Список використаних джерел:

1. Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений: учеб. пособие. Харьков : Юрид. ин-т, 1985. С. 22.
2. Криміналістика : підручник / [Шепітько В. Ю. та ін.] ; за ред. д-ра юрид. наук, проф., акад. Нац. акад. прав. наук України В. Ю. Шепітька ; Нац. юрид. ун-т ім. Ярослава Мудрого. – 5-те вид., перероб. та допов. – Київ : Ін Юре, 2016. 632 с.
3. Журавель В. А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом : наук.-практ. посіб. Харків : ТОВ «Одіссей», 2005. С. 28.
4. Фомина А. С. Расследование убийств, совершаемых по сексуальным мотивам // Расследование преступлений против личности : учеб. пособие / под ред. О. Я. Баева. Воронеж : Изд-во Воронеж. гос. ун-та, 1998. С. 95.
5. Кримінальний кодекс України [Електронний ресурс]: Закон України від 05.04.2001 № 2341-II // Верховна Рада України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n110

Ключові слова: вбивство з необережності, спосіб вчинення, досудове розслідування, типові сліди.

Key words: manslaughter, method of commission, pre-trial investigation, typical traces.

ДИНТУ ВАЛЕРІЯ АРКАДІЇВНА

Національний університет «Одеська юридична академія»,
доцент кафедри криміналістики, кандидат юридичних наук, доцент

THE IMPACT OF CRYPTOCURRENCIES TO THE TERRORIST FINANCING

Technological advances and transformative scientific achievements have changed the familiar way of life and, consequently, criminal behavior as part of human activity. The transition to the digital economy, in addition to positive improvements such as the high speed of transactions, unification of the global payment system, etc., has created new challenges that modern society has to face. More precisely, because of digitalization, the methods and ways of committing some crimes have changed.

In particular, digitalization has led to the improvement and development of traditional types of crime that have been known for a long time. Ordinary criminal activity has shifted to the online space, which has made it more productive and efficient thereby modernizing its characteristics such as speed, anonymity, limitlessness, etc. For example, the Internet and Darknet are used as a platform for the illegal sale of drugs (Silk Road, Evolution, Agora, etc.), and digital payment systems are used for money laundering (Liberty Reserve case, etc.). In addition, crypto-currency is used for pump-and-dump schemes that used to apply to stocks. In the schemes mentioned in

recent years, scammers use susceptible cryptocurrency markets to create artificial attention and demand based on far-fetched information and encourage unwitting investors to buy the currency. What's more, offenders can issue a new token and spread positive news about its use, as they did with SaveTheKids in 2021. Additionally, digitalization has led to the emergence of a new type of crime that did not exist before the invention of the computer and the Internet, namely cybercrime. Technically, the realization of these crimes is impossible without special digital electronic devices. For example, malicious software (malware), hacker attacks, ransomware attacks, etc. It is noteworthy that despite its recent appearance, the development of cybercrime has reached impressive scale. According to a new report by the Center for Strategic and International Studies (CSIS) and McAfee, cybercrime now costs the world nearly $600 billion, or 0.8 percent of global GDP (Economics of Cybercrime, 2017). In 2017, for example, one of the most devastating cyber attacks occurred with the NotPetya malware, which caused an estimated $10 billion in damage. It should be noted that the development of cybercrime is in step with the times and responsive to change. For example, in 2020, the CovidLock malware became widespread due to the COVID-19 pandemic. It was claimed to give users access to statistical information about COVID-19.

However, it was infected with ransomware. CovidLock had a screen lock feature that denied the victim access to their phones. The main purpose of ransomware is to extort money, which in this case was done in Bitcoin. CovidLock demanded $100 in Bitcoin in 48 hours. Otherwise, there was a threat of public leakage of personal data and erasure of phone memory. Thus, digitalization has created an environment that has fostered the development of existing crimes and the creation of new crimes that have a huge impact on the growth of crime. This process is constantly in flux.

It is worth emphasizing that terrorists are always among the first users of new technologies that can increase the profitability of their efforts and push them to achieve their malevolent goals. According to the Global Terrorism Index 2020 report, the global economic impact of terrorism in 2019 was $26.4 billion [1].

It should come as no surprise that terrorists have adapted the function of the digital economy with all its advantages. Initially, terrorist organizations used fiat currency to transfer funds and raise money, the use of which caused many problems (money laundering controls, bank policies, etc.). Nowadays, despite its relatively short existence, terrorists have significantly increased their attention to cryptocurrency, particularly Bitcoin.

Bitcoin is a decentralized digital currency for storing and validating transaction data based on a peer-to-peer (P2P) distributed network [2]. Data is stored in a public ledger, the basis of which architecture is blockchain. Blockchain organizes its data into blocks that are connected in a chain. Each block contains a hash of the previous block and a Merkle tree of transactions. Any changes in the transaction information cause the Merkle root hash and, consequently, the hash of a particular block to change.

For a better understanding of the nature of Bitcoin, it is worth considering the Elliptic Curve Digital Signature Algorithm (ECDSA) as an essential part of it. ECDSA is the elliptic curve analog of the Digital Signature Algorithm (DSA). DSA can be considered as a variant of the ElGamal signature scheme. The possibility of using the discrete logarithm problem in public key cryptosystems was recognized in 1976, when Diffie & Hellman [3] introduced public key cryptography. Koblitz [4] and Miller [5] independently introduced Elliptic-curve cryptography. Scott Vanstone proposed the ECDSA in 1992 in response to a request from the National Institute of Standards and Technology for public comment on their Digital Signature Standard (DSS) proposal. It can be seen as an effective variant of ElGamal's [6] digital signature scheme. It was adopted: in 1998 as an International Standards Organization standard (ISO 14888-3); in 1999 as an American National Standards Institute I standard (ANSI X9.62); in 2000 as an Institute of Electrical and Electronics Engineers standard (IEEE 1363-2000) and Federal Information Processing Standard (FIPS 186-3).

In continuation of the above, any user can create a fake address that includes the corresponding public/private key pairs stored in the user's wallet. The problem of forgery can be solved by signing the created transaction with the user's private key. The information about the transaction must then be sent out to the P2P network nodes. The payer's public key can be used to verify the correctness of the corresponding private key, which was used to sign the transaction. Accordingly, the characteristics of Bitcoin, such as decentralization, transparency, and irreversibility, increase its reliability. Since the use of blockchain eliminates the need for a central authority, each user can have access to any public address, transaction, and furthermore, transaction history cannot be changed.

Digitalization has changed all areas of human activity, including criminal ones. This contributed to the improvement of conventional crimes, the development and creation of new types, which, accordingly, could not be created without special digital electronic devices. The gradual increase in the number of cybercrimes demonstrates the applicability of new technologies in criminal activity. The main characteristics that attract criminals to cybercrime are the high speed of action, accessibility, limitlessness, uncertain jurisdiction of states, and difficulty for legal investigation.

It is worth emphasizing that one of the clear results of digitalization is the creation of cryptocurrency. Bitcoin and other cryptocurrencies have changed not only the financial system, but also the ways and means of criminal activity. The global nature of blockchain has pushed crime beyond national borders. Peer-to-peer networks, mixers and other means of increasing anonymity have made it possible to hide financial transactions. Digital infrastructure has created a favorable environment for money laundering, other financial crimes, and international funding of terrorist organizations.

Terrorist organizations are now using an integrated approach, combining social media, messengers and cryptocurrencies for international fundraising. The terrorist organization attracts many donors around the world by posting detailed instructions on the cryptocurrency transaction process on social

networks and messenger channels, following which potential donors can discreetly invest in terrorist ideology.

Thus, in this context, law enforcement agencies must continually raise their awareness of rapidly evolving cryptocurrencies and the ways in which they can be abused in order to counter their threats.

References:

1. Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney, November 2020 (2020). The official website of Institute for Economics & Peace. Available at: https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf (accessed 05 June 2022).
2. Nakamoto S. (2009). Bitcoin: A peer-to-peer electronic cash system (2009). Bitcoin.org. Available at: https://bitcoin.org/bitcoin.pdf (accessed 05 June 2022).
3. Diffie W., & Hellman M. (1976). New directions in cryptography. IEEE transactions on Information Theory, vol. 22, no. 6, pp. 644–654.
4. Koblitz N. (1987). Elliptic curve cryptosystems. Mathematics of computation, vol. 48, no. 177, pp. 203–209.
5. Miller V. S. (1986). Use of Elliptic Curves in Cryptography. In: Williams H. C. (eds) Advances in Cryptology – CRYPTO'85 Proceedings. CRYPTO 1985, pp. 417–426. Lecture Notes in Computer Science, vol. 218. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/3-540-39799-X_31
6. Elgamal T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472. CiteSeer^{x} Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.476.4791&rep=rep1&type=pdf (accessed 08 December 2021).

Ключові слова: криптовалюта, Біткойн, фінансування тероризму, кримінальне розслідування, де-анонімізація.

Key words: cryptocurrency, Bitcoin, terrorism-financing, criminal investigation, de-anonymization.

АВДЄЄВА ГАЛИНА КОСТЯНТИНІВНА

Науково-дослідний інститут вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, провідний науковий співробітник, кандидат юридичних наук, старший науковий співробітник

ПРОБЛЕМИ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ В УМОВАХ ВОЄННОГО СТАНУ

Військові РФ вчинили в Україні безліч злочинів, серед яких – масові вбивства мирних громадян, знищення житлових і інфраструктурних об'єктів, мародерство, ґвалтування та ін. Через це порушені права громадян України, які закріплені у Розділі І Європейської Конвенції про