Viktoriia Ivaniuk, Serhiy Banakh*

Cryptocurrency-Related Cybercrimes in Ukraine

Abstract

Cybercrime, including cryptocurrency-related cybercrime, has become widespread in recent years. Despite a thorough study of cybercrime issues, there is still no legislative position on the legal regulation of cryptocurrencies and the responsibility for cryptocurrency-related cybercrime in Ukraine. The authors classify and characterize all cryptocurrency-related cybercrimes into five groups. In view of the spread of cryptocurrency-related cybercrimes, the EU's counteraction measures have been analyzed. Ways to prevent and counteract to cryptocurrency-related cybercrimes in Ukraine are suggested.

I. Introduction

The main feature of the globalization trends of our time is the dynamic development of all spheres of society, in particular, various innovative technologies. The convenience of paying for goods in online stores, the high speed of transactions, the use of modern technologies to ensure the security of financial transactions have led to the popularity of cryptocurrencies around the world. However, in May 2018, United Nations Secretary-General *António Guterres* outlined significant benefits for humanity provided by new technologies, including big data and analytics, artificial intelligence and automation, but highlighted new forms of crime creation in an address on the opening day of the 27th Session of the UN Commission on Crime Prevention and Criminal Justice[1]. *Cybersecurity Ventures* predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015[2].

Cybercrimes are constantly modifying and the mechanism of their implementation is improving. As a result, cryptocurrency-related cybercrimes have emerged. In addition, there are difficulties in investigating cybercrimes as law enforcement agencies need to be knowledgeable in modern technology at least like cybercriminals. Cyberat-

* *Viktoriia Ivaniuk*, Postgraduate Student at the Department of Constitutional, Administrative and Financial Law, Ternopil National Economic University, Ternopil, Ukraine; *Serhiy Banakh*, Candidate of Juridical Sciences (Ph. D.), Associate Professor at the Department of Criminal Law and Procedure, Ternopil National Economic University, Ternopil, Ukraine.

1 United Nations Secretary-General António Guterres highlights priorities, urgent need to tackle global threats at UN Crime Commission in Austria. www.unodc.org. Retrieved from https://www.unodc.org/unodc/en/press/releases/2018/May/united-nations-secretary-general-antnio-guterres-highlights-priorities--urgent-need-to-tackle-global-threats-at-un-crime-commission-in-austria.html.

2 *Morgan, S.*, Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. cybersecurityventures.com., 2018. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

OER 1/2020, DOI: 10.5771/0030-6444-2020-1-217

tacks are becoming more complex, harder to detect, and at the same time, these methods are quickly reaching a wide audience. That is why improvements in the hardware and software available to cybercriminals, existence of an illegal market for cybercrime sales caused the rise of cybercrimes. From this perspective, cryptocurrency-related cybercrimes, ways to prevent and counteract them are pressing issues for research.

II. The concept of cybercrime

In accordance with the content of Convention on Cybercrime 2001, cybercrime is an action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data, for which the criminalisation is provided[3]. Having ratified the Convention, Ukraine has identified cybercrime as a socially dangerous act in cyberspace and / or with its use, the responsibility for which is provided by the law of Ukraine on criminal liability and / or recognized as a crime by international treaties of Ukraine (Article 1 of the Law of Ukraine 'On the basic principles of ensuring cybersecurity in Ukraine')[4]. At the same time, there is no complete list of crimes envisaged by the Criminal Code of Ukraine, considered as cybercrime, and even more so cryptocurrency-related cybercrimes.

Considering the fact that cryptocurrency can be traded on specialized online exchanges, with the development of the cryptocurrency market has appeared many wishing to gain it illegally, in particular by theft of malicious software, hacking cryptocurrency wallets and exchanges. In that context, on January 27, 2018, the news came out that one of the largest cryptocurrency exchanges in the world *Coincheck* has lost some $534 m (£380 m) worth of cryptocurrencies in a hacking attack on its network[5]. That is why, in order to formulate proposals on prevention and counteraction to cryptocurrency-related cybercrimes, we will distinguish their main types and features.

III. Types of cryptocurrency-related cybercrimes

The growth of cryptocurrency types and amount has led to the creation of new criminal activities. We classify all cryptocurrency-related cybercrimes into five main types:

1. Crypto-jacking is a criminal offense that involves the introduction of a special code on a website on the Internet that can generate cryptocurrencies, using the power of the site users' CPU, that is, in fact, secretly mining cryptocurrencies

3 Convention on Cybercrime, 23.XI.2001. European Treaty Series – No. 185. www.europarl.europa.eu. Retrieved from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

4 Zakon Ukrainy «Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny» [The Law of Ukraine «On the basis of ensuring cyber security in Ukraine»]. zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

5 Coincheck: World's biggest ever digital currency 'theft' (2018). www.bbc.com. Retrieved from https://www.bbc.com/news/world-asia-42845505.

without users' explicit permission on behalf of a hacker[6]. Typically, cryptojacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it. The invisible page could be a malicious page, or a legitimate page the user did not intend to visit – for example, a page on the user's banking site that authorizes the transfer of money[7].

2. Cryptocurrency theft via hacks of third-party intermediaries that support cryptocurrency transactions and mining. Such intermediaries include currency exchanges used to convert cryptocurrencies into and from hard currencies and other virtual currencies, marketplace escrow services, cryptocurrency cloud mining marketplaces used to sell and buy hashing power, online wallets and mixing services. According to data gathered and assessed by *Chainanalysis*, thefts via hacks account for approximately 847,000 Bitcoin to date. A much-publicised and costly example of such theft occurred via the hack of the *MtGox Bitcoin* exchange from 2011 to 2013, which resulted in the loss of approximately 660,000 Bitcoins, which is approximately 80 % of all Bitcoin stolen from 2011 to 2018[8].
3. Substitution of payment details. The principle of committing this crime is that when transferring cryptocurrency from one wallet to another, a virus is triggered that replaces the address of the wallet to which the transfer is being made. Not every participant in the cryptocurrency market re-checks the copy of the e-wallet copied. Thus, cryptocurrencies do not fall into that electronic purse, and it is impossible to identify the owner.
4. Cryptocurrency phishing. The essence of this crime is that the participants of the cryptocurrency market are lured to a fake site, where he downloads his e-wallet and enters a password. Thus, these data fall into the hands of criminals, who further steal cryptocurrencies available in the electronic purse. Attackers send a seemingly legitimate text message from user's crypto wallet provider that requires user to perform an action, such as cancel a transaction or login to user's account[9]. So, on June 16, 2018, the cyber police of Ukraine exposed online fraudsters who created fake cryptocurrency web exchanges. The criminal group was defrauding citizens who wanted to conduct cryptocurrency transactions. Attackers, with specific programming knowledge and skills, have created their own CMS content management system for sharing sites. The web resources created mimicked the legal activity of web-based exchangers on multidirectional conversion of cryptocurrencies and received bogus positive ratings. The victims transferred the money to

6 *Imam, F.*, Malware spotlight: Crypto-jacking. 2019, securityboulevard.com, Retrieved from https://securityboulevard.com/2019/10/malware-spotlight-crypto-jacking/.

7 Clickjacking. www.imperva.com. Retrieved from https://www.imperva.com/learn/application-security/clickjacking/.

8 *Broadhead, St.*, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180–1196.

9 *Sinkevičiūtė, E.*, Crypto phishing: digital pickpockets are coming for your wallet, 2019, www.fyde.com. Retrieved from https://www.fyde.com/resources/crypto-phishing-digital-pickpockets-are-coming-for-your-wallet.

electronic wallets, registered on counterfeit documents of foreign citizens. After the money was credited, the abusers stopped the web exchanger and opened a new fraudulent web resource instead[10].

5. Darknet markets offerings. The darknet is a network "that is purposefully hidden; it has been designed specifically for anonymity... the darknet is accessible only with special tools and software — browsers and other protocol beyond direct links or credentials". Such tools and software include "The Onion Router" (Tor) network and browser. The ready availability of illicit goods and services, coupled with near-anonymity, makes the darknet a key, if niche, part of the cybercrime ecosystem[11].

IV. Ways to prevent and counteract to cryptocurrency-related cybercrimes

The spread of cryptocurrency-related cybercrimes is setting more stringent security standards around the world today. To equip Europe with the right tools to deal with cyber-attacks, the European Commission and the High Representative are proposing a wide-ranging set of measures to build strong cybersecurity in the EU. This includes a proposal for an EU Cybersecurity Agency to assist Member States in dealing with cyber-attacks, as well as a new European certification scheme that will ensure that products and services in the digital world are safe to use. It will improve the EU's preparedness to react by organising yearly pan-European cybersecurity exercises and by ensuring better sharing of threat intelligence and knowledge through the setting up of Information Sharing and Analyses Centres. In addition, it will help implement the Directive on the Security of Network and Information Systems which contains reporting obligations to national authorities in case of serious incidents[12].

Moreover, Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, containing Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises was adopted in 2017. According to this Blueprint, in case of an EU wide crisis with cyber elements, coordination at Union political level of the response shall be carried out by the Council, using the Integrated Political Crisis Response (IPCR) arrangements. Within the Commission, coordination will take place in accordance with the ARGUS rapid alert system. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the EEAS Crisis Response Mechanism is activated. The Blueprint describes how these well-established Crisis Management mechanisms should

10 *Chabanova, D.*, Kiberzlochyntsi v Ukrayini stvoryuvaly feykovi veb-obminnyky kryptovalyut [Cybercriminals created fake web exchanges of cryptocurrencies in Ukraine], 2018, www.unn.com.ua. Retrieved from https://www.unn.com.ua/uk/news/1736432-kiberzlochintsi-v-ukrayini-stvoryuvali-feykovi-veb-obminniki-kriptovalyut [in Ukrainian].

11 *Broadhead, St.*, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180–1196.

12 State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks. ec.europa.eu. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193.

make full use of existing cybersecurity entities at EU level as well as of cooperation mechanisms between the Member States[13].

In Ukraine, we propose to take a number of following measures to prevent and counteract to cryptocurrency-related cybercrimes at the national level:

1. To establish the legal status of cryptocurrency and provide liability for the unlawful possession of cryptocurrency. From that perspective it is necessary to:
   - adopt Law of Ukraine that would regulate the legal regime of cryptocurrencies, mining, activity of cryptocurrency exchanges, other problematic aspects;
   - amend the Criminal Code of Ukraine on Cryptocurrency-related cybercrimes. These changes should concern 5 sections of the Special Part of the Criminal Code of Ukraine:
     1. Chapter VI. Criminal Offenses against Property.
     2. Chapter VII. Economic Criminal Offenses.
     3. Chapter IX. Crimes Against Public Safety.
     4. Chapter XVI. Criminal Offenses Related to the Use of Electronic Computing Machines (Computers), Systems and Computer Networks and Telecommunication Networks.
     5. Chapter XVII. Criminal Offenses In Office.

These changes should consist of a new version of the criminal norms containing the features of already existing corpus delicti and the adoption of the criminal law rules with new corpus delicti.

First of all, we consider it expedient to legally determine cryptocurrency as the subject matter in such crimes as: "Theft" (Article 185 of the Criminal Code of Ukraine), "Legalization (laundering) of criminally obtained income" (Article 209 of the Criminal Code of Ukraine), "Financing of terrorism" (Article 258–5 of the Criminal Code of Ukraine), "Acceptance of an offer, promise or illegal benefit by an official" (Article 368 of the Criminal Code of Ukraine).

Disposition of the norm of Art. 185 of the Criminal Code of Ukraine reveals signs of simple corpus delicti "Theft", where "someone else's property" is defined as subject matter of the crime. However, in the law enforcement practice of Ukraine, mistakes in the qualification of criminal acts are frequent, since the subjects of law enforcement activities do not always correctly interpret the notion of "someone else's property" in the context of this crime.

Therefore, we propose to the legislator to supplement the clause contained in Art. 185 of the Criminal Code of Ukraine ("Theft") by an additional clause, which shall read as follows:

> "5. In Articles 185, 190, 191, under other people's property it should be understood property that has a value and is alien to guilty person (movable and immovable property, cash, securities, cryptocurrencies, etc.), as well as the right to property and property actions, electrical and thermal energy".

13 Annex to the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, 13.9.2017. ec.europa.eu. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF.

As for the composition of the crime “Legalization (laundering) of criminally obtained income” (Article 209 of the Criminal Code of Ukraine), the subject matter of the crime are both funds and other property obtained as a result of committing a socially dangerous unlawful act that preceded the legalization (laundering) of income.

It should be noted that neither the disposition of the provision that criminalize the legalization (laundering) of criminally obtained income, nor clause to it, do not disclose the meaning of “other property.” Therefore, we consider it advisable if Art. 209 of the Criminal Code of Ukraine would contain a clause that would disclose the meaning of “other property.” Therefore, in the context of Art. 209 of the Criminal Code of Ukraine under “other property” we offer to mean “movable and immovable things, securities, cryptocurrencies, etc.”

Similar situation exists with Art. 258–5 of the Criminal Code of Ukraine «Financing of terrorism». The subject matter to promote the creation or operation of a terrorist group or terrorist organization are funds (including funds obtained or acquired through the use of property owned or controlled, directly or indirectly, by persons assisting terrorism or related legal and natural persons) or other property. "Other property" may be property obtained both legally and illegally, as property that is in free civilian circulation and property that is in restricted circulation or at all removed from it. In turn, we consider that the financing of terrorism can be carried out using cryptocurrencies. Therefore, we are convinced of the need for the legislator to amend Art. 258–5 of the Criminal Code of Ukraine, which would consider the possibility of financing terrorism through the use of cryptocurrencies.

The expediency of introducing cryptocurrency as the subject matter of crime can be seen in Art. 368 of the Criminal Code of Ukraine, that provides for criminal liability for acceptance of an offer, promise or illegal benefit by an official. It is well known that the subject matter of this crime is illegal benefit. Today the content of subject matter of this crime is disclosed in a clause to Art. 364–1 of the Criminal Code of Ukraine (“Abuse of authority by an official of private legal entity, regardless of organizational form”) as following: under “illegal benefit” it should be understood cash or other property, benefits, privileges, services, intangible assets, any other intangible or non-monetary benefits that are offered, promised, given or received without legal grounds.

In turn, we propose to the legislator to carry out a new revision of the content of this clause, by detailing "other property" as the subject matter of crimes, provided by Art. 368, 368–3, 368–4, 369, 369–2, 369–3, 370 of the Criminal Code of Ukraine, stating that under “other property” it should be understood movable and immovable things, valuable metals, securities, cryptocurrencies, etc.

Moreover, in the direction of criminal protection of the sphere of cryptocurrencies we propose the legislator to introduce two separate crimes into the Criminal Code of Ukraine: "Forgery of Means Providing Access to Cryptocurrencies, Unlawful Issuance or Use of Cryptocurrencies" and "Creation, Use, and Dissemination of Harmful Computer Programmes Intended for Unsanctioned Access to Cryptocurrencies, Electronic Money".

Therefore, Chapter VII of the Special Part of the Criminal Code of Ukraine (“Economic Criminal Offenses”) is proposed to supplement with Art. 200–1 of the Criminal Code of Ukraine, which would read as follows:

"Article 200–1. Forgery of means providing access to cryptocurrencies, unlawful issuance or use of cryptocurrencies

1. Forgery of means providing access to cryptocurrencies, unlawful issuance or use of cryptocurrencies, -
   shall be punishable by imprisonment for a term of three to seven years.
2. The same actions, if repeated or committed by a group of persons upon their prior conspiracy, or in respect of large amount, -
   shall be punishable by imprisonment for a term of five to ten years with forfeiture of property.
3. Any such actions as provided for by paragraph 1 or 2 of this Article, if committed by an organized group or in respect of especially large amount, -
   shall be punishable by imprisonment of eight to twelve years with forfeiture of property».

Accordingly, Chapter XVI "Criminal Offenses Related to the Use of Electronic Computing Maschines (Computers), Systems and Computer Networks and Telecommunication Networks" should provide for criminal liability for the creation, use, and dissemination of harmful computer programmes intended for unsanctioned access to cryptocurrencies, electronic money. Signs of the corpus delicti should be set out in Art. 361–3 of the Criminal Code of Ukraine, the content of which would be as follows:

"Article 361–3. Creation, Use, and Dissemination of Harmful Computer Programmes intended for unsanctioned access to cryptocurrencies, electronic money

1. Creation, use, and dissemination of harmful computer programmes or other computer information, which are knowingly intended for unsanctioned access to cryptocurrencies, electronic money, –
   shall be punishable by restraint of liberty for a term of up to four years, or by compulsory labour for a term of up to four years,
2. The deeds provided for by Part One of this article which are committed by a group of persons by previous concert or by an organised group, or by a person through his/her official position, as well as which have caused a major damage or which have been made because of vested interest, –
   shall be punishable by restraint of liberty for a term of up to six years, or by compulsory labour for a term of up to six years with deprivation of the right to hold specified offices or to engage in specified activities for a term of up to four years.
3. The deeds provided for by Parts One or Two of this article if they have entailed heavy consequences or have posed a threat of their occurrence, –
   shall be punishable by deprivation of liberty for a term of up to eight years".

- To simplify access to electronic evidence by law enforcement agencies. A more effective law enforcement response, focused on identifying, tracking, and prosecuting cybercriminals, is critical to building an effective barrier to committing such crimes. In order to facilitate effective investigation and prosecution of criminal offenses, access to electronic evidence needs to be simplified.
- To use VPN services. This heavily secured connection ensures that sensitive data is securely transmitted without any interference from unauthorized persons. While

there is no perfect one-size-fits-all VPN service, choosing the best VPN service for you is key to securing your investment in cryptocurrencies and ensuring that no criminal activity is carried out via your space[14].

- To take privacy-enhancing measures to limit identity leakage. These measures include reliance on mixing services or tumblers (i.e., intermediaries who obfuscate transactions' traces), chain-hopping (i.e., converting into different virtual currencies) and not re-using Bitcoin addresses for different transfers. Here, it should be noted that these privacy-enhancing measures can facilitate anonymous cash-outs of ill-gotten gains from activities such as successful ransomware deployments.[15]
- To monitor quantitative data on various illegal activities in the field of cryptocurrency activity in order to form a purposeful effort to develop, adopt and apply standardized methods of counteraction to cryptocurrency-related cybercrimes.
- National and international agencies, organizations and institutions should collaborate in their efforts to curb cybercrime.

V. Conclusions

From these facts, one may conclude that cybercrime is one of the most pressing problems facing the international community today, as information and communication technologies are being implemented and developed much faster than legislators and law enforcement agencies can respond to. Therefore, the unified legislative regulation of the legal status of cryptocurrencies is a major task for both the international community and Ukraine. In order to prevent cryptocurrency-related cybercrimes, it is necessary to constantly monitor information threats, thorough studies of the functioning and development of cryptocurrency-related cybercrimes. Last but not least, the specialized legal education of the subjects of the cryptocurrency market should take place. We are convinced that the proposed changes in the article will help to prevent the commission of cryptocurrency-related cybercrimes and to implement the correct criminal-legal qualification of illegal actions in the sphere of cryptocurrency-related cybercrimes in Ukraine.

14 *Onibalusi, S.*, Is Cryptocurrency the New Target for Cyber Criminals?, 2019, readwrite.com. Retrieved from https://readwrite.com/2019/10/20/is-cryptocurrency-the-new-target-for-cyber-criminals/.

15 *Broadhead, St.*, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180–1196.