts at one of the exchanges also transacted with darknet markets, which sold drugs, stolen information, and other illicit products. Moreover, four out of the five BTC accounts at two of the three BTC exchanges did not have a registered name associated with these accounts, indicating that customers holding accounts at these exchanges provided incomplete "know your customer" (KYC) information.[19]

Dark Web Overview

The World Wide Web can be divided into the surface web, deep web, and dark web. The surface web consists of websites that are indexed, meaning that they can be accessible via search engines. The deep web consists of websites that are not indexed, such as content behind a paywall, or which requires sign-in credentials. The dark web is a subset of the deep web that can be only accessed using specific browsers such as the Tor browser, which anonymizes a user's web traffic.[17]

According to the WTV indictment issued by the U.S. Department of Justice, an undercover agent sent BTC to different BTC addresses provided by WTV. In a number of instances, within two days following those transfers, Son then transferred the BTC to a single BTC address, which in turn was linked to an account at a virtual currency exchange. The signature card at this exchange revealed that the account was held in the name of Son and also listed Son's phone number and email account. Son cashed out Bitcoin held at the exchange to a bank account held in his name.[20]

17 Darren Guccione, *What is the dark web? How to access it and what you'll find,* CSO, Nov. 18, 2020, *at* https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.

18 *United States v. Twenty-Four Cryptocurrency Accounts,* No. 19-cv-3098 (DLF) (D.D.C. Oct. 16, 2019), *at* https://www.justice.gov/opa/press-release/file/1210461/download.

19 *Id.*

20 United States v. Jong Woo Son, *supra* note 7.

WTV Takeaways

- The transactional pattern in this case appeared to first follow a one-to-one pattern, whereby BTC was sent from a BTC address linked to WTV customer to a unique WTV BTC address associated with that customer. This was followed by a many-to-one pattern whereby funds were sent from the WTV BTC addresses to a single BTC address belonging to Son that was stored at an account held at a virtual currency exchange.

- Both Son and the customers of WTV utilized accounts at virtual currency exchanges. Approximately one-fifth of these customer accounts also transacted with darknet markets.

- In certain instances, the virtual currency exchanges held KYC information for accounts linked to WTV customers, while for four accounts, customers provided incomplete KYC information.

DarkScandals

In March 2020, the U.S. Department of Justice indicted 32-year-old Dutch national Michael Rahim Mohammad (Mohammad), who operated DarkScandals, a site on both the darknet and surface web that distributed obscene sexual content, including videos that depicted sexual assault and CSEM.[21]

[21] *United States v. Michael Rahim Mohammad,* 20-cr-0065 (D.D.C. Mar. 5, 2020), *at* https://www.justice.gov/usao-dc/press-release/file/1257641/download.

The site, which was created in 2012, offered users two ways to access content: users could either pay for "packs" of content or upload their own videos and receive content packs in exchange.[22]

According to the DarkScandals forfeiture complaint issued by the U.S. Department of Justice during the course of the WTV investigation, a review of the virtual currency records of a Washington, D.C.-based WTV customer led to the discovery of DarkScandals.

DarkScandals advertised that these packs contained approximately 2,000 videos and images. DarkScandals received approximately 1,650 deposits totaling 188.6631 BTC (valued at approximately $1.6 million as of March 1, 2020) and 26.724 of ETH (valued at approximately $5,730).[23] In March 2016, one customer, based in Washington, D.C., who was also a customer of WTV, made a single payment of 0.15 BTC to DarkScandals.[24] All said, Mohammad, also known as "Mr. Dark," received almost $2 million from selling obscene and illicit content.

A large share of the payments sent to DarkScandals originated from accounts hosted at eight virtual currency exchanges offering BTC/ETH wallet services. According to a forfeiture complaint, 303 virtual currency accounts held at these eight exchanges were linked to virtual currency addresses that made at least one payment to DarkScandals.[25] Many of these accounts appeared to have been solely opened and used to send funds to the site. Moreover, many of these virtual currency addresses that had other payment activity also sent or received funds to and from darknet markets that sold drugs, stolen information, and other illicit products. The forfeiture complaint also noted that many of the 303 accounts held at the exchanges were opened with either false or no KYC documents.[26]

DarkScandals originally directed users to transfer fiat currency to an account associated with the site. But beginning in or around November 2013, the site directed users to send payments

22 *United States v. Three Hundred Three Virtual Currency Accounts, DarkScandals Domain, and DarkScandals.co Domain,* No. 20-cv-712 (D.D.C. Mar. 12, 2020) *at* https://www.justice.gov/usao-dc/press-release/file/1257581/download.

23 *Id.*

24 U.S. Department of Justice, U.S. Attorney's Office, District of Columbia, *Dutch National Charged in Takedown of Obscene Website Selling Over 2,000 "Real Rape" and Child Pornography Videos,* Funded by Cryptocurrency, Mar. 12, 2020, *at* https://www.justice.gov/usao-dc/pr/dutch-national-charged-takedown-obscene-website-selling-over-2000-real-rape-and-child; *See also*, United States v. Three Hundred Three Virtual Currency Accounts, *supra* note 22.

25 United States v. Three Hundred Three Virtual Currency Accounts, *supra* note 22.

26 *Id.*

of BTC to a specific BTC address that was created by Mohammad in order to access the site's content. Mohammad subsequently directed users to send payments to two additional BTC addresses and one ETH address.[27] Mohammad used his own identifying information to create accounts at banks as well as at virtual currency exchanges to convert funds into fiat currency.

A number of the BTC addresses linked to virtual currency exchanges that sent BTC to one of the BTC addresses created by Mohammad also sent or received funds to and from darknet markets.[28]

DarkScandals was jointly investigated by the U.S. Internal Revenue Service Criminal Investigation (IRS-CI) and Homeland Security Investigations. The Dutch National Police, Europol, and the German Federal Criminal Police assisted and provided coordination with their parallel investigations.[29]

"Criminals should know if you leave a digital footprint, we will find you. If you exploit our children, we will put you behind bars. If you thought you were anonymous, think again."

-IRS Chief of Criminal Investigations, Don Fort
As quoted in Department of Justice press release, March 12, 2020[30]

DarkScandals Takeaways

- The transactional pattern in the DarkScandals case appeared to follow a many-to-one pattern whereby in a number of instances BTC was sent from unique BTC addresses belonging to customers of DarkScandals to a single BTC address that was created by the administrator of DarkScandals.

27 *Id.*
28 *Id.*; *See also,* United States v. Michael Rahim Mohammad, *supra* note 21.
29 *Kelly Phillips Erb, Dark Déjà vu: IRS Announces Charges in Takedown of Multi-Million Dollar Child Exploitation Website Funded by Bitcoin,* FORBES, Mar. 13, 2020, *at* https://www.forbes.com/sites/kellyphillipserb/2020/03/13/dark-deja-vu-irs-announces-charges-in-takedown-of-multi-million-dollar-child-exploitation-website-funded-by-bitcoin/?sh=4c12be5b28ae.
30 U.S. Department of Justice, *supra* note 24.

- In numerous instances, accounts created by DarkScandals customers that were held at virtual currency exchanges were opened with either false or no KYC documents. Moreover, a number of these customer accounts sent or received funds to and from darknet markets.

- DarkScandals was identified through the analysis of the BTC transaction records of a WTV customer.

Lessons Learned from the Use of Virtual Currencies

Predominance of Bitcoin

In both cases highlighted above, Bitcoin was used in the overwhelming majority of the transactions. WTV appeared to have used Bitcoin exclusively, while DarkScandals dealt predominately in Bitcoin, with only a tiny fraction of deposits via Ethereum.

Transactional Pattern

The WTV and DarkScandals sites operated differently with regard to how their customers sent virtual currency to the sites. In the case of WTV, customers sent Bitcoin from their personal BTC address to a WTV BTC address unique to each individual customer. DarkScandals, by contrast, had customers in numerous instances send BTC from their personal BTC addresses to a single BTC address that was controlled by the administrator of site.

Both WTV and DarkScandals, however, were similar in that they consolidated BTC received from their customers into a single BTC address. In the case of WTV, Bitcoin was often consolidated from various WTV BTC addresses and sent to a single BTC address that belonged to the administrator of WTV. Similarly, DarkScandals customers sent Bitcoin from their personal BTC addresses to a single BTC address controlled by the administrator of DarkScandals.

Figure 2: WTV Transactional Pattern

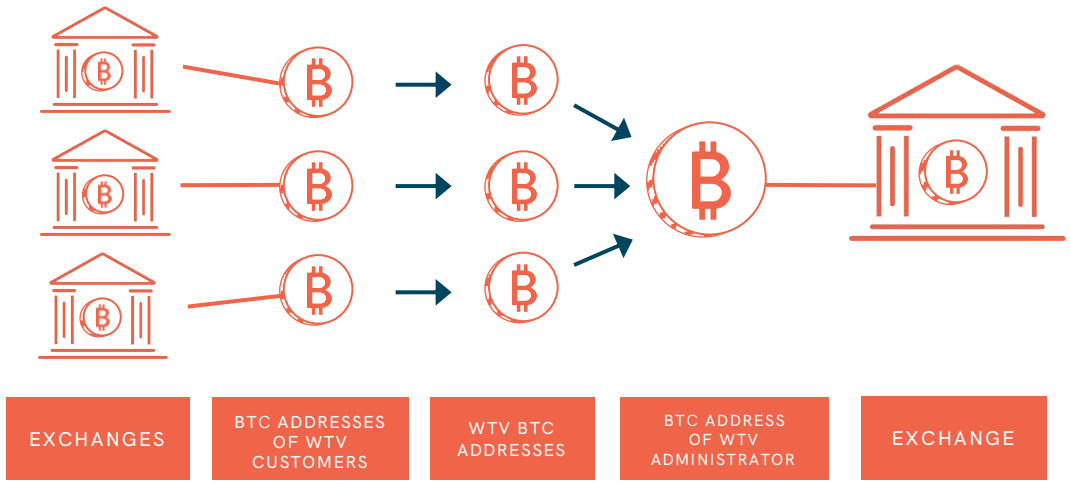
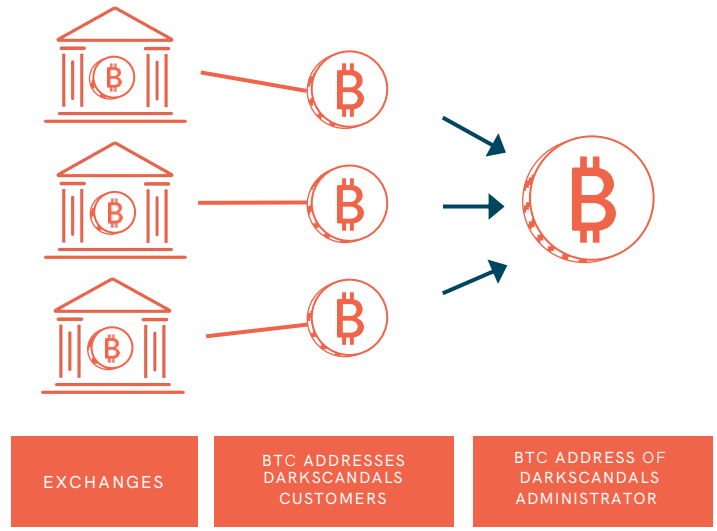


Figure 3: DarkScandals Transactional Pattern



The Role of Virtual Currency Exchanges

Customers of both WTV and DarkScandals used BTC addresses linked to accounts held at exchanges to send Bitcoin to these sites. A number of these exchanges maintained KYC information, and as a result, law enforcement agencies were able to link customers of both sites to accounts held at these exchanges. In both of these cases, however, there were multiple instances in which individuals who used accounts at exchanges to send Bitcoin to WTV and DarkScandals provided no or incomplete KYC information. Some DarkScandals customers even provided false KYC documents. Therefore, even those exchanges that maintain complete KYC information for customers can still experience exposure to CSEM markets. Moreover, BTC addresses linked to accounts at virtual currency exchanges that transacted with both sites also transacted with other darknet markets that sold drugs, stolen information, and other illicit products.

> Even those exchanges that maintain complete KYC information for customers face the risk of exposure to CSEM

Site Administrators

In both cases, the administrators appeared to have operated these sites as well as the associated virtual currency addresses on their own without the assistance of others.

Identifying New CSEM Markets by Analyzing Transactions of Known CSEM Customers

Law enforcement was able to identify a new CSEM darknet market, namely DarkScandals, by analyzing BTC transactions of a customer of an already known CSEM darknet market, namely WTV.

Additional Typologies of CSEM Cryptocurrency Transactions

In addition to the specific patterns described in the WTV and DarkScandals case studies, there a number of typologies that could indicate that a cryptocurrency address is transacting with a provider of CSEM.

According to Chainalysis, cryptocurrency payments made on a recurring basis to one or a group of addresses belonging to the same entity could indicate a possible subscription to a provider of CSEM. Chainalysis observed in one instance, that a BTC address identified as belonging to a CSEM provider consistently received transfers for 0.0021 Bitcoin. Chainalysis also observed that the majority of BTC/ETH payments from South Korean virtual currency exchanges to CSEM markets between December 2013 and March 2020 occurred during nighttime hours.[31]

Privacy Coins

Over the years, a number of cryptocurrencies known as privacy coins have been created in order to address the privacy concerns associated with the predominant cryptocurrencies, namely Bitcoin and Ethereum, which are pseudonymous. Unlike pseudonymous cryptocurrencies, privacy coins conceal transaction details so that there is no public record of the sender's and receiver's addresses or the transaction amount. Some of these privacy coins include Monero, Dash, and ZCash. In June 2019, the Financial Action Task Force (FATF), an inter-governmental body that sets international standards to combat money laundering and terrorist financing, adopted its recommendation that virtual currency exchanges should pass customer information to each other when transferring funds, as financial institutions are required to do, and obtain and maintain records of the originator and beneficiary on virtual asset transfers.

In the U.S., this requirement is known as the funds "Travel" rule, which requires financial institutions to obtain and maintain records of the identity of the sender and recipient for any transmittal of funds of $3,000 or more. Following the release of the FATF Guidance in June 2019, a number of virtual currency exchanges determined that they could not continue to list privacy coins while complying with the new FATF recommendation and a number of privacy coins including Monero, Dash, and ZCash lost between 50% and 60% of their market value. At the same time, FATF and the Financial Crimes Enforcement Network (FinCEN) based in the U.S. have not issued an outright ban on privacy coins. Instead, FinCEN, for example, clarified that money transmitters dealing in anonymity-enhanced convertible virtual currencies are required to obtain the identity of the transaction's sender or recipient.[32]

While privacy coins are not explicitly banned from regulated exchanges by the new FATF recommendations, it is unclear whether privacy coins will become increasingly accepted in commercial CSEM marketplaces. Unlike privacy coins, Bitcoin is more accessible, has greater widespread adoption, and has a higher level of trust compared to privacy coins, which were only established in recent years whereas Bitcoin was released in 2009.

31 Chainalysis, *supra* note 4.

32 FinCEN Guidance, *supra* note 16.

The Association of Certified Financial Crime Specialists (ACFCS) also identified a number of indicators of cryptocurrency transactions related to human trafficking that are also applicable for detecting cryptocurrency transactions related to CSEM including: 1) frequent purchases in multiples of small amounts of cryptocurrencies; 2) engaging in transactions between 11:00pm and 5:00am; 3) engaging in cryptocurrency transactions tied to prepaid and credit cards; 4) cryptocurrency transactions to sites associated with adult service providers; and 5) using cryptocurrencies to purchase tokens associated with or specifically designed for the adult industry.[33]

Conclusion

In our 2017 publication, *Cryptocurrency and the BlockChain: Technical Overview and Potential Impact on Commercial Child Sexual Exploitation,* we examined the potential impact of cryptocurrency on commercial child sexual exploitation and noted how law enforcement can and should employ a number of tools to combat it. Specifically, we highlighted the potential to identify criminal users of Bitcoin, despite the fact that it is a pseudonymous cryptocurrency. The cases outlined above demonstrate that law enforcement has in fact had such success in dismantling online commercial CSEM markets, in large part by taking aim at Bitcoin transactions.

In our ongoing mission to fight commercial child sexual exploitation, the International Centre for Missing & Exploited Children and the Financial Coalitions Against Child Sexual Exploitation will continue to follow these emerging payment methods and their use in CSEM markets. We hope that all stakeholders in this fight, including law enforcement and the financial industry, benefit from the insights provided here and use the lessons learned in their own efforts to keep children safe.

[33] Brian Monroe, *Top five ways to detect, counter human trafficking in bank, crypto exchange transactions,* Association of Certified financial Crime Specialists, Jan. 30, 2020, *at* https://www.acfcs.org/top-five-ways-to-detect-counter-human-trafficking-in-bank-crypto-exchange-transactions/.

International Centre™
FOR MISSING & EXPLOITED CHILDREN

www.icmec.org