Criminal legal regulation of the blockchain functioning sphere in Russia: challenges and barriers

Sona Martirosovna Mkrtchian*

FSAEI HE "Volgograd State University", Department of Criminal Law/Institute of Law, Volgograd, Russia

Abstract. Research background. Despite the enormous attention of the scientific community, legislators, and law enforcement officials to the development and implementation of measures to combat cybercrime, the sphere of blockchain functioning and cryptocurrency circulation remains outside the scope of most criminal law research. This causes perplexity in the context of the desire of state bodies to introduce blockchain technology in many significant areas of society, as well as to introduce a regulatory framework dedicated to the issues of private and public legal regulation of digital financial assets. Concerns are also caused by the increase in the number of cybercrimes and the increasing involvement in them of the blockchain technology and virtual currencies, the circulation of which is carried out based on blockchain. The need to study the prospects for criminal law regulation of the blockchain functioning spheres in the territory of the Russian Federation becomes more and more obvious in such conditions. Study objective: to identify and to study the main challenges (problems) for modern criminal law regulation of the blockchain functioning sphere, possible barriers (obstacles) that reduce the effectiveness of such regulation, as well as potential directions for responding to these challenges and overcoming such barriers. Methods: formal legal and comparative legal research methods are widely used in conjunction with systemic, logical, and philological methods of interpreting the norms of law. The empirical part of the study is based on the investigation of judicial and other law enforcement practices, as well as transcripts of meetings of the State Duma of the Russian Federation and information from the media about criminal offenses that have become widespread in the sphere of blockchain functioning. The analysis of modern foreign and Russian scientific literature relevant to the selected research topic is carried out. Results and novelty: it is the first time that comprehensive analysis of the challenges of the current stage of the blockchain functioning sphere development, as well as legislative, law enforcement, doctrinal, and social barriers for creating a system of effective and comprehensive criminal law regulation of the named sphere, is carried out. The author's concept of the directions of responding to the analyzed challenges and overcoming the corresponding barriers is presented.

*Corresponding author: s.mkrtchian1992@volsu.ru

Keywords: crime; Russian Federation; legislative acts; computer programs

1 Introduction

According to the Prosecutor General of the Russian Federation I. Krasnov, the number of crimes in the field of information technology has increased by 25 times and amounted to 294 thousand over the past five years, while only a quarter of them was solved [1]. At the same time, the Prosecutor General paid special attention to such features of modern cybercrime as the emergence of new methods of data encryption that maximize the anonymity of criminal actions, as well as the widespread criminal use of cryptocurrencies [1]. These data are of even greater interest in the light of recognizing the blockchain technology at the state level as a breakthrough digital technology capable of influencing the global financial system, the significance of this technology as well as other encryption and crypto protection technologies as conditions for the development of the electronic industry of the Russian Federation (based on the texts of orders of the Government of the Russian Federation dated August 14, 2019 No. 1797-r and dated January 17, 2020 No. 20-r). Moreover, from January 1, 2021, Federal Law No. 259-FZ of July 31, 2020, designed to regulate the sphere of circulation of digital financial assets, comes into force.

In such conditions, the questions of whether the Russian criminal legislation is ready to regulate relations arising in the sphere of blockchain functioning, and what obstacles may the Russian lawmaker and law enforcement face in the process of developing this area of relations naturally arise?

2 Methods

Formal legal and comparative legal research methods are widely used in conjunction with systemic, logical, and philological methods of interpreting the norms of law to study the provisions of Russian and foreign criminal legal and non-branch legislative acts. The empirical basis of the study was the judicial and other law enforcement practices of the Russian Federation, transcripts of the State Duma of the Russian Federation, as well as the information posted on the media about criminal offenses that have spread in the sphere of blockchain functioning. Particular attention is paid to the analysis of Russian and foreign criminal law and criminology literature to establish trends in scientific research on the topic under consideration.

3 Results

Table 1 shows main results.

Table 1. Main results.

Challenges/problems	Barriers/obstacles	Ways of overcoming
Transnational nature of the criminal activity	Legislative: an extremely narrow range of elements of computer crimes, liability for which is provided for by the Criminal Code of the Russian Federation	Harmonization of Russian and foreign/international legislation in the field of combating cybercrime
	Law enforcement: inability to identify and prosecute	

	criminals under the jurisdiction of other states	
	Doctrinal: a small number of relevant scientific research of a comparative legal nature on the issues of criminal law regulation of the modern information technologies sphere	
The emergence of cybercrime infrastructure	Legislative: the establishment of criminal liability only for the already accomplished fact of violation of the information protection regime	- extension of the norms of the Criminal Code of the Russian Federation to the areas of training criminal cyber practices and their technical support; - stiffening of licensing legislation in terms of control over the production and distribution of equipment and software for encrypting data or overcoming access to information.
	Law enforcement: Criminal prosecutions usually target either ordinary members of cybercriminal groups or individuals who have purchased malicious products from distributors	
	Doctrinal: lack of criminological research on cybercriminal groups and their professional spheres of influence;	
	Social: expanding the influence of virtual space on the lives of minors and young people	
The increased public danger of the perpetrators and the acts they commit	Legislative: - excessively mild sanctions for computer crimes or other crimes committed with the use or in relation to computer information; - lack of proper means of individualizing responsibility for computer and other similar crimes;	- harmonization of the limits of liability for computer crimes, taking into account foreign and international experience; - carrying out scientific research on the differentiation and individualization of responsibility; - expanding the range of measures to prevent victimization in the area under study, as well as centers for helping victims of cybercriminals; - expansion of educational activities on the essence of cybercrimes and their consequences for the individual, the society, and the state
	Law enforcement: the presence of an excessively wide range of grounds for mitigation of liability in the text of the Criminal Code of the Russian Federation	
	Doctrinal: lack of scientific research on the differentiation and individualization of liability for the computer or similar crimes.	
	Social: society does not always negatively assess such crimes, but at the same time accuses the victims of criminals of imprudence	

Constant update of schemes, methods, and means of committing cybercrime	Legislative: - casuistic legislative formulations; - lack of technologically neutral legislation.	- development by the Plenum of the Supreme Court of the Russian Federation and the General Prosecutor's Office of the Russian Federation of recommendations regarding the application and interpretation of the Code of the Russian Federation norms on crimes committed using information systems or in relation to them; - carrying out scientific research in this area with the emergence of breakthrough computer technologies being considered.
	Law enforcement: lack of uniformity in judicial and law enforcement practice	
	Doctrinal: lack of a sufficiently developed scientific basis for the study of criminal practices in the field of blockchain functioning	
Growth in the number of Russian citizens and organizations involved in illegal activities in the field of cryptocurrency turnover	Legislative: - uncertainty of the legislator's position regarding the essence of blockchain, cryptocurrencies and other similar technologies and categories; - constant desire to compensate for the lack of regulation of legitimate turnover by criminalizing certain acts in this sphere;	Invitation of the IT sphere representatives to a broad discussion of the problems of blockchain and cryptocurrency regulation at the legislative and law enforcement levels
	Law enforcement: incorrect application of the Criminal Code of the Russian Federation without considering the international legislation	
	Social: distrust of the IT community in statutory innovations and the activities of the legislator in this area in general	

4 Discussion

Currently, there are entire communities of professional cybercriminals who support the illegal acts of “non-professional hackers”, for example, Ransomware-as-a-Service (RaaS) [2]. Unfortunately, the provisions of Article 273 of the Criminal Code of the Russian Federation cannot cover the entire spectrum of such acts (as long as it only deals with the creation and distribution of malicious software). Article 138.1 of the Criminal Code of the Russian Federation is not intended for these purposes either. It is noteworthy that the foreign legislator has achieved some success here, establishing criminal liability for the distribution of instructions to produce malicious programs (part 2 of Article 144bis of the Criminal Code of Switzerland) or for advertising and possession of such programs, as well as equipment, access codes and passwords (Section 9a of Chapter 34 of the Criminal Code of Finland).

Analysis of the transcripts of the State Duma of the Russian Federation meetings for the period from 2015 to 2020 allows drawing the following conclusions: the distributed ledgers (blockchain) technology finds support in most cases (see, for example, transcripts of meetings from December 02, 2016, June 09, 2017, May 30, 2019, etc.), but reviews of cryptocurrency and initial coin offering are far from being unambiguous (transcripts of meetings from December 02, 2015, June 07, 2017, November 22, 2017, January 12, 2018, May 30, 2018, May 30, 2019, etc.). This uncertainty is largely the reason for the lack of uniformity in law enforcement practice. So, if the energy and computing power are used for the hidden mining of cryptocurrency illegally through a real connection to power units, then clause "b" of Part 2 of Article 165 of the Criminal Code of the Russian Federation applies; if infection of an indefinite number of computers with a botnet-type malware or unauthorized access to user traffic of Internet sites are executed, then in some cases Article 273 of the Criminal Code of the Russian Federation without reference to Article 165 of the Criminal Code of the Russian Federation is used, and in the other Article 165 without reference to Articles 272 and 273 of the Criminal Code of the Russian Federation is used. Considering the development of the cybersphere, the comprehensive protection of the interests of citizens and organizations is out of the question in the absence of official rules for qualifying crimes in similar and many other cases.

The doctrine of criminal law does not contribute to the formation of unity in legislative and law enforcement practice. So, the sphere of blockchain functioning and cryptocurrency turnover is either not considered at all as an object of criminal law research [3, 4], or these areas are considered only as areas of the spread of crimes against property or computer information or individual groups of economic crimes [5, 6]. Most foreign scientists pay attention only to the technical side of the issue. The legal aspects of blockchain and cryptocurrencies are given attention only from the standpoint of financial, economic, or tax law [7]. At the same time, attention should be paid to the predominantly criminological [8–10] with economic or statistical inclusion [11–13] or criminal procedure [14–16] biases of the relevant foreign studies. The question of the criminal liability scope remains without scientific discussion. This concerns not only sanctions for crimes against computer information but also means of individualizing responsibility. So, according to clause "k" of part 1 of Article 63 of the Criminal Code of the Russian Federation, the use of specially manufactured technical means is recognized as an aggravating circumstance, but nothing is said about the use of special skills and knowledge (for example, in the field of encryption and programming).

5 Conclusion

Areas of responding to challenges and overcoming barriers are shown in the Results table. Only the simultaneous implementation of these areas can guarantee effective and consistent criminal law regulation of the sphere of blockchain functioning and the turnover of cryptocurrencies. The results of this study can be useful in formulating the directions of Russia's criminal law policy in the field of combating cybercrime and improving the practice of applying the provisions of the Criminal Code of the Russian Federation. The study of the selected topic should be continued, for example, by studying the criminological aspect of the relevant topic, as well as foreign and international law enforcement practice.

The reported study was funded by RFBR, project number 20-011-00823.

References

1. I. Egorov, Genprokuror rasskazal o roste chisla kiberprestuplenii v Rossii v 25 raz [Prosecutor General spoke about the increase in the number of cybercrimes in Russia by 25 times]. Accessed on: March 9, 2021. [Online]. Available: https://rg.ru/2020/07/17/genprokuror-rasskazal-o-roste-chisla-kiberprestuplenij-v-rossii-v-25-raz.html
2. G. Hull, H. John, B. Arief, Crime Sci. **8**, 2 (2019). https://doi.org/10.1186/s40163-019-0097-9
3. N. Letelkin, Ugolovno-pravovoe protivodeistvie prestupleniiam, sovershaemym s ispolzovaniem informatsionno-telekommunikatsionnykh setei: vkliuchaia set "Internet" [Criminal and legal counteraction to crimes committed using information and telecommunication networks: including the Internet], Abstract of a PhD thesis (Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, 2018)
4. A. Zharova, Int. J. Cyber Criminol. **13(2)**, 255-269 (2019). Accessed on: March 9, 2021. [Online]. Available: https://www.cybercrimejournal.com/AnnaZharovaVol13Issue2IJCC2019.pdf
5. M. Prostoserdov, Ekonomicheskie prestupleniia, sovershaemye v kiberprostranstve, i mery protivodeistviia im [Economic crimes committed in cyberspace and applicable countermeasures]. Abstract of a PhD thesis (Russian State University of Justice, Moscow, 2016)
6. O. Stepanov, D. Pechegin, Russian Law Journal, **6(3)**, 149-171 (2018). https://doi.org/10.17589/2309-8678-2018-6-3-149-171
7. C. Rueckert, J. Cybersecur. **5(1)** (2019). https://doi.org/10.1093/cybsec/tyz004
8. M. Paquet-Clouston, B. Haslhofer, B. Dupont, J. Cybersecur. **5(1)** (2019). https://doi.org/10.1093/cybsec/tyz003
9. I. Agrafiotis, J.R.C. Nurse, M. Goldsmith, S. Creese, D. Upton, J. Cybersecur. **4(1)** (2018). https://doi.org/10.1093/cybsec/tyy006
10. C.M.M. Reep-van den Bergh, M. Junger, Crime Sci. **7**, 5 (2018). https://doi.org/10.1186/s40163-018-0079-3
11. M. Möser, R. Böhme, J. Cybersecur. **3(2)**, 127-135 (2017). https://doi.org/10.1093/cybsec/tyx007
12. A. Feder, N. Gandal, J.T. Hamrick, T. Moore, J. Cybersecur. **3(2)**, 137-144 (2017). https://doi.org/10.1093/cybsec/tyx012
13. S. Jain, E. Felten, S. Goldfeder, J. Cybersecur. **4(1)** (2018). https://doi.org/10.1093/cybsec/tyy003
14. J. Kamps, B. Kleinberg, Crime Sci. **7**, 18 (2018). https://doi.org/10.1186/s40163-018-0093-5
15. D.A. Bermudez Villalva, J. Onaolapo, G. Stringhini, M. Musolesi, Crime Sci. **7**, 17 (2018). https://doi.org/10.1186/s40163-018-0092-6
16. A. Leppänen, T. Toiviainen, T. Kankaanranta, International J. Cyber Criminol. **14(1)**, 63-80 (2020). Accessed on: March 9, 2021. [Online]. Available: https://www.cybercrimejournal.com/Lepp%C3%A4nenetalVol14Issue1IJCC2020.pdf