Problemy Prawa Karnego 2024, T. 8, nr 2
s. 1 z 16
ISSN 2353-9712
https://doi.org/10.31261/PPK.2024.08.02.01

Zsolt Gáspár
University of Pécs,
Hungary

https://orcid.org/0000-0003-3889-9560

The criminalization of cryptojacking in Hungary

Abstract: The study deals with the illegal abuse of cryptocurrency-mining, the phenomenon of the so-called 'cryptojacking', which is such an unknown crime that it has not even had a Hungarian name so far. The aim of the study is to examine the illegal mining of cryptocurrencies – as an abstract act – giving a detailed description about their characteristics and their place in the present Hungarian criminal law system. A further aim of the study is to make suggestions to the legislature and law enforcement bodies for the criminal assessment of the illegal mining of cryptocurrencies, based on the review of the relevant legal acts and the related cases.

Keywords: *cryptocurrencies, mining, criminal law, criminology*

1. Introduction

With the continuous expansion of the user base of the cryptocurrencies, the possibilities for their criminal use have significantly expanded. Due to this, we can encounter two types of cases in the practice. On the one hand, they can be the objects and the means of classic crimes (for example, fraud, money laundering), but, on the other hand, completely new, still unknown crimes can emerge, for which both the legislators and the law enforcement authorities must be prepared.

With the entry into force of the Act CXIX. of 2019[1], the legislators implemented a part of the rules of Directive 2018/843/EU[2], which ex-

[1] Act CXIX. of 2019 on the Prevention of Money Laundering and Terrorist Financing and on the Modification of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing.

[2] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial sys-

tended the scope of Act LIII. of 2017[3] to virtual currencies, exchange service providers between virtual currencies, and to custodian wallet providers[4], in addition, it introduced new definitions to the provisions of the ML Act.[5]

As a result, the concept of "virtual currency" has been defined in Section 3 (47) of the Act:

> *'A digital display of value not issued or guaranteed by a central bank or any public administration; does not have the legal status of a legal tender; it is electronically stored, accepted as an exchange, and in particular, it is electronically transferable and suitable for electronic trading.'*

Regarding cryptocurrencies, there are often doubts about their legal classification and categorization. [6] It is so because the domestic legal system rarely contains detailed rules, definitions, or provisions (likewise in the EU legislation). Ideally, the legal classification should be clear, comprehensible and beyond dispute, as differences of professional opinion during the application of the law, and the time spent on research and disputes between individual bodies can significantly prolong the legal procedures, not to mention that in such cases there is also the possibility of false justification.

The technological basis for cryptocurrencies is the blockchain, in which newer blocks of data are added individually to each previous block

tem for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

[3] Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing

[4] Act CXIX. of 2019, 1. § (1) n) - o)

[5] See further: Gál István László, 'A pénzmosás új magyar szabályozása 2021-től' (2021) 1 Büntetőjogi Szemle and Gál István László, 'A pénzmosás új elkövetési tárgya' in Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (eds.), Kriptoeszközök világa a jog és a gazdaság szemszögéből: konferenciakötet: 2021. március 19. Kriptoeszközök világa a jog és gazdaság szemszögéből konferencia válogatott tanulmányok (Pécs, Pécsi Tudományegyetem Állam-és Jogtudományi Kar, 2021)

[6] See further from the perspective of financial law: Szívós Alexander Roland, A kriptoeszközökkel kapcsolatos adózási kérdések áttekintése in Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (eds.), Kriptoeszközök világa a jog és a gazdaság szemszögéből: konferenciakötet: 2021. március 19. Kriptoeszközök világa a jog és gazdaság szemszögéből konferencia válogatott tanulmányok (Pécs, Pécsi Tudományegyetem Állam-és Jogtudományi Kar, 2021) and

^{S}zívós Alexander Roland, 'A kriptoeszközök és az adózás' in Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (eds.), Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet – Válogatott tanulmányok (Pécs, Pécsi Tudományegyetem, Állam-és Jogtudományi Kar, 2021) of data, resulting in a decentralized system.[7] From the user's point of view, the most important elements are the wallet and the private key. The two definitions are extremely closely related because to initiate or receive transactions in the cryptocurrency ecosystem, the user needs a wallet that he/she can create for any cryptocurrency. During this process, the service provider creates a series of data for the user, the so-called a private key, which is essentially a series of codes. This private key provides control over the user's cryptocurrencies.

The Section 315 (2) of the Hungarian Criminal Procedure Code[8] provides a method of enforcing the seizure of "*the electronic data used for payments*" in which "*an operation is performed on the electronic data that prevents the subjected person from disposing of the value of the data expressed by the electronic data*". The provision is particularly relevant to the private keys mentioned above, as the Criminal Procedure[9] Code thus allows the seizure of the private keys of a given cryptocurrency. [10]

According to the Criminal Procedure Code and its commentary, we can deduct the legal category of cryptocurrencies to which the law uses the term 'property value'. In terms of the European Union regulations, cryptocurrencies can also be classified as "property".[11] After reviewing the concept and legal quality of cryptocurrencies, it is worth addressing the so-far mentioned with the concept of mining. For a given transaction to be considered final, it is necessary to verify the operations. In the cryptocurrency systems, these processes are mostly performed by specified users using the computational capability of their computer gear to convert the transactions collected in each block into code sequences (hash) us-

[7] Kecskés András; Bujtár Zsolt, 'Felvetések a kripto eszközök szabályozása terén' (2019) 2 Controller Info 49, 49

[8] Act XC of 2017 on the Criminal Procedure

[9] See further: Herke Csongor, 'Magyar büntető eljárásjog' Pécs, (Baufirma, 2021) and Herke Csongor, 'Hungarian criminal procedure law' Pécs, (Baufirma, 2021) and Herke Csongor; Antonio Silva Sánchez; Alejandro Platero Alcón, 'Proceso penal en Hungría' Sevilla, (McGraw-Hill, 2020)

[10] Czine Ágnes, 'A kényszerintézkedések' in Belegi József (ed.), Büntetőeljárás jog: kommentár a gyakorlat számára – harmadik kiadás, (Budapest, HVG-ORAC, 2018), 693

[11] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC fixes in (3) of Article 3 the definition of 'property' as: assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets.

ing mathematical formulas.[12] Because the former process is quite energy-demanding, the system generates new cryptocurrencies for the miners as compensation, which are added to the cryptocurrency wallets predefined by the miner. In fact, this process can also be considered as the original way of obtaining cryptocurrencies. As more and more transactions take place in the system of each cryptocurrency, computers must solve increasingly complex mathematical formulas. As a result, mining a given unit of cryptocurrency costs a lot more energy, and the process damages the computer hardware in a more severe way.

2. Possible occurrences of illegal crypto-mining

After reviewing the above-mentioned conceptual fundamentals, it can be concluded that cryptocurrency mining is based entirely on the principle of voluntariness, so ideally the user is free to consider the expected costs, revenues, and other benefits of the operation. However, there are more and more cases when offenders pass on the negative consequences of mining to another person and use the computing capacity of that person to carry out the process. This act could take place in several ways, and it is worrying that we are finding examples of more and more cases of organized crime.[13]

2.1. Illegal cryptocurrency mining excessing the scope of authorization

One possible (and perhaps the easiest) way to carry out illegal mining is when the perpetrator uses computer tools that are already available to him/her even without prior acts. In this case, the computer equipment is often in the possession of the perpetrator or is easily accessible to him/her. This could be done, for example, when the perpetrator illegally uses a portable computer device entrusted to him or her by the employer, for mining purposes. Thus, although the perpetrator has the right of access

[12] Mátyás Szabolcs; Frigyer László; Prilenszky Géza, 'A virtuális fizetőeszközök szerepe és jelentősége a vagyonvisszaszerzés során' (2021) 3 Belügyi Szemle, 423

[13] See further on organized crime: Kőhalmi László, 'Szervezett bűnözés' in Barabás A. Tünde (ed.), Alkalmazott kriminológia. (Budapest, Ludovika Egyetemi Kiadó, 2020) and Tóth Mihály; Kőhalmi László, 'A szervezett bűnözés' in Borbíró Andrea; Gönczöl Katalin; Kerezsi Klára; Lévay Miklós (eds.), Kriminológia. (Budapest, Wolters Kluwer Kft., 2016) and Tóth Dávid; Gál István László; Kőhalmi László, 'Organized Crime in Hungary' (2015) 1 Journal Of Eastern-European Criminal Law

to the given information system, going beyond the scope of this right, he/she carries out the process to gain material benefits for him/herself or for a third party with the device concerned. This act – if no other violation occurs – may be suitable for committing a *'violation of the information system (data)'* defined in Section 423 (1) of the Criminal Code[14], but this must be separated from the crime of *'information system fraud'* pursuant to Section 375 of the Criminal Code.

Section 375 (1) of the Criminal Code defines the information system fraud as the following:

> *'Any person who, for unlawful financial gain, introduces data into an information system, or alters or deletes data processed therein, or renders data inaccessible, or otherwise interferes with the functioning of the information system, and thereby causes damage, is guilty of a felony punishable by imprisonment not exceeding three years.'*

Basically, the distinction between the two offenses is based on the fact of the damage, so in the case of illegal cryptocurrency mining, since the damage is an essential element of the offense, it follows that the crime of information system fraud should be established in such cases. This is because the two offenses cannot constitute a set of offenses, as the breach of information systems or data are the necessary means of committing the offense of information system fraud.[15] In this case, there is an apparent material set between the two crimes. In the case of the example mentioned above, it should be noted that the quality of the job or workplace is also an important condition. Pursuant to Paragraph 423 (4) of the Criminal Code, the above-mentioned act – if the violation of the information system (data) is committed against a public interest enterprise[16] – is classified a criminal offense, which is punished with imprisonment for two to eight years. If this qualifying circumstance exists, then, referring to the merger doctrine, an apparent formal set should be established, since in this case the act constitutes a more serious violation of the law, so the legal system must also respond to it with an adequate sanction. Accordingly, if the illegal cryptocurrency min-

[14] Act C of 2012 on the Criminal Code

[15] Akácz József, 'A vagyon elleni bűncselekmények' in Kónya István (ed.), Magyar Büntetőjog. Kommentár a gyakorlat számára, (Budapest, HVG-ORAC, 2015) 1378, 1415

[16] According to Paragraph 459. § (1) 21. of the Hungarian Criminal Code, a public interest enterprise means a public utility, a public transport operation, an electronic communications network; a logistic, payment or information center or operation operated to carry out the public interest tasks of a universal postal service provider, a plant manufacturing war materials or military equipment, and plants producing power or raw materials intended to be used in a plant.

ing is committed to the detriment of a public interest enterprise, in my opinion the crime of violating an information system or data *(Paragraph 423 (1) and (4) of the Criminal Code)* must be established, as the act completely exhausts the facts prescribed by the paragraph mentioned above. The significance of this can be illustrated by an incident in Russia, which happened in 2018. In that case, a group of nuclear researchers were arrested, and they were accused of illegally trying to mine Bitcoin in a top-secret nuclear assembly plant. According to the media reports, the perpetrators were employees of the Federal Nuclear Center in Sarov, western Russia, where they attempted cryptocurrency mining with the facility's supercomputer. The incident was also confirmed by the press service of the center concerned. The perpetrators were prosecuted after they were handed over to the Federal Security Service by the nuclear department's security department.[17]

2.2. Cyber-attacks launched for the purpose of illegal cryptocurrency mining (the so-called 'cryptojacking')

Another possible form of illegal cryptocurrency mining is referred to as 'cryptojacking' in the Anglo-Saxon literature. The point is that the perpetrator gains unauthorized access to the victims' computer equipment and then, using their computing capacity, the offender mines cryptocurrency for him/herself or third party. In practice, this is usually carried out by installing a malicious program (containing scripts) on the victim's computer that allows the perpetrator to access the device. This most often happens by clicking on links in e-mails of unknown origin or by visiting 'infected' websites.[18] Compared to the previous scenario, this form of illegal cryptocurrency mining therefore requires significantly more preparation on the part of the perpetrator, as in this case he/she does not have the concerned computer device at his/her disposal. The first phase of the offense is to place the program containing the malicious scripts in e-mail messages or on web pages, which always happens in a disguised form. It is common for the offenders to copy the 'image' of public service providers, banks or other service providers who are considered authentic by the average users, typically by using promotional letters, fee requests, invoices or other e-mails that are more common in everyday life, with the aim to build trust in the victims regarding their fake web surfaces and e-mails. Some e-mail

[17] 'Russian nuclear scientists arrested for, Bitcoin mining plot' https://www.bbc.com/news/world-europe-43003740 accessed 6 March 2022

[18] 'https://www.interpol.int/Crimes/Cybercrime/Cryptojacking' accessed 19 December 2021

service providers can distinguish these messages with relatively high accuracy and identify them as spams, but (especially) weaker e-mail programs require special care when opening these types of messages.

As in the other scenario, this type of illegal cryptocurrency mining also involves the perpetrator's intent to make a profit. One of the key elements of the ecosystem is that the mining users receive a so-called 'compensation' for making his/her computing capacity available to the system, but it should be noted that this compensation is rather low for the more valuable cryptocurrencies used by most users and for less frequently used cryptocurrencies, it means less money due to the lower value of the cryptocurrency. For the mining of more valuable cryptocurrencies, the computing capacity of the simple personal computers is usually not sufficient, therefore the so-called 'mining computers' or complete servers are usually used for this task. Based on this, the perpetrator, as most users have less powerful personal computers, can make quite a small profit per victim. Concerning this, during the investigation of such crimes, special attention should be paid to the detection of the full range of the victims, as for the above-mentioned reason, in most of the cases, perpetrators try to reach a layer as wide as possible. Thus, this form of illegal cryptocurrency mining, when examined in terms of proportionality, does not necessarily favor criminals.

A good example for the above-mentioned case can be the Japanese lawsuit alleging that a 24-year-old perpetrator, called Yoshida Shinkaru illegally used a program called Coinhive for mining Monero, which is one of the most infamous cryptocurrencies. To conduct this activity, he/she encrypted the script in a program that is used in computer games to 'facilitate' the participation in the game, more directly, to cheat. The program was posted by the perpetrator on his own online blog for free access and download. As the installation was successful, the program started to mine Monero for the offender from the devices of the unsuspecting downloaders. To highlight the disproportionate and unfavorable nature of the conditions, it is worth noting that despite the fact that the program made available by the perpetrator has been downloaded more than 90 times, Yoshida Shinkaru has only made a total profit of 5,000 Japanese yen, which is around 14,000 HUF calculated at the exchange rate of 25th February, 2022, however, the offender has been sentenced by the Sendai District Court to one year in prison, the execution of which sentence was suspended for three years.[19]

[19] Charlie Osborne, 'Japan issues first-ever prison sentence in cryptojacking case' https://www.zdnet.com/google-amp/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/?fbclid=IwAR00OIs2mLn5akKQKdoSZ0_lySM6Y2KeQ4_vlD2tfaKdQlRjPH0RMU86qfo accessed 25 February 2022

In such cases, the determination of the number of victims is of paramount importance, as the scope of the circle of victims is also essential for the specific definition of the crime. As detailed above, the commission of a crime does not necessarily cause significant material damage, however, the fact of the damage is obvious. According to the current Criminal Code in force, if the legal requirement establishes the crime of information system fraud in these cases, however, taking into account the fact that the damage is insignificant in relation to the number of victims and again referring to the merger doctrine, the correct step should be the establishment of the offense of violating a significant number of information systems or data dealt under Paragraph 423 (2) of the Criminal Code, in order to enforce the objectives of the law and trigger a law enforcement response best suited to the crime committed.

In addition to increasing the number of victims, perpetrators try to find solutions to the above-dealt problem in other ways, too. One good solution to that is to focus on the quality instead of the quantity. It is therefore appropriate to target victims who use high-performance machines that are more powerful than the simple computers of the average users. These machines can be found especially in large enterprise environments; therefore, such enterprises are more exposed to the risk of illegal cryptocurrency mining. In February 2018, for example, the vulnerability of the 'Kubernetes' open source application management software used by the automotive company Tesla was exploited[20] by the perpetrators for illegal mining, but so was the multinational insurance company, Aviva and the international digital security company, Gemalto.[21] RedLock's report on security trends on cloud services for 2018 found that 25% of the large enterprises experienced illegal cryptocurrency mining for their cloud services, which shows a significant increase from the 8% that they measured the year before.[22] For companies with such significant technological resources, there is a risk of much more significant damage than for ordinary users. This is perfectly supported by the case of two Iranian citizens who are alleged to have hacked cloud services[23] used by a Missouri-based

[20] Charlie Osborne, 'Tesla cloud systems exploited by hackers to mine cryptocurrency' https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/ accessed 25 February 2022

[21] Warwick Ashford, 'Unprotected Kubernetes consoles expose firms to cryptojacking' https://www.computerweekly.com/news/252435544/Unprotected-Kubernetes-consoles-expose-firms-to-cryptojacking accessed 25 February 2022

[22] 'https://redlock.io/news/redlock-cloud-security-trends-report-highlights-lack-of-compliance-with-industry-standards' accessed 28 February 2022

[23] See further on the topic: Klein Tamás, 'A felhőszolgáltatások egyes jogi kérdései – különös tekintettel az Európai Unió szabályozására' in Klein Tamás (ed.), Tanulmányok a technológia-és cyberjog néhány aktuális kérdéséről. (Budapest, Médiatudományi Intézet,

company for illegal cryptocurrency mining, resulting in the cloud provider billing the company $ 760,000.[24] As in the previous case, the protection of critical infrastructures is of paramount importance, so that attacks against such objects, whether internal or external, should be adequately sanctioned by the criminal law. It should be emphasized that similar incidents have already taken place within Europe, where the perpetrators have broken into the IT system of the public utility plant with the intention of mining cryptocurrency.[25]

2.3. Other methods of illegal crypto mining

In addition to the two scenarios mentioned above, there are also more difficult-to-judge cases of illegal cryptocurrency mining. Typically, this is the case if the offender commits the act by means located in certain community spaces (libraries, internet cafes, universities, schools). If services are available in the relevant community area, within the framework of which the service provider makes the given devices and the Internet access available to the users of the service for a limited period of time – unless otherwise provided by the internal regulations of the service provider – I consider that the violation can only be established beyond the timeframe paid by the users, more precisely the information system fraud, due to the fact of the damage. However, this applies only in the case of the offense described in the first scenario, since if the offender acts as mentioned in the second case, he/she did not have any right to the service provided nor did he give even a partial compensation for the service providers, so in these cases the information system fraud can be identified for the full time-interval.

In cases where we cannot talk about a specific time limit (typically cryptocurrency mining in schools, universities, some libraries), it is less clear how to judge such acts. It should be emphasized, however, that in these cases a distinction must also be made between the types of offense detailed above. Similarly to the previous conditions, the place of the as-

2018) and Máté István Zsolt, 'A felhőszolgáltatások igazságügyi informatikai szakértői vizsgálata' (2015) Infokommunikáció és Jog

[24] 'https://www.justice.gov/usao-edmo/pr/two-iranian-nationals-indicted-local-cryptojacking-case?fbclid=IwAR0fNFkcbq1qXDXDLD5o3Ill9RVBjetXK78VhBb3YB5Dg7oS-LKYk8b_KsoM' accessed 6 March 2022

[25] A good example for the above-mentioned situation is the case of a water plant. See further: Lily Hay Newman, 'Now Cryptojacking Threatens Critical Infrastructure, too' https://www.wired.com/story/cryptojacking-critical-infrastructure/ accessed 6 March 2022

sessment of the crime is a key issue. The reason for this is that it is not always possible to establish a criminal offense, since – if the given service provider has made its devices and Internet access available to users without restrictions - the act does not exhaust any of the crimes prescribed by the Criminal Code. If such a situation arises, in my viewpoint, it is the responsibility of the service providers to limit the use of their resources within the framework of their own internal regulations, which should draw the attention of the users to the possible criminal and civil law consequences for the non-compliance with their regulations. If this happens, in my opinion, in the case of subsequent incidents, it is already possible to refer to the exceeding of the right of access, which justifies the violation of the information system or data. Internal regulations would not be necessary to establish the offense of information system fraud, however, the essential factual element of establishing this crime is the damage taken, which is quite difficult to find in those cases where users have unrestricted access to the service provider's resources, let it be the Internet access or the use of specific devices (e.g., computers, tablets, smartphones[26]). The damages in these acts can usually manifest in increased power consumption or the shorter lifespan of the hardware, but none of these factors can be measured exactly, and it would not be viable, neither expected of the victims to prove these facts in accurate numbers. Based on these, I believe that it is more appropriate and effective to supplement the internal regulations to have a simpler legal assessment.

Of course, in addition to the detailed crime patterns, illegal cryptocurrency mining can occur in multiple ways and even extremely abstract legal cases can appear. A good example of this is the so-called Siacoin-case, which took place in China in 2017. A group of hackers have made a conspiratorial agreement with several Chinese Internet cafe maintenance companies that a program developed by them for cryptocurrency mining, called Siacoin will be placed on the devices of the Internet cafes as part of a system upgrade. The perpetrators used hundred thousands of computers for unauthorized cryptocurrency mining, earning more than 5 million Chinese yuan (approximately $800,000 at the exchange rate of the time concerned). [27] [28]

[26] See further on the dangers of smartphones: Kraut Andrea; Kőhalmi László; Tóth Dávid, 'Digital Dangers of Smartphones' (2020) 1 Journal of Eastern-European Criminal Law.

[27] Wolfie Zhao, 'Internet Cafes Hacked to Mine $800k in Siacoin Cryptocurrency' https://www.coindesk.com/markets/2018/06/19/internet-cafes-hacked-to-mine-800k-in-siacoin-cryptocurrency/ accessed 2 March 2022

[28] The case was still being investigated while this study was written. See further: https://hznews.hangzhou.com.cn/shehui/content/2018-06/16/content_7020998_2.htm accessed 2 March 2022

3. The investigation of the crime

It is a common problem in Hungary that the investigation of crimes involving cryptocurrencies is hampered since in many cases the staff of the investigating authorities and the district prosecutor's offices competent to supervise the investigation do not have the necessary IT skills to solve such crimes. Certain forms[29] of cybercrime[30], whether they involve cryptocurrencies or not – after decades of their first appearance – are still a phenomenon that the investigating authorities cannot solve or do not want to deal with due to their complexity and the cumbersome investigative tasks that they require.[31] However, it should be emphasized, that these tools, especially but not exclusively among the younger age groups, seem to be becoming more widespread, with more and more investors, companies, and in some cases, entire countries.[32] The material gravity of the certain crimes committed in connection with cryptocurrencies also requires that the cases should not be closed by a termination decision based on the unidentifiable identity of the offender or lack of jurisdiction. It is a fact that this type of crime almost without exception affects several jurisdictions, and in most cases the perpetrators are non-Hungarian citizens living abroad, however, the relevant EU and domestic legislation implementing them fully establishes jurisdiction, even in cases when the crime was only partially committed in Hungary.[33]

[29] Just like the cases of online identity theft. See further on the topic in more details: Tóth Dávid, 'Identity crimes on the darknet and the social media' (2021) KSZ. Büntetőjogi Szemle and Tóth Dávid, 'Személyiséglopás az interneten' (2020) 1 Büntetőjogi Szemle

[30] See: Herke Csongor, 'A kiberbűnözés és a teljesen önvezető járművek' in Barabás Andrea Tünde; Christián László (eds.), Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est. (Budapest, Ludovika Egyetemi Kiadó, 2021)

[31] Mátyás Szabolcs, Frigyer László and Prilenszky Géza have also highlighted in their study that the investigating authorities should need more detailed courses on the topic of cryptocurrencies to facilitate their practice. See: Mátyás; Frigyer; Prilenszky, Op. Cit. 427.

[32] A good example can be the case of El Salvador, where the world's best-known cryptocurrency, Bitcoin, was adopted for the first time as a legal tender. With this milestone, the country's economic actors also had to adapt to financial services and challenges augmented by cryptocurrencies. See further: Kate Linthicum, 'El Salvador's president buys bitcoins 'naked,' he boasts. His experiment is costing his nation millions' https://www.latimes.com/world-nation/story/2022-02-23/el-salvador-bitcoin-experiment accessed 19 March 2022 and Marco Quiroz-Gutierrez, 'El Salvador says tourism is up 30% since it made Bitcoin legal, but the country is still on the brink of economic disaster' https://fortune.com/2022/02/23/el-salvador-bitcoin-law-tourism-up-30-percent-imf-senate/ accessed 19 March 2022

[33] See further: Tóth Dávid; Gáspár Zsolt, 'Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén' (2020) 2 Büntetőjogi Szemle.

Thanks to innovations in the Anti-Money Laundering Act and the Criminal Procedure Code, the investigative authorities have also been given a legal basis to take measures in the field of asset recovery.[34] The SIRIUS project[35], which operates within the framework of Europol, is a great help in this process. A list has been drawn up at the request of the investigating authorities to contact the major cryptocurrency service providers, which – based on the practical experience – contains details such as the additional requirements that are expected for data release (such as a prosecutorial license or a judicial license). Evidently, the list does not cover all cryptocurrency service providers, but in most cases, it can help to identify the perpetrator and conduct the investigation.

4. Conclusions

Based on the above, it can be concluded that the illegal mining of cryptocurrencies poses a potential threat that affects not only ordinary users, but also larger players in the corporate sector, and even utilities classified as critical infrastructures, therefore the danger of the act to the society is an indisputable fact. In this very diverse crime, as highlighted above, the quantity and quality of the victims is a key factor, so great emphasis should be placed on exploring the circle of victims as fully as possible during the investigation.

The other element of the crime is the fact of the damage, which, according to the analyzed legal cases, can range from the insignificant value to the significant or particularly significant value. Therefore, largely due to the need for an individual assessment in each case, it will be a very difficult task to develop a uniform law enforcement practice.

Although the ‘closure’ of Coinhive in 2019[36] reduced the amount of these crimes relatively significantly, the problem cannot be considered resolved as illegal cryptocurrency mining has not disappeared, this crime is still often committed by the perpetrators to seek financial gain and it is also a matter of time that a similar program like Coinhive spreads among users which will instantly multiply the number of such cases.

In my opinion – keeping in mind the remarks made in the study – according to the provisions of the current Hungarian Criminal Code, it is

[34] See: Szathmáry Zoltán, ‘Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban’ (2015) 11 Magyar Jog

[35] https://www.europol.europa.eu/operations-services-innovation/sirius-project accessed 15 March 2022

[36] Michal Salat, ‘The End of Coinhive; The end of cryptojacking?’ https://blog.avast.com/coinhive-shuts-down accessed 14 March 2022

rather difficult to classify the different occurrences of illegal cryptocurrency mining in the practical application of the law, because of which it is almost impossible to develop a uniform practice. In many cases it is necessary to go back to the principles of criminal law for the purpose of the law to be enforced by the law enforcement body, and eventually the subjective legal position of the judicial employee will appear in the case instead of an objective legal regulation. Regarding cybercrime, the Criminal Code sets out rather just broad facts, which in the practice is only partially a solution, as they cover a significant part of the ways in which crimes can be committed, but it must be highlighted that the technological development has reached a level that this type of legislation will not necessarily be sustainable.

In the present case, since the reviewed criminal offenses can be classified according to the Criminal Code in force, instead of amending the act, it would be sufficient to address the relevant issues in the commentary of the Criminal Code, possibly in the form of a legal unity decision, which would highly facilitate the activities of the investigating authorities, the prosecution, and the court.

I also consider it necessary to organize professional trainings for investigative authorities and judicial staff about the cryptocurrencies to prepare the professionals, during which, after the overview of the minimum IT knowledge concerned, the practical law enforcement issues and certain related procedural acts, the classification of criminal offenses and the possibilities for asset recovery should be emphasized.

It is equally important to accentuate the need for university courses that focus on the technological innovations of the past decade. In general, the prevailing view in law schools is that the greatest emphasis should be placed on the teaching of classical legal subjects, however, the challenges of the present age are often pushed into the background as a result. The same can be stated for law enforcement training. It is an indisputable fact that future new professionals must practice in this changed world surrounded by technological innovations[37], and as a result, in addition to respecting classical legal subjects, new challenging phenomena[38] such as cryptocurrencies must be included in legal and law enforcement training.[39]

[37] See more further on the relationship between the technological development and criminal tendencies: Korinek László, 'Tendenciák korunk bűnözésében és bűnüldözésében' (2014) 1 Jura

[38] See for example: Miskolczi Barna; Szathmáry Zoltán, 'Büntetőjogi kérdések az információk korában: Mesterséges intelligencia, Big Data, Profilozás' (Budapest, HVG-ORAC, 2018) and Szathmáry Zoltán, 'Etikus és nem etikus hacking – a kéretlen sérülékenységvizsgálat büntetőjogi kérdései' (2020) 6 Magyar Jog

[39] See further: Polt Péter, 'Rendészeti képzés – az alkalmazható tudásra fókuszálva' in Boda József; Tóth Nikolett Ágnes (eds.), 50 éves a rendészeti felsőoktatás. (Budapest, Ludovika Egyetemi Kiadó, 2021)

Bibliography

Akácz József, ‘A vagyon elleni bűncselekmények’ in Kónya István (ed.), Magyar Büntetőjog. Kommentár a gyakorlat számára, (Budapest, HVG-ORAC, 2015) 1378, 1415

Charlie Osborne, ‘Japan issues first-ever prison sentence in cryptojacking case’ https://www.zdnet.com/google-amp/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/?fbclid=IwAR00OIs2mLn5akKQKdoSZ0_lySM6Y2KeQ4_vlD2tfaKdQlRjPH0RMU86qfo accessed 25 February 2022

Charlie Osborne, ‘Tesla cloud systems exploited by hackers to mine cryptocurrency’ https://www.zdnet.com/article/tesla-systems-used-by-hackers-to-mine-cryptocurrency/ accessed 25 February 2022

Czine Ágnes, ‘A kényszerintézkedések’ in Belegi József (ed.), Büntetőeljárás jog: kommentár a gyakorlat számára – harmadik kiadás, (Budapest, HVG-ORAC, 2018), 693

Gál István László, ‘A pénzmosás új elkövetési tárgya’ in Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (eds.), Kriptoeszközök világa a jog és a gazdaság szemszögéből: konferenciakötet: 2021. március 19. Kriptoeszközök világa a jog és gazdaság szemszögéből konferencia válogatott tanulmányok (Pécs, Pécsi Tudományegyetem Állam-és Jogtudományi Kar, 2021)

Gál István László, ‘A pénzmosás új magyar szabályozása 2021-től’ (2021) 1 Büntetőjogi Szemle

Herke Csongor, ‘A kiberbűnözés és a teljesen önvezető járművek’ in Barabás Andrea Tünde; Christián László (eds.), Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére: Navigare necesse est. (Budapest, Ludovika Egyetemi Kiadó, 2021)

Herke Csongor, ‘Magyar büntető eljárásjog’ Pécs, (Baufirma, 2021)

Herke Csongor, ‘Hungarian criminal procedure law’ Pécs, (Baufirma, 2021)

Herke Csongor; Antonio Silva Sánchez; Alejandro Platero Alcón, ‘Proceso penal en Hungría’ Sevilla, (McGraw-Hill, 2020)

https://www.europol.europa.eu/operations-services-innovation/sirius-project accessed 15 March 2022

https://hznews.hangzhou.com.cn/shehui/content/2018-06/16/content_7020998_2.htm accessed 2 March 2022

‚https://www.interpol.int/Crimes/Cybercrime/Cryptojacking’ accessed 19 December 2021

‘https://www.justice.gov/usao-edmo/pr/two-iranian-nationals-indicted-local-cryptojacking-case?fbclid=IwAR0fNFkcbq1qXDXDLD5o3Ill9RVBjetXK78VhBb3YB5Dg7oSLKYk8b_KsoM’ accessed 6 March 2022

‚https://redlock.io/news/redlock-cloud-security-trends-report-highlights-lack-of-compliance-with-industry-standards’ accessed 28 February 2022

Kate Linthicum, ‘El Salvador’s president buys bitcoins ‘naked,’ he boasts. His experiment is costing his nation millions’ https://www.latimes.com/world-nation/story/2022-02-23/el-salvador-bitcoin-experiment accessed 19 March 2022

Kecskés András; Bujtár Zsolt, 'Felvetések a kripto eszközök szabályozása terén' (2019) 2 Controller Info 49, 49

Klein Tamás, 'A felhőszolgáltatások egyes jogi kérdései - különös tekintettel az Európai Unió szabályozására' in Klein Tamás (ed.), Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről. (Budapest, Médiatudományi Intézet, 2018)

Korinek László, 'Tendenciák korunk bűnözésében és bűnüldözésében' (2014) 1 Jura

Kőhalmi László, 'Szervezett bűnözés' in Barabás A. Tünde (ed.), Alkalmazott kriminológia. (Budapest, Ludovika Egyetemi Kiadó, 2020)

Kraut Andrea; Kőhalmi László; Tóth Dávid, 'Digital Dangers of Smartphones' (2020) 1 Journal of Eastern-European Criminal Law

Lily Hay Newman, 'Now Cryptojacking Threatens Critical Infrastructure, too' https://www.wired.com/story/cryptojacking-critical-infrastructure/ accessed 6 March 2022

Máté István Zsolt, 'A felhőszolgáltatások igazságügyi informatikai szakértői vizsgálata' (2015) Infokommunikáció és Jog

Marco Quiroz-Gutierrez, 'El Salvador says tourism is up 30% since it made Bitcoin legal, but the country is still on the brink of economic disaster' https://fortune.com/2022/02/23/el-salvador-bitcoin-law-tourism-up-30-percent-imf-senate/ accessed 19 March 2022

Mátyás Szabolcs; Frigyer László; Prilenszky Géza, 'A virtuális fizetőeszközök szerepe és jelentősége a vagyonvisszaszerzés során' (2021) 3 Belügyi Szemle, 423

Michal Salat, 'The End of Coinhive; The end of cryptojacking?' https://blog.avast.com/coinhive-shuts-down accessed 14 March 2022

Miskolczi Barna; Szathmáry Zoltán, 'Büntetőjogi kérdések az információk korában: Mesterséges intelligencia, Big Data, Profilozás' (Budapest, HVG-ORAC, 2018)

Polt Péter, 'Rendészeti képzés – az alkalmazható tudásra fókuszálva' in Boda József; Tóth Nikolett Ágnes (eds.), 50 éves a rendészeti felsőoktatás. (Budapest, Ludovika Egyetemi Kiadó, 2021)

'Russian nuclear scientists arrested for ‚Bitcoin mining plot' https://www.bbc.com/news/world-europe-43003740 accessed 6 March 2022

Szathmáry Zoltán, 'Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban' (2015) 11 Magyar Jog

Szathmáry Zoltán, 'Etikus és nem etikus hacking – a kéretlen sérülékenységvizsgálat büntetőjogi kérdései' (2020) 6 Magyar Jog

Szívós Alexander Roland, A kriptoeszközökkel kapcsolatos adózási kérdések áttekintése in Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (eds.), Kriptoeszközök világa a jog és a gazdaság szemszögéből: konferenciakötet: 2021. március 19. Kriptoeszközök világa a jog és gazdaság szemszögéből konferencia válogatott tanulmányok (Pécs, Pécsi Tudományegyetem Állam-és Jogtudományi Kar, 2021)

Szívós Alexander Roland, ‘A kriptoeszközök és az adózás’ in Bujtár, Zsolt; Szívós, Alexander Roland; Gáspár, Zsolt; Szilovics, Csaba; Breszkovics, Botond (eds.), Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet – Válogatott tanulmányok (Pécs, Pécsi Tudományegyetem, Állam-és Jogtudományi Kar, 2021)

Tóth Dávid, ‘Identity crimes on the darknet and the social media’ (2021) KSZ. Büntetőjogi Szemle

Tóth Dávid, ‘Személyiséglopás az interneten’ (2020) 1 Büntetőjogi Szemle Tóth Dávid; Gáspár Zsolt, ‘Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés területén’ (2020) 2 Büntetőjogi Szemle

Tóth Dávid; Gál István László; Kőhalmi László, ‘Organized Crime in Hungary’ (2015) 1 Journal Of Eastern-European Criminal Law

Tóth Mihály; Kőhalmi László, ‘A szervezett bűnözés’ in Borbíró Andrea; Gönczöl Katalin; Kerezsi Klára; Lévay Miklós (eds.), Kriminológia. (Budapest, Wolters Kluwer Kft., 2016)

Warwick Ashford, ‘Unprotected Kubernetes consoles expose firms to cryptojacking’ https://www.computerweekly.com/news/252435544/Unprotected-Kubernetes-consoles-expose-firms-to-cryptojacking accessed 25 February 2022

Wolfie Zhao, ‘Internet Cafes Hacked to Mine $800k in Siacoin Cryptocurrency’ https://www.coindesk.com/markets/2018/06/19/internet-cafes-hacked-to-mine-800k-in-siacoin-cryptocurrency/ accessed 2 March 2022

Regulations and Documents

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Act CXIX. of 2019 on the Prevention of Money Laundering and Terrorist Financing and on the Modification of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing

Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing

Act XC of 2017 on the Criminal Procedure

Act C of 2012 on the Criminal Code