Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

MISTI 10.85.51
Scientific article

https://doi.org/10.32523/2616-6844-2024-147-2-230-241

Features of the use of cryptocurrencies in the commission of crimes in the field of high technology

A.G. Kan[1], T.M. Korzhumbayeva[2], S.Kh. Abdullina[3]

[1, 2, 3] Almaty Academy of the MIA of the Republic of Kazakhstan named after M. Esbulatov

(E-mail: [1]kan_torsan@mail.ru, [2]deadpoollol69@mail.ru, [3]sabinulya88@mail.ru)

Abstract. Today, a serious challenge for law enforcement is the threats posed by the so-called anonymous segments of the Internet, which are actively used by organized criminal communities to prepare and commit crimes, as well as for their safe financing using cryptocurrencies. The results of the study indicate that in scientific and practical terms, this area has been studied extremely poorly and needs comprehensive research. A significant foundation for this can be the advanced foreign experience of countries that have faced these threats before us and are currently developing effective methods of countering crimes in the field of high technology. The analysis of various materials in this direction shows the elements of the methodology of their disclosure, which, with appropriate systematization, can be adapted to Kazakh conditions and will contribute to effective counteraction by law enforcement agencies.

Keywords: internet, anonymous networks, cryptocurrency, blockchain, server, encryption, mining, transaction.

Received: 06.06.2024. Accepted: 08.06.2024. Available online: 30.06.2024.

Introduction

The commission of high-tech crimes using anonymous networks is largely related to the turnover of cryptocurrencies, which, in turn, is also anonymous. At the same time, despite its potential criminal component, the circulation of cryptocurrencies in the world is increasing, which is facilitated by global negative geopolitical and economic trends.

In 2017, speaking on the sidelines of the Astana Economic Forum, he outlined the specific mechanisms of these processes, noting that the phenomena of cryptocurrencies and blockchain technology will entail drastic changes for the financial market, including banks. Most countries are actively exploring the possibilities of their adaptation to the current configuration of financial systems [1].

According to N. Nazarbayev, this will save the world from currency wars, speculation, avoid distortions in trade relations, and reduce volatility in the markets. A currency should have a simple, transparent emission mechanism that is subject to its consumers. Taking into account digitalization, the development of technologies such as blockchain, such a unit of account can be created in the form of a cryptocurrency [2]. At the same time, he also acknowledged that digitalization accompanies the growth of cybercrime, which in 2017 was recognized as the most serious threat to business [1].

Therefore, given the complexity and ambiguity of these processes, it seems necessary to study in more detail the institute of cryptocurrencies and the technologies on which they are built – blockchain.

The methodology

When writing the article, methods of both general scientific and legal nature were used in combination. More often, such methods as dialectical, statistical, comparative legal, and system-logical were used. In addition, cognitive methods such as synthesis, analysis, deduction, induction, questioning, interpretation, discursive analysis, and expert assessment were used. The use of these methods in combination made it possible to identify the high criminogenic potential of crimes in the field of information technology committed using cryptocurrencies through anonymous networks.

Findings/Discussion

The results of the study show that the volume of criminal content in anonymous networks increases significantly due to the active use of "dual-use" technologies by criminal formations, such as blockchain and cryptocurrencies. This contributes to the involvement of organized criminal groups in the commission of crimes, which, thanks to these technologies, develop their activities by increasing the efficiency of "laundering" criminal proceeds and their transfer to the legitimate economy.

A blockchain is a distributed database in which data storage devices are not connected to a common server. This database stores an ever-growing list of ordered records called blocks. Each

block contains a timestamp and a link to the previous block. The use of encryption ensures that users can change only those parts of the blockchain that they "own" in the sense that they have private keys, without which writing to the file is impossible. In addition, encryption ensures that copies of the distributed blockchain are synchronized for all users. Security in blockchain technology is provided through a decentralized timestamped server and peer-to-peer network connections. As a result, a database is formed, which is managed autonomously, without a single center. This makes blockchains very convenient for recording events (for example, making medical records), data operations, identity management, and verifying the authenticity of the source [4].

This technology was first implemented in 2009 as a component of the digital currency Bitcoin, where the blockchain plays the role of the main general registry for all transactions. Thanks to blockchain technology, Bitcoin has become the first digital currency that solves the problem of double spending (unlike physical coins or tokens, electronic files can be duplicated and spent twice) without using any reputable authority or a central server.

It should be noted that the emergence of blockchain technology and cryptocurrencies was preceded by a number of large-scale studies in the field of encrypted transactions. In 1983, David Chaum, a member of the Faculty of Computer Engineering at the University of California, Santa Barbara, thought about how to combine the anonymity of payments and their transparency for all market participants. The scientist proposed using the so-called "blind signature" algorithm, which allowed for a secret transaction between two anonymous participants, but at the same time informed outside observers about its occurrence. Then, together with his Israeli colleagues, Chaum developed "electronic cash" protocols, through which the conditional seller approves the transaction only after confirming the authenticity of an anonymous payment by a third party, and the buyer only needs to have proof of sending virtual money. This technology then became the basis for making transactions using Bitcoin [5].

The prototype of the mechanism for creating the cryptocurrency itself was invented in 1997 by the Briton Adam Beck. He suggested using the Hashcash anti-spam system, in which the sender performs many time-consuming operations, and the recipient verifies their authenticity very quickly. A year later, researcher Nick Szabo began work on a decentralized Bit gold monetary system that would save users from a variety of threats, including theft, counterfeiting, and even inflation. Szabo worked on his project until 2005 but was never able to ensure its launch.

All of the above developments were used by an unknown person or group of persons under the pseudonym Satoshi Nakamoto to create an electronic currency with completely anonymous transactions. At the end of October 2008, its technical description and the first version of the code appeared on the network. The blockchain system has become the basis for transactions with new electronic money, partly based on research by Chaum and Beck. The creators of Bitcoin developed a database that stores all transactions ever made in the form of publicly available blocks of information. A special mathematical algorithm links the blocks together so that when you change the contents of one of them, you will have to make edits to the next block, and then to the entire chain. Copies of the database are stored in Bitcoin wallets - encrypted clients that users create for themselves. The first wallet was created by Nakamoto himself in early 2009. With the help of a wallet, each of the completed and confirmed transactions is recorded

in one of the blocks, which is then attached to the common chain. When registering, the user is assigned their personal address, which is indicated when sending Bitcoin and ensures complete anonymity [5].

According to the idea of the developers, cryptocurrency is the "gold" of the virtual world. The amount of this "gold" is limited by calculations of the possible maximum allowable number of its presence in each specific system. There are three ways to get digital money:

1) purchase at a virtual currency exchange point;

2) on a virtual exchange;

3) by direct "mining", i.e. activities aimed at creating cryptocurrencies and/or validation in order to receive remuneration in the form of cryptocurrencies [6, p.34].

These operations are available to any user of the Internet information and telecommunications network, provided they have the appropriate software and hardware. At the same time, the use of the technology of the type under study faces a number of problems. So, in order to maintain a high level of security, the system constantly needs complex calculations, which is possible only on the basis of a high resource base. For Bitcoin, the developers solved this problem simply. Users who are associated with its "mining" are assigned a commission so that they provide their resource, that is, confirm the possibility of mining. In addition, for the security of the system, it is important that the resource base is distributed, and not under the control of a group that can use resources for various manipulations.

The mining process, named by analogy with mining, requires solving a number of complex mathematical problems, so miners need to use powerful computing resources on specially equipped computers. For each block created, they receive a reward in the form of a commission from transactions or newly created Bitcoin, and the complexity of mining is automatically adjusted every two weeks depending on the total number of blocks that have appeared during this time. At the same time, the first miners could only generate virtual money on their computers and transfer it to each other. The approximate Bitcoin exchange rate in 2009 ranged from 700 to 1600 units per dollar and increased over time [5].

A characteristic feature is that the cash volume of Bitcoin is always limited, it is impossible to replicate (print) this currency at someone's request. Its "extraction" is difficult from the point of view of a technical approach. Calculations are known that indicate that the viability of the cryptocurrency is provided by a certain algorithm and it is possible to "extract" no more than 21 million bitcoins. After that, "mining" is not possible.

At the same time, the amount of energy consumed plays an important role here. So, in December 2017, employees of the Federal Security Service of the Russian Federation conducted searches at Vnukovo airport due to cryptocurrency mining. The security services detained an airport employee who worked at the air traffic control center, from where controllers give commands to planes over Moscow and the region. A local system administrator assembled a cryptocurrency mining farm right at work, but the management noticed the power surges [7].

Similarly, in Kazakhstan, in early 2018, employees of the National Security Committee identified a criminal group that was engaged in mining cryptocurrencies using servers of state information systems of the departments of state Revenue of the Ministry of Finance in Karaganda, Atyrau, Aktobe and North Kazakhstan regions. These offenses fall under articles 207

("Disruption of the operation of an information system or telecommunications networks") and 210 ("Creation, use or distribution of malicious computer programs and software products") of the Criminal Code of the Republic of Kazakhstan [8].

Such facts are not isolated. A number of Kaznet sites promote the "mining" of cryptocurrency by intruders. Such conclusions were made at the Kazakhstan Center for Analysis and Investigation of Cyber Attacks. Increasingly, so–called mining scripts can be found on websites that use a client machine to mine cryptocurrencies. Using the WebTotem web resource monitoring system, the Center managed to register about 25 sites in Kaznet in just a day, the entrance to which is automatically provided by a computer to perform calculations related to the "mining" of cryptocurrency by an attacker. The list includes university websites (for example, enu.kz) and well-known company catalogs (nurbiz.kz): acastana.kz, adizel.kz, alemtour.kz, aql.kz, autism.kz, brp.kz, casualshoes.kz, cfakazakhstan.kz, tutmebel.kz, winners.kz, dizelya.kz, ecoislamicbank.kz, emu.kz (ENU), enu.kz, extremal.kz, gift-card.kz, gup.kz, investfunds.kz, invitation.kz, kazbilim-edu.kz, ksip.kz, edical-tour.kz, nashservice.kz, natures.kz, nspastana.kz, and nurbiz.kz [9].

At the same time, the history of the development and formation of Bitcoin is quite interesting. A year after its appearance, in February 2010, the first Bitcoin Market cryptocurrency purchase service appeared on the network, and in May, a user of the cryptocurrency forum decided to buy two pizzas for 10 thousand Bitcoin. In July, this cryptocurrency was written about on the Slashdot portal, popular among computer scientists, and the number of virtual money users began to grow sharply. As a result, within a month, 10,000 Bitcoins were worth $ 600, and many network users began actively mining cryptocurrency for themselves. This led to the emergence of the first Bitcoin exchange MtGox, which allowed not only to purchase, but also to exchange them for real money. The Bitcoin exchange rate rose rapidly – from 6 cents per unit in July to 50 cents in November; at the same time, the total market volume was estimated at $ 1 million.

In February 2011, Bitcoin equaled the value of the dollar, and in March exchanges were opened to exchange them for British pounds and Brazilian reals. At the same time, the Wikileaks website, famous for its revelations, began accepting donations from them. In April, Time magazine wrote about cryptocurrency, and the total volume of the Bitcoin market exceeded $ 10 million. In the summer of 2011, Bitcoin experienced a series of hacker attacks that seriously affected the exchange rate of the virtual currency. At first, one of the users stated that 25 thousand coins were stolen from him, which was approximately equal to 375 thousand dollars. And six days later, the MtGox exchange database was hacked, and the logins and passwords from the wallets of 60 thousand users were freely available. On the same day, hackers took over the account of one of the site's administrators, lowered the Bitcoin exchange rate from $ 17 to 1 cent per unit and tried to buy several thousand coins. The exchange had to be closed for a week; all prices were restored.

The negative effect was offset by the first Bitcoin conference held at the World Expo in New York in the same year 2011. A similar event was held in Prague in November. In parallel, materials about Bitcoin were published by Forbes and The Economist, and for the New York Times, a column about cryptocurrency was written by Nobel laureate in economics Paul Krugman. As a result, Bitcoin was talked about as a real alternative to traditional currencies.

In this regard, it is quite logical that the cryptocurrency itself has become the subject of criminal encroachment. On February 28, 2014, Mt. Gox (Japan), the oldest and largest electronic

currency exchange, declared bankruptcy. The exchange's management took this step after the largest hacker attack on the system, which led to the theft of about 750,000 Bitcoins, which accounted for approximately 6% of the issue of the entire cryptocurrency in circulation.

This crime has been solved. On July 25, 2017, at the request of American law enforcement agencies, Russian programmer Alexander Vinnik was detained in Greece, who was charged with laundering 4 billion US dollars criminally obtained through the cryptocurrency exchange, committing cyber fraud, stealing personal data, as well as hacking the Japanese Mt. Gox exchange, which provoked its bankruptcy.

2017 was a breakthrough year for Bitcoin and all known cryptocurrencies in general, as everyone learned about the cryptocurrency market. In 2017, Bitcoin rose from $908 in January 2017 to $12,300 as of December 30 (according to the Bitfinex exchange), and in December it reached $20,000. In 2018, its rate dropped sharply, falling below $7,000 by the middle of the year, then slowly went up, reaching by mid-2019, almost $8,000. After a series of ups and downs, by the middle of 2020, it reached values of more than $11,000.

According to experts, such fluctuations are due to the fact that the cryptocurrency is not provided by any economic factors (gold, gross domestic product, etc.), so its rate can easily collapse. This and other economic shortcomings arouse the distrust of the Governments of many States towards it. However, in some countries there are economic institutions, online stores or services that accept Bitcoin as payment for goods and services. In the modern world, virtual currency can be exchanged for rubles, dollars, electronic money using online servers such as, for example, 60sec, BaksMan, Ychanger, 24PayBank, ProstoCash, WMGlobus, Xchange. The crypto exchanges EXMO, BitFlip, BitMEX, LocalBitcoins, etc. are also known. Currently, there are about 600 different cryptocurrencies in circulation. Although most often payment transactions are made in Tether (36.8%), Bitcoin (23.4%) and Ethereum (13.1%) [10].

Kazakhstan also has its own cryptocurrency. So, in December 2017, Halyk Bank warned Kazakhstanis against investing in the so–called "first national cryptocurrency - Halykcoin". The bank warned that it has nothing to do with its creation and does not provide any guarantees regarding the safety of investments in this financial instrument. At the same time, the Internet resource www.halykcoin.org, declared as the official website of the project, is registered to an unidentified person, which raises doubts about the desire of developers to ensure proper transparency of the project. This site is anonymous, the main part of the functionality does not work, which most likely indicates fraud [11].

Apparently, this fact is an "echo" of more global processes. Thus, experts note that in 2015-2016, a network of groupings has developed in the European Union that provide services related to cryptocurrencies on a contractual basis. The locations of these groups are Germany, France, Italy and Spain. Within the framework of the "crime as a service" model, the groups carried out attacks on 160 portals, databases and the largest Bitcoin wallets. A distinctive feature of these groups is that they carry out criminal fishing as a service in the interests of some criminal groups against other criminal groups. Thus, 2015-2016 became the first years of documented cyberwarfare between criminal gangs. At the same time, the criminal component of Bitcoin and cryptocurrencies in general is largely related to the ability of crypto criminals to profit from Bitcoin enthusiasts. According to Europol, starting in mid-2014, European organized crime

began to actively use the TOR-Bitcoin bundle. The bundle is used both for communication and for the deployment of criminal trade, as well as the recruitment of new members into criminal networks [12].

In this regard, in January 2017 Interpol, Europol and the Basel Institute of Management, in cooperation with the Qatar National Fund for Combating Money Laundering and the European Union Committee on Combating Illicit Financial Flows and the Financing of Terrorism, held the First Global Conference on Combating Money Laundering and Digital Currencies in Doha. The conference was attended by 400 participants from law enforcement agencies, international and transnational financial institutions, as well as businesses from 60 countries around the world. It was predicted that the annual total capitalization of the global cryptocurrency market could be approximately $ 50 billion. Nevertheless, despite the dizzying growth rates of capitalization, cryptocurrencies occupy an extremely small share in the total amount of funds.

Crime and the crypto community have different views on the main functions of cryptocurrencies. For the crypto community and investors, cryptocurrencies, primarily Bitcoin, are an asset and a means of speculation. Another cryptocurrency, Ethereum, is used by the crypto community not so much as a currency, but as a development environment for various blockchain–based financial applications. Organized crime is primarily interested in cryptocurrencies as a means of payment and cashing out. Despite the fact that, according to estimates by the Europol cryptocurrency research group, more than 95% of the turnover of cryptocurrencies used by criminals is accounted for by Bitcoin, criminals are trying to abandon this cryptocurrency. In 2016, its total annual turnover amounted to approximately 12 billion dollars. Of these, criminal turnover is estimated at about $ 3 billion, of which $ 0.6-0.9 billion is accounted for payments on the TOR network for various kinds of criminal goods and services. Criminals practically do not keep savings in Bitcoin, because they consider them highly volatile, where there is a high risk of not only earning, but also losing funds. High volatility suits investors and speculators, but criminals who are interested in a stable payment unit are not satisfied.

According to the Basel Institute of Management and the Bank for International Settlements, criminals have bet on a new, completely anonymous Dash currency. It provides not only complete privacy of transactions, but also anonymity of payment wallets guaranteed by several levels of encryption. In addition, Dash provides almost instant transactions that occur within 15-20 seconds, compared to 5-10 minutes for Bitcoin. Finally, Dash allows you to create various applications. The creators of this cryptocurrency have announced that on its basis it will be possible to conclude anonymous contracts with any purpose. Dash organizers position the currency as PayPal 2.0 for free people who despise the state. By the beginning of 2017, Dash's capitalization had reached half a billion dollars. Given that this currency was launched only in the middle of 2016, no cryptocurrency, including Ethereum and Bitcoin, has grown with such rapid capitalization. At the same time, restrictions on volatility are built into the Dash program code, which makes it an ideal means of payment and cashing out for criminals.

Along with Dash, criminals are actively using two more types of cryptocurrencies. In the USA, Mexico and Latin America, it is Monero. In European countries, including the post-Soviet space, the recently appeared ZCASH cryptocurrency is of great interest to criminals.

Although these cryptocurrencies appeared several years ago, practically none of the operational employees of the internal affairs agencies knows details about them and, accordingly, they have not encountered them in their daily work.

According to experts, Europol believes that so far, the concealment of criminal proceeds, their storage, as well as transactions are carried out within the framework of the usual financial system. The share of cryptocurrencies in total criminal payments and savings is still elusively small. However, according to the Interpol and Europol research groups, the growth rates of cryptocurrencies will be exponential in the next 5-6 years. Accordingly, law enforcement agencies and financial institutions have a small amount of time to develop and implement a set of legal, programmatic and other measures that prevent criminals from using cryptocurrencies.

As noted in the Europol report on organized crime "Crime in the Age of Technology" (February 2017), the most important direction for the development of organized criminal groups is to increase the effectiveness of laundering criminal proceeds and their transfer to the legitimate economy. Criminal networks and groups are constantly striving to use the latest technologies, such as cryptocurrencies and anonymous payment methods. The rapid processing of transactions and the proliferation of effective anonymization tools make it difficult for law enforcement agencies to evidence-based identification of the real beneficiaries of proceeds of crime [12].

It should be noted that due to the increasing growth in the development of information and telecommunication technologies, one of the most important tasks of legal science and practice is to improve the legal regulation of public relations in the field of information security [13, p.81]. A lot of work is being done in this direction in the Republic of Kazakhstan aimed at improving the legal framework. In this regard, on February 6, 2023, the Law "On Digital Assets" [14] became effective in the Republic of Kazakhstan, which was adopted in order to create a legal framework for the development of activities for the issuance and turnover of digital assets and digital mining, and legalized the use of cryptocurrency, which will directly contribute to the economic development and competitiveness of the Republic of Kazakhstan. In addition, the operation of this law will allow to develop new legislative mechanisms for the search and identification of signs of criminal acts in the field of high technologies and contribute to the creation of a legal framework for the development of the blockchain technology industry.

Conclusion

Summarizing a brief description of anonymous information networks as the main area of commission of particularly dangerous crimes in the field of high technology, it should be emphasized:

1. The increased public danger of anonymous networks is due to the difficulty of implementing law enforcement measures in them, since clear methods of such measures have not yet been developed in the internal affairs bodies of the Republic of Kazakhstan.

2. The volume of criminal content of anonymous networks is increasing many times due to the active use of "dual-use" technologies by criminal formations, such as blockchain and cryptocurrencies.

3. The results of the study show that the phenomenon of anonymous networks continues to develop dynamically further, as a result of which new and unexplored technologies appear that require adaptation to traditional police activities.

Against the background of these factors, insufficient legal regulation of the high-tech sector in Kazakhstan has a certain negative effect.

In conclusion, it should be noted that the study of the features of the use of cryptocurrencies in the commission of high-tech crimes is necessary to develop effective methods to counter these threats. The results of the analysis show that the introduction of international standards for the regulation of the circulation of cryptocurrencies, as well as the development of mechanisms for identifying participants in transactions, will contribute to the creation of a legal framework for the fight against crimes in the field of high technology. The experience of foreign countries, which have already faced similar problems and developed effective countermeasures, can serve as a basis for the development of national legislation and law enforcement practices in this area.

The contribution of the authors

Kan A.G. – critical revision of the content of the article, approval of the final version of the article for publication. **Korzhumbaeva T.M.** – the concept of the article, collection, analysis or interpretation of the results of the work, the design of the work. Abdullina S.H. – writing a text, collecting and analyzing empirical material.

References

1. Дебаты 70-й сессии Генассамблеи ООН [Электрон. ресурс]. – 2018. – URL: https://www.akorda.kz/ru/speeches/external_political_affairs/ext_speeches_and_addresses/vystuplenie-prezidenta-respubliki-kazahstan-nnazarbaeva-na-obshchih-debatah-70-i-sessii-genassamblei-oon (Дата обращения: 15.09.2023).

2. О создании правил использования криптовалют [Электрон. ресурс]. – 2018. - URL: https://tengrinews.kz/kazakhstan_news/nazarbaev-prizval-sozdat-pravila-ispolzovaniya-kriptovalyut-344425/ (Дата обращения: 15.09.2023).

3. О создании международной криптовалюты [Электрон. ресурс]. – 2017. – URL: https://tengrinews.kz/kazakhstan_news/nazarbaev-predlojil-sozdat-mejdunarodnuyu-kriptovalyutu-320433/ (Дата обращения: 15.09.2023).

4. Что такое блокчейн? Расскажем простыми словами [Электронный ресурс]. – 2017. - URL: https://coinspot.io/beginners/chto-takoe-blokchejn-rasskazhem-prostymi-slovami/ (Дата обращения: 17.09.2023).

5. Карта бита: история становления биткоина – первой анонимной интернет-валюты [Электрон. ресурс]. – 2015. - URL: https://lenta.ru/articles/2015/12/11/bitcoin/ (Дата обращения: 17.09.2023).

6. Баринов С.В. Особенности доказывания преступных нарушений неприкосновенности частной жизни, совершаемых в информационно-телекоммуникационной сети Интернет // Уголовно-процессуальные и криминалистические чтения на Алтае: Проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий. – Сб. науч. статей. – Вып. XV. – Барнаул, 2018. – С. 26-34. [Электрон. ресурс]. – 2018. - URL: http://kalinovsky-k.narod.ru/b1/XV_krimctenia_altai_2018.pdf (Дата обращения: 15.09.2023).

7. ФСБ обыскала Внуково из-за майнинга криптовалюты [Электрон. ресурс]. – 2017. - URL: https://tengrinews.kz/russia/fsb-obyiskala-vnukovo-iz-za-mayninga-kriptovalyutyi-333368/ (Дата обращения: 18.09.2023).

8. КНБ: Сотрудники Минфина майнили криптовалюты на государственных серверах [Электрон. ресурс]. – 2018. - URL: https://tengrinews.kz/crime/knb-sotrudniki-minfina-maynili-kriptovalyutyi-336735/ (Дата обращения: 18.09.2023).

9. Пользователи Казнета стали жертвами криптовалютной аферы [Электрон. ресурс]. – 2017. - URL: https://tengrinews.kz/internet/polzovateli-kazneta-stali-jertvami-kriptovalyutnoy-aferyi-330974/ (Дата обращения: 19.09.2023).

10. Крупнейшая биржа биткоинов Mt. Gox объявила о банкротстве [Электрон. ресурс]. – 2014. - URL: https://www.vedomosti.ru/finance/articles/2014/02/28/krupnejshaya-birzha-bitkoinov-mt-gox-obyavila-o-bankrotstve (Дата обращения: 19.09.2023).

11. Halyk Bank предостерег казахстанцев от инвестиций в «первую народную криптовалюту – Halykcoin» [Электрон. ресурс]. – 2017. - URL: https://tengrinews.kz/money/Halyk-Bank-predostereg-kazahstantsev-investitsiy-pervuyu-333749/ (Дата обращения: 15.09.2023).

12. Овчинский В. Финансовая «Матрица» [Электрон. ресурс]. – 2017. - URL: http://svop.ru/main/24182/ (Дата обращения: 15.09.2023).

13. Бисалиев М.С., Шакиров К.Н. Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет // Вестник Евразийского национального университета имени Л.Н. Гумилева. Серия право. – 2023. – Т.142. №1. – С. – 81-98. doi:https://doi.org/10.32523/2616-6844-2023-142-1-81-98.

14. Майнинг и криптовалюта: Токаев подписал закон о цифровых активах в Казахстане [Электрон. ресурс]. – 2023. - URL: https://ru.sputnik.kz/20230206/tokaev-podpisal-zakon-o-tsifrovykh-aktivakh-v-respublike-kazakhstan-31812025.html (Дата обращения: 15.09.2023).

А.Г. Кан[1], Т.М. Коржумбаева[2], С.Х.А бдуллина[3]

[1, 2, 3]Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы

Жоғары технологиялар саласында қылмыс жасау кезінде криптовалюталарды пайдалану ерекшеліктері

Аннотация. Бүгінгі күні құқық қорғау органдары үшін күрделі мәселе ұйымдасқан қылмыстық қауымдастықтар қылмыстарды дайындау және жасау үшін, сондай-ақ криптовалюталарды пайдалана отырып, оларды қауіпсіз қаржыландыру үшін белсенді түрде пайдаланатын интернеттің анонимді сегменттері деп аталатын қауіптер болып табылады. Зерттеу нәтижелері ғылыми және практикалық тұрғыдан бұл сала нашар зерттелгенін және жан-жақты зерттеуді қажет ететіндігін көрсетеді. Бұған дейін бізге осы қауіп-қатерлермен бетпе-бет келген және қазіргі уақытта жоғары технологиялар саласындағы қылмыстарға қарсы іс-қимылдың пәрменді әдістемелерін әзірлеп жатқан елдердің озық шетелдік тәжірибесі маңызды іргетас бола алады. Осы бағыттағы әртүрлі материалдарды талдау оларды ашу әдістемесінің элементтерін көрсетеді, олар тиісті жүйелеу кезінде қазақстандық жағдайларға бейімделуі мүмкін және құқық қорғау органдары тарапынан пәрменді қарсы іс-қимылға ықпал ететін болады.

Түйінді сөздер: интернет, анонимді желілер, криптовалюта, blockchain, сервер, шифрлау, майнинг, транзакция.

А.Г. Кан[1], Т.М. Коржумбаева[2], С.Х. Абдуллина[3]

[1,2,3]Алматинская академия МВД Республики Казахстан имени М. Есбулатова,

Особенности использования криптовалют при совершении преступлений в сфере высоких технологий

Аннотация. Сегодня серьезным вызовом для правоохранительной деятельности являются угрозы, которые таят в себе так называемые анонимные сегменты Интернета, которые активно используются организованными криминальными сообществами для подготовки и совершения преступлений, а также для их безопасного финансирования с применением криптовалют. Результаты исследования свидетельствуют о том, что в научном и практическом плане эта область изучена крайне слабо и нуждается во всестороннем исследовании. Весомым фундаментом для этого может стать передовой зарубежный опыт стран, которые раньше нас столкнулись с этими угрозами и в настоящее время вырабатывают действенные методики противодействия преступлениям в сфере высоких технологий. Анализ различных материалов в этом направлении показывает элементы методики их раскрытия, которые при соответствующей систематизации могут быть адаптированы к казахстанским условиям и будут способствовать действенному противодействию со стороны правоохранительных органов.

Ключевые слова: интернет, анонимные сети, криптовалюта, blockchain, сервер, шифрование, майнинг, транзакция.

Information about the authors:

Kan A.G. **–** correspondence author, Candidate of Law, Associate Professor (Associate Professor), Police Colonel, Head of the Faculty of Additional Education of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Utepova str., 29, 050057, Almaty, Kazakhstan

Korzhumbaeva T.M. **–** Candidate of Law, Associate Professor (Associate Professor), Police Colonel, Head of the Department of Administrative and Legal Disciplines of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Utepova str., 29, 050057, Almaty, Kazakhstan

Abdullina S.H. **–** PhD, Police Major, Associate Professor of the Department of Criminal Procedure and Criminalistics of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Utepova str., 29, 050057, Almaty, Kazakhstan

Кан А.Г. **–** автор для корреспонденции, кандидат юридических наук, ассоциированный профессор (доцент), полковник полиции, начальник факультета дополнительного образования Алматинской академии МВД Республики Казахстан имени М. Есбулатова, ул. Утепова, 29, 050057, Алматы, Казахстан

Коржумбаева Т.М. **–** кандидат юридических наук, ассоциированный профессор (доцент), полковник полиции, начальник кафедры административно-правовых дисциплин Алматинской академии МВД Республики Казахстан имени М. Есбулатова, ул. Утепова, 29, 050057, Алматы, Казахстан

Абдуллина С.Х. **–** доктор PhD, майор полиции, доцент кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан имени Макана Есбулатова, ул. Утепова, 29, 050057, Алматы, Казахстан

Кан А.Г. **–** хат-хабар үшін автор, заң ғылымдарының кандидаты, қауымдастырылған профессор (доцент), полиция полковнигі, Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы қосымша білім беру факультетінің бастығы, Өтепов көшесі, 29, 050057, Алматы, Қазақстан

Коржумбаева Т.М. **–** заң ғылымдарының кандидаты, қауымдастырылған профессор (доцент), полиция полковнигі, Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы әкімшілік-құқықтық пәндер кафедрасының бастығы, Өтепов көшесі, 29, 050057, Алматы, Қазақстан

Абдуллина С.Х. **–** философия докторы (PhD), полиция майоры, Қазақстан Республикасы ІІМ Мақан Есболатов атындағы Алматы академиясының қылмыстық іс жүргізу және криминалистика кафедрасының доценті, Өтепов көшесі, 29, 050057, Алматы, Қазақстан