The Survey of Darknet, Illicit Drug Interdiction, FBI Network Investigative Technique, and Fourth Amendment

Thomas Ngo, Mircea Dumitrache, Yusuke Tomatsu, and Sami Aliraqi

**Abstract**— The purpose of this survey paper is to summarize the current researches about the Darknet. This paper provides a critical assessment of the concept of Darknet and the background of the illegal drug market. It includes information about the overall situation of Darknet and its current state. Besides, we discuss the Fourth Amendment's interpretation and Rule 41 change that affects the Darknet market. Due to data privacy controversy, there are many cases and investigations related to the 4th Amendment throughout history. As a result, that leads us to the discussion of NIT and the Impact on the prosecution process. With that said, the paper provides insight and hindsight about how the Fourth Amendment is used in Fifth circuit court rules and the debate of privacy values over Bitcoin. Also, we identify and present how cryptocurrencies are used in drug dealing. There are multiple ways that drug dealers utilize cryptocurrencies in the Darknet network, but we only concentrate on three main approaches in this paper. First, cryptocurrencies can be used as a security layer to protect and conceal illicit drug activities. Second, malicious actors, such as criminal organizations, use cryptocurrencies to help them reduce the illicit drug market's visibility and a means to widen their global trading. Third, cryptocurrencies are used for money laundering after drug dealing.

**Index Terms**—*Darknet, cryptocurrencies, Fourth amendment, NIT, prosecution process, illicit drug interdiction, Rule 41 change*

# Introduction

To understand the Darknet and illegal drug, we first need to understand the concept of these two. According to Moore and Rid, the Darknet is an in-depth web that is nearly hidden and not accessible by search engines like Google or Bing [2]. However, it uses the standard HTTP/HTTPS protocol and can be found in popular browsers such as Chrome. Like the Deep Web, the Darknet is hidden and cannot be accessed by search engines. However, the Dark Net differs from the Deep Web in that it requires a specific piece of software called the Tor browser to access it. Therefore, the Darknet is covered by the Tor network, which includes many nodes and encryption, and is highly anonymous, and it is complicated to trace the criminal activities. Darknet is dark; malicious people sell various kinds of illegal stuff such as drugs, weapons, and malware. The initial concept of the Darknet was about providing information while ensuring privacy and avoiding censorship. However, because of its Anonymity, the Darknet is highly used for criminal activities nowadays. The most famous Darknet was once called the Silk Road. Silk road sells illegal drugs, services, and weapons; the Silk Road was known as eBay for drugs. The owner of the Silk Road: Ross Ulbricht, was arrested by the FBI in October 2013.

# What are illegal drugs?

A drug affects the way the body functions. When a drug is classified as illegal, this means that the drug is prohibited by law. Several illegal drugs have different effects on a person, and many factors influence these terrible effects. This fact makes illegal drugs unpredictable and dangerous for our health, especially for young people. The effects of illegal drugs are affected by the following factors; the types of drug consumed, individual characters of the person who use drugs, and how many types of drugs are used at one time.

As we mention later, there are many types of illegal drugs such as cocaine, MDMA, Heroin, and Methamphetamine. Illegal drugs are classified into the following three types; Depressants, Stimulants, and Hallucinogens. According to the positive choice institute, Depressants are drugs that slow down the central nervous system. Besides that, depressants send messages to both the brain and the body[19]. The messages decrease people's concentration, and the drug slows the response of the person. The name 'depressant' indicates that these drugs often make a person feel depressed, but this does not always happen. The term indicates the effect of slowing down the central nervous system as a depressant for this kind of drug. Some examples of depressants include alcohol, opioids, and GHB[19]. Stimulants are also referred to as psychostimulants. Stimulants are drugs that stimulate the central nervous system and speed up the messages in contrast to a depressant. These drugs typically make people high; the drug increases the body's energy, heart rate, and appetite. Some examples of psychostimulants include methamphetamine, cocaine, caffeine, MDMA[19]. Hallucinogens are drugs that often change how a person perceives the world. Hallucinogens can change how a person sees, hears, tastes, and smells. The drug also changes the feel of the thing and makes things that do not exist at all. Some examples of hallucinogens include ketamine, magic mushrooms, and LSD[19].

# Illicit drug market

According to the EMCDDA report, 62% of the darknet content is Drugs and drug-related chemicals, and 77% of its content is about illicit drugs [1]. This fact means that illicit drug transactions are very active in the Darknet. Addiction center states that Illicit drugs are very addictive and illegal substances like MDMA, crystal meth, and Cocaine [4]. According to the Drug Enforcement Administration (DEA), MDMA produces an energizing effect, distortions in time and perception, and enhanced enjoyment of tactile experiences. The simple explanation is that in humans, for example, when we are angry or excited, we release hormones and neurotransmitters. MDMA can produce such substances in the brain.  It has the effect of making the body produce many feelings like "I am sorry, I don't know what to do," which increases the feeling of happiness and excitement. However, continued abuse can lead to mental confusion and memory problems, and in some cases, death [3]. Crystal meth is a stimulant. This drug is a potent and highly addictive human-made stimulant that causes aggressive, violent, or psychotic behavior [3]. Crystal meth also makes people addicted to drug abuse easily since it is available widely and cheaper than other illegal drugs.   Cocaine is extracted from the coca leaf and was created as a painkiller. It is usually inhaled through the nose, and its powder is absorbed into the bloodstream from the nasal tissues. It can also be ingested by mouth or applied to the gums. According to DEA, the intensity of cocaine's effects on the user depends on how quickly the drug reaches the brain; this depends on the dose and usage method. Smoking or injections, cocaine can reach the brain in a few seconds. This rapid-onset, intense euphoric can cause an effect called "rush" [3]. Once you start taking this drug, you know that it is almost impossible to be free from its control, both physically and mentally.

As many people know, an addiction to illegal drugs can completely change the person. Addiction causes damage to the brain permanently, so it is challenging to recover from it.

Moore and Rid stated that the motivation to buy drugs from the Darknet is because of the quality of the illicit drugs; higher quality of drugs is available on the Darknet than other platforms. Drug benders are also willing to take the risk of shipping illicit drugs worldwide. Moore and Rid also mentioned the merit of buying drugs online. The buyer's main merit is that customers do not need to face the drug dealer; facing the drug dealer may end in violence when the negotiation goes wrong [2]. On the other hand, buying the drug online still needs the address to be delivered, so customers still risk their privacy. For drug vendors, there are two advantages to using the Darknet to sell drugs. According to EMCDDA, underground markets provide a convenient and safe place for individual criminals and organized crime groups. Distributors can reduce the risk of detection while advertising their drugs to potential new customers widely on the Darknet.

EMCDDA stated that the challenges of catching darknet drug dealing are increasing because of new forms of parcel delivery and new software development that can secure illegal drug trading. Law enforcement has to monitor and assess the Darknet and understand the overall drug market [1]. Darknet provides a stable sales platform for technologically savvy drug users, and illicit drug trading in the Darknet can grow in the long term.

# Darknet in current Covid-19 situation

Martin stated that vendors on the Darknet sell fake coronavirus cures, including fake vaccines and antidotes [5]. This study shows that malicious dark web dealers are trying to exploit the current pandemic and seek to defraud uneducated customers. Fortunately, the number of products related to coronavirus is relatively small; it accounts for about 0.2% of all Darknet items [5]. Marin also found out that some owners of the crypto markets-imposed ban on vendors who try to seek benefits from the pandemic.

# Overall situation

Darknet is a highly anonymous network, and this feature can make the trade secure for illicit drugs. Users need to use Tor to access the Darknet, and Tor can hide your record on the Darknet. The most famous Darknet was called Silk Road, made by Ross Ulbricht. The website itself made 1.2 billion dollars in sales, and He was getting $80 million in brokerage commissions. Various kinds of illicit drugs were sold on the Darknet even after the closure of Silk Road.  There are some merits for both vendors and customers to sell drugs on a darknet platform; vendors can scale their business functionally using the Darknet. Customers can get illicit drugs safely compared to in-person trading. Besides, new forms of parcel delivery and new software development also can make trading more secure than before, so illicit drug trading can be growing in the long term. The current situation of Covid-19 also attracts potential customers since in-person trading is dangerous to do in this pandemic, and law authorities can watch malicious people easily since everyone is encouraged to stay home.

# Interpretations of the Fourth Amendment

The fourth Amendment states that people have the right to be secure against unreasonable searches and seizures of their persons, houses, papers, and effects. Such searches and seizures are only constitutional under a warrant issued "on probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [9]

The fourth Amendment applies to packages sent using the U.S. Post Office, and those packages may contain drugs or other illegal items. Drug dealers use the dark web to conduct transactions anonymously, and is hence filled with illegal surfers. Once a transaction is complete on the dark web, the drug dealers send the package containing the drug under an alias. Such a package would be under the protection of the Fourth Amendment; however, the courts that have identified this as an issue have not adequately resolved it.

There have been several cases in which the fourth Amendment was interpreted differently and slightly changed over history. Initially, the Amendment would protect the people's property, which would include sealed letters or packages from being searched. This was a conclusion of the case Olmstead v. the United States. The court decision shifted in the case Katz v. United Stated by discarding the property law as part of the fourth Amendment and replacing it with an expectation of privacy and recognizing such an expectation as reasonable by society. In the case of Rakas v. Illinois, the court decision evolved from the previous case once again, inquiring whether the defendant has a reasonable expectation of privacy and if not, then the defendant could not challenge the government's search. The problem in question has changed from property to privacy. [6]

Further cases have investigated how the fourth Amendment's expectation of privacy would include packages sent through the mail and whether the sender should be expecting privacy even when sending this package while using aliases. However, there are still debates on how such an expectation should be analyzed. [6]

In a court case, the United States v. Villarreal, the fourth amendment protection was given to both defendants, basing their decisions on the United States v. Richards where Richards and the alias "Mehling Arts & Crafts" were denoted to be the same and had a legitimate expectation of privacy. This was concluded even after the package was opened, and heroin was found inside. On the other hand, in the court cases the United States v. Walker and United States v. Pitts, the defendants were not protected by the Fourth Amendment; in the former case because the defendant did not have a right to expect privacy due to the package and alias being used in a criminal scheme, and in the latter case because the defendant had no right to expect privacy due to the use of an alias. [6]

# Rule 41 Change

Rule 41, title "Search and Seizure," gives a magistrate judge that has authority in any district where activities related to a crime may have occurred the ability to issue a warrant. The warrant allows remote access to any number of unknown devices and the ability to search, copy, and seize information from them if a device's location is obscured by technological means or if crimes are being investigated in at least five districts. [7]

Rule 41 was amended to address the change in criminal movement. Most criminals have adapted to use the internet and technological advancement of the present to pursue cyber-threatening and encryption. Hacking crimes have risen, and it is simple to hide a computer while retaining Anonymity through the current encryption technologies and the use of the dark web. With such changes, people fear that the government may be utilizing this technology and Rule for more than seizing criminals and illegal actions. It has become a debate on whether the Rule should be used for the security of the people despite their right to privacy or if people's privacy is important. [8]

The people sending packages through the U.S. Post Office using an alias may be criminals attempting to utilize the fourth Amendment in a criminal scheme, such as the transport of illegal drugs. However, using an alias may not be enough evidence of a criminal scheme, as people may use aliases to send questionable but legal goods to another individual. Similarly, entirely because a user is concealing their identity, it does not make them a criminal, like many voters, authors of controversial publications, journalists, and others utilize the Darknet to maintain their Anonymity. [8]

# NIT and the Impact on the Prosecution Process

One of the FBI techniques to provide access to a remote computer is called the Network Investigation Technique, or NIT, which is a form of malware that is designed to provide access to the computer through a "drive-by" download. [10]

However, when the NIT is used, it is often used alongside social engineering to make the target open a fictitious email or webpage. The webpage or email in question contains malicious code injected into it, forcing the browser to download the program and silently execute the application, which will search for information and remotely send it back to the FBI agent. A specific instance illustrating the use of the NIT warrant can be discerned from Operation Torpedo, in which a website selling child pornography was infected with the malware. The malware would search for the computers accessing the website and any of its images, data, or private messages. This information was used to prosecute visitors to the website in question. [8]

While the NIT can effectively search a computer remotely or utilize other means of seizing information on anonymous people, the targeted people may not necessarily be criminals, and the information is not part of a criminal scheme. However, due to the nature of the prosecution process, it is difficult to tell if a person has been searched by the FBI, mostly when the government also anonymously exists on the Darknet.

In addition to this, the NIT makes use of vulnerabilities and exploits to such vulnerabilities to continue searches, and most of such vulnerabilities and exploits can be found on the Darknet as well. This becomes a question of whether the government will inform developers of such vulnerabilities or reserve them for further NIT warrants. [8]

# Bitcoin, Fourth Amendment and Rule 41

Bitcoin is pseudonymous and not tangible, similar to an email, meaning that there are unique identities associated with each one. The only difference between them is the personal identity attached to them; just like an email, someone can have a random email or Bitcoin address without a given name, but unlike an email, the Bitcoin can be traced to an origin. Since this would remove the user's privacy, Bitcoin's development is driven by many people who believe that the online market should give users the ability to retain their privacy.

A considerable concern within the Bitcoin community revolves around the Federal Government privacy policies. Many users who buy and sell Bitcoin are deeply concerned with losing their assets by seizure of the Federal Government. For example, if one user sells to another user involved in criminal activities, both users will be overseen by the Federal Government. The laws that allow this to happen are under the Fourth Amendment and Rule 41 policies created by the Supreme Court.

The Fourth Amendment protects citizens from unlawful searches and seizes without probable cause, supported by the Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized [11]. In other words, the federal government cannot take, search, or freeze any, or all private property, unless someone is suspected of a crime with reasonable evidence. The 'Third-Party Doctrine' suppresses the idea of having the right to privacy since there is no legitimate expectation of privacy in information if a user voluntarily accepts the third-party provider's policies.

Whenever a user lacks a reasonable expectation of privacy and allows these third parties to access their information, then the Fourth Amendment's protections against unreasonable searches and seizures are not triggered [11]. This would allow the Federal Government to search through criminals involved with illegal transactions through the Blockchain of Bitcoin exchanges. If the Bitcoin originates from a third party or online exchange, Bitcoin is subjected to being seized by the Federal Government if a crime was committed.

Rule 41 is similar to the Fourth Amendment; however, differences apply for specific instances of probable cause. Under Rule 41, persons or property will be subject to search and seizure if one of the four criteria is met—one evidence of a crime leading to a suspect's arrest. Two, contraband or fruits of crime or other items illegally possessed. Three, a property designed for use, intended use, or used in committing a crime. Four, a person to be arrested or a person who is unlawfully restrained. Once the judge of the state authorizes the affidavit, the warrant allows search for and seizer of a person or property with the authorized and use of a tracking device [12].

The governing laws allow Rule 41 to act independently when dealing with Bitcoin transactions used for criminal activities. Authorities who suspect someone of a crime may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant [12]. Since Bitcoin is considered to be stored electronically, this means that the Federal Government has the power to place Bitcoin underneath this Rule. In other words, all online transactions are considered to be electronically stored information and must be treated as such.

These two legal proceedings work together when trying to prosecute someone for a crime. The tracking bitcoin through a currency exchange would be similar to using a tracking device on a person or property. Implementing some sort of indication system that allows authorities to be notified when suspicious activity occurs would disrupt the frequent movement of funds between bank accounts held by different persons or located in other foreign countries. One case follows these proceedings as an example of these two legal actions taking place.

# Fourth Amendment used in Fifth Circuit Court Rules

According to the ruling of a three-judge panel from Fifth Circuit courts, the American government's Fourth Amendment does not apply to bitcoin transactions that are used in a crime if they stem from virtual currency exchanges [13]. This does not apply to bitcoins from peer to peer transactions originating from mining pools or finding bitcoins through mining pools. Any bitcoin generated from mining is considered to be under the protection of the Fourth Amendment.

In other words, bitcoin exchanges are considered bank entities, and under the Supreme Court decision from 1939 called the United States v. Miller, any bank records are not protected by the Fourth Amendment [13]. These include bitcoin exchanges since they originate from bank transfers. Exchanges are considered a financial institution, with virtual currency exchanges, providing Bitcoin users with a transfer method [13]. For example, if someone is suspected of selling illegal drugs by transferring bitcoin, then the same rules apply in court if the cryptocurrency is generated from an online exchange. However, if the transaction used bitcoins and that cryptocurrency did not originate from an exchange, then the search and seizure of those bitcoins would not be held up in the court of law.

This creates jurisdictional issues since the locating and seizing of bitcoins requires either the physical location of the bitcoin wallet or the private keys to the virtual online wallet, making the detection of illegitimate use of bitcoin transactions harder for authorities. Even though each transaction is publicly recorded onto the ledger, tracing the origin easier allows the owner to retain their Anonymity. Now, if other U.S. Judges make contradictory rulings on this particular manner of authority, then Bitcoin might be appealed again as a personal asset protected by the Fourth Amendment. Until then, Bitcoin's originating from virtual exchanges like Coinbase will not be protected and will be subjected to seized by the Federal Government.

# Privacy Values over Bitcoin

Blockchain does much more than just tangle around some of the most troubling criminal cases. More profoundly, it distinctively upsets the structural design of the fundamental beliefs on privacy policy for American citizens. The debate begins when someone uses blockchain transactions to commit crimes. Individuals who purchased their cryptocurrency from a reputable exchange will have their transactions followed back to them if they are suspected of committing a crime. The doctrinal proxy of privacy arises when an individual mines from the genesis block and uses their bitcoin to commit a crime [14].

Bitcoin and ledger technology is now hitting the mainstream, and countless human interactions, legitimate and illegitimate, are being recorded permanently—and visibly— into distributed digital ledgers. Authorities will have an easier time locating criminals with the advancement of this technology in the digital age. The open-sourced ledger technology, shared digital architecture thus challenges authorities to reassess two core premises of modern Fourth Amendment doctrine: that a "reasonable expectation of privacy" upholds the Amendment's promise of a right to be "secure" against "unreasonable searches," and that "a reasonable expectation of privacy" is tantamount to total secrecy [14].

In the court's view, the "main difference" between cryptocurrency exchanges and a traditional brick-and-mortar bank was that cryptocurrency exchanges deal with virtual currency while traditional banks deal with physical fiat currency. The court deemed that difference insignificant since both virtual and traditional banks were subject to the same regulatory scrutiny as financial institutions, such as the Bank Secrecy Act, and maintained the same "limited" information concerning customer identities and transactions [15].

This creates technological difficulties for the early detection of Bitcoins being illegitimately used and does not give authorities any advantages for figuring out if the suspect is the Bitcoin wallet owner. Despite these disadvantages, the search and seizure of Bitcoins are possible. The most effective way for law enforcement to seize these assets would be through obtaining the private keys linked to the Bitcoins or by confiscating the Bitcoin wallet.

# How cryptocurrencies used in drug dealing

Information technology has been rapidly developed in recent decades. This helps modern society transform many aspects of people's life nowadays. The development and transformation in technology allow people to gain many technical advantages in pharmaceutical and trading. That said, the advent of cryptocurrency has opened a new path for trading goods in modern life. Cryptocurrencies like Bitcoin, Ethereum, and Ripple have emerged and allowed people to amass their wealth with billions of digital currencies. While many people invest their savings funds in the cryptocurrency exchange to make legal money, others take advantage of cryptocurrency's anonymity feature to gain illicit profit on the dark side. For instance, many malicious actors or criminals utilize the cryptocurrency to make an illegal profit while hiding their identities behind the system. According to Kristin Finklea, many criminal organizations and individuals have been using an overlay network called Darknet to conceal themselves and exploit this system by carrying out so many illegal activities such as drug dealing, gun trading, and counterfeit money [16]. Thus, this section investigates and focuses on how cryptocurrencies are used in the sale of illicit drugs.

# Cryptocurrencies act as the security layers for drug dealing

According to Judith and David, the crypto markets have tremendously changed online criminal markets by providing four security levels [18]. First, crypto markets require their customers to obtain and use an "anonymizing tool such as Tor or the Invisible Internet Project (I2P)" to hide their secret identities when doing business. In the joint report of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), the authors stated that darknet markets are accessible via an online anonymous network called Tor, which stands for The Onion Router [1]. The United States Naval Research Laboratory staff originally developed this superior service. Notably, Paul Syverson, Michael G. Reed, and David Goldschlag are the critical people in Tor's project. Besides, Tor was intentionally designed to protect the U.S intelligence from malicious attackers or terrorists under anonymous communication. That said, Tor is an anonymization service that "allows users to browse the web without revealing their identity or location" [1]. In other words, Tor is a perfect tool to disguise someone under many pseudonyms and enable many anonymous hosts to publish controversial and sensitive content on their websites without exposing themselves to the public [1]. Due to these features, many criminal organizations exploit and take advantage of Tor to anonymously sell illicit drugs on the darknet market. Second, all the participants in crypto markets must use cryptocurrencies such as Bitcoin for their digital payments. This is because the transactions via cryptocurrencies are complicated to trace. The criminals protect themselves by using cryptocurrencies along with Tor to mask their identity when the transaction happens completely. With the help of cryptocurrencies, buyers and sellers are entirely becoming anonymous on the darknet network. According to the report of EMCDDA, darknet marketplaces have achieved covering the illicit drug trading using cryptocurrencies [1]. Hence, the malicious actors add another hidden layer above Tor's protection using cryptocurrencies such as Bitcoin. The goal is to remove the government's unnecessary involvement to cover up all traces of illegal activities. Without the need to use fiat currencies, cryptocurrencies enable the darknet marketplace to be free from the government's control and the judiciary's interference. Third, crypto markets also implement escrow systems that add extra security and increase their confidence in the transactions. Finally, crypto markets develop feedback and review systems that are like Amazon or eBay. This helps the customers evaluate and get better ideas about the vendors and their illicit drugs. Thus, this demonstrates that cryptocurrencies become an exchange tool for a criminal purpose, especially drug dealing, because it provides many security layers to protect participants' identities in the darknet markets.

# Cryptocurrencies reduce the visibility of drug dealing and contacts with global customers

To further understand how cryptocurrencies are used in drug dealing, let us investigate the difference between the traditional offline and drug crypto markets. According to Judith and Rebecca, drug dealers use many strategies to operate the offline drug market to avoid the detection of law enforcement as much as possible [17]. For example, drug dealers may choose the locations that help them stay away from the range of police's presence or even employ the 'ward' to track and identify where the drug transaction should occur. Besides, the traditional offline drug dealers attempt to reduce their visibility to the police or law enforcement by using inexpensive mobile phones to arrange the transaction between buyers and sellers. In this strategy, the buyers and sellers must know each other through the trusted introductions [17]. Hence, the traditional offline market is considered a "closed" drug market [17].

On the other hand, drug dealing in crypto markets is completely reversed. The drug vendors set up their business "in plain sight of law enforcement," thanks to the help of Tor and cryptocurrencies [17]. The buyers and sellers can make the deal through the darknet forum or hidden website under anonymous names. This creates obstacles for law enforcement hard to find and trace illegal activities as well as participants. However, Judith and Rebecca stated that "cryptocurrencies, like bitcoin, are not completely anonymous" [17]. In other words, if the digital money is used for criminal purposes, the use of cryptocurrencies does not provide "complete anonymity and the immunity from prosecution" [1]. There are chances that law enforcement can track and reveal the darknet users' identities. With that said, darknet users must find a way to improve the cryptocurrencies and ensure their identity is concealed. The popular way of obscuring traces between payments and users is tumbling or mixing [1] [17]. For example, the tumblers, like BitBlender, Grams, and Bitcoin Frog, provide reliable concealment of a user's destination that makes blockchain analysis becoming extremely difficult to perform [17]. Therefore, cryptocurrencies allow vendors to open and expand their business worldwide via the darknet network. The vendors can particularly transact business with unknown or strange customers online without risking their identity to be detected. Thus, the crypto market is recognized as an "anonymous open" drug market [17].

# Cryptocurrency is a method for money laundering in drug dealing

The proliferation of cryptocurrencies enables darknet users to trade in illicit drugs under untraceable transactions. After each transaction, vendors typically receive their payments in cryptocurrencies such as Bitcoin. These amounts of money can be either used to purchase other goods or convert into fiat currencies as money laundering. Unlike the fiat currencies, which can be traced back to the original buyers and sellers, the cryptocurrencies hide both parties' identities, create anonymous transactions, and conceal the server's locations or where the transaction takes place. Accordingly, this makes cryptocurrencies a perfect medium of exchange for selling illicit goods and services such as drug dealing. For example, according to the report of EMCDDA, the Greek law enforcement authorities discovered and arrested a Russian criminal who was responsible for operating huge laundering cash in the United States. The culprit was accused of laundering more than 4 billion in USD via Bitcoin transactions [1]. Therefore, cryptocurrencies are undoubtedly becoming attractive in the criminal market, and money launderers worldwide use them to collect and disperse funds for their crimes.

# Conclusion

The survey paper has summarized the current researches on Darknet, the illegal transactions being marketed, their connection to the Fourth Amendment and rule 41, the use of the Network Investigation Technique (NIT), and the amounts of protection used for user privacy on the illegal markets.

The marketing and selling of illegal drugs by criminals have been a recurring event throughout the ages of human society. With each age, the marketing and transaction method has been adapted to newer techniques to outmaneuver the law. In the present age, information and Anonymity have taken root as the most critical aspects of drug dealing transactions, and the Darknet became the connection between dealers and addicts. Criminals use Tor to search the Darknet for illegal services and cryptocurrencies such as bitcoin to pay for them anonymously. In addition to this, drug dealers use shortcomings of the law, as seen by how courts interpret the Fourth Amendment, to send services either physically, such as mailing drugs, or virtually, such as downloading illegal programs or media. Rule 41 attempts to virtually address this issue by allowing access, search, and seizure of computer information if specific criteria are met. The NIT is one method of exercising the warrant given by Rule 41, one example being malware accessing a suspect device and sending any information found back to the agent employing this method. Cryptocurrencies are widely used when dealing with illegal services because it allows privacy and Anonymity when concluding transactions, mainly when used alongside Tor. While the bitcoins can be traced, if they are traced using a ledger, the bitcoins owner will remain anonymous, and if traced by the coin exchange, the trace may be subject to fourth amendment rights. The illegal transactions on Darknet utilize multiple layers of protection for preserving the privacy of the users involved, such as the use of Tor, purchasing using cryptocurrencies, and escrow systems. This allows the markets to conduct business in plain sight of the law enforcers, who can explore the illegal marketplace but can not trace the host or users of it.

The interpretation of the law regarding virtual crime continues to change to cover unforeseen loopholes. As searching and prosecuting methods evolve, the illegal side of the internet continues to search for methods of evading the searches and prosecutions.

# Reference

[1] *Drugs and the darknet: perspectives for enforcement, research, and policy*, 01-Nov-2017. [Online]. Available: https://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet\_en. [Accessed: 01-Nov-2020].

[2] A. authors, D. M. & T. Rid, and Additional informationNotes on contributorsDaniel MooreDaniel Moore is a cyber-threat intelligence engineer and a PhD candidate in the Department of War Studies at King's College London.Thomas RidThomas Rid is a professor at King's. His new book, "Cryptopolitik and the Darknet," *Taylor & Francis*. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085. [Accessed: 01-Nov-2020].

[3] "Illicit Drug Abuse and Addiction," *Addiction Center*, 18-Sep-2020. [Online]. Available: https://www.addictioncenter.com/drugs/illicit-drugs/. [Accessed: 01-Nov-2020].

[4] Dea.gov. 2020. [online] Available at: <https://www.dea.gov/sites/default/files/drug\_of\_abuse.pdf> [Accessed 1 November 2020].

[5] The Mandarin. 2020. *The Darknet – A Wild West For Fake Coronavirus' Cures'? The Reality Is More Complicated (And Regulated) | The Mandarin*. [online] Available at: <https://www.themandarin.com.au/132732-the-darknet-a-wild-west-for-fake-coronavirus-cures-the-reality-is-more-complicated-and-regulated/> [Accessed 1 November 2020].

[6] Stewart, K., 2020. *THE FOURTH AMENDMENT, DARK WEB DRUG DEALERS, AND THE OPIOID CRISIS*. [ebook] Available at: <http://www.floridalawreview.com/wp-content/uploads/Stewart.pdf> [Accessed 1 November 2020].

[7] Korff, D., 2012. Comments on Selected Topics in the Draft E.U. Data Protection Regulation - Summaries and Proposed Amendments Only. *SSRN Electronic Journal*,.

[8] Adams, D., 2020. *The 2016 Amendments To Criminal Rule 41: National Search Warrants To Seize Cyberspace, 'Particularly' Speaking*. [online] Papers.ssrn.com. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3335987> [Accessed 1 November 2020].

[9] Constituteproject.org. 2020. *Constitute*. [online] Available at: <https://www.constituteproject.org/constitution/United\_States\_of\_America\_1992> [Accessed 1 November 2020].

[10] En.wikipedia.org. 2020. *Network Investigative Technique*. [online] Available at: <https://en.wikipedia.org/wiki/Network\_Investigative\_Technique> [Accessed 1 November 2020].

[11] “Fourth Amendment,” *Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/constitution/fourth\_amendment. [Accessed: 01-Nov-2020].

[12] “Rule 41. Search and Seizure,” *Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/rules/frcrmp/rule\_41. [Accessed: 01-Nov-2020].

[13] Satoshi Nakamoto's Bitcoin White Paper: A 12-Year Old Summary of Robust Unstructured Simplicity NEWS, "4th Amendment Does Not Protect Bitcoin Data, U.S. Fifth Circuit Court Rules," *Bitcoin News*, 05-Jul-2020. [Online]. Available: https://news.bitcoin.com/4th-amendment-does-not-protect-bitcoin-data-us-fifth-circuit-court-rules/. [Accessed: 01-Nov-2020].

[14] School, S., 2020. *Transparency Is The New Privacy: Blockchain'S Challenge For The Fourth Amendment | Stanford Law School*. [online] Stanford Law School. Available at: <https://law.stanford.edu/publications/transparency-is-the-new-privacy-blockchains-challenge-for-the-fourth-amendment/> [Accessed 1 November 2020].

[15] Amendment, A., 2020. *A Little Less Privacy: Cryptocurrency Transactions Under The Fourth Amendment | New York Law Journal*. [online] New York Law Journal. Available at: <https://www.law.com/newyorklawjournal/2020/07/27/a-little-less-privacy-cryptocurrency-transactions-under-the-fourth-amendment/?slreturn=20200923011537> [Accessed 1 November 2020]

[16] Finklea, K., 2017. *Dark Web*. [ebook] Congressional Research Service. Available at: <https://fas.org/sgp/crs/misc/R44101.pdf> [Accessed 1 November 2020].

[17] J. Aldridge and R. Askew, "Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement," *International Journal of Drug Policy*, 11-Jan-2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0955395916303140. [Accessed: 01-Nov-2020].

[18] J. Mounteney, A. Oteo, and A. Bo, *The internet and drug markets*. Luxembourg: Office for Official Publications of the European Communities, 2016.

[19] "What are illegal drugs?," *Positive Choices*. [Online]. Available: https://positivechoices.org.au/students/what-are-illegal-drugs. [Accessed: 04-Nov-2020].