Kozlovska A., Kirilieva A. New challenges for financial security in Ukraine: Using cryptocurrency in criminal income legislation/A. Kozlovska, A. Kirilieva//Проблеми та перспективи розвитку фінансово-кредитної системи України: збірник матеріалів IV Всеукраїнської науково-практичної on-line конференції: у 2 ч. (м. Суми, 21-22 листопада 2019 року) / Навчально-науковий інститут бізнес-технологій «УАБС» Сумського державного університету. – Суми : Сумський державний університет, 2019. – Ч. 1. – С.130-133

Kozlovska Anna
Candidate of Philological Sciences, Associate Professor
Sumy State University, Sumy
Кіріл'єва Анастасія Віталіївна,
Студентка,
Сумський державний університет, м. Суми

NEW CHALLENGES FOR FINANCIAL SECURITY IN UKRAINE: USING CRYPTOCURRENCY IN CRIMINAL INCOME LEGALIZATION

In Ukraine, as well as in other regions of the world, sectors of economic activity, used in manufacturing, computer technology and the Internet are constantly expanding. That can be proved by the results of international organizations' survey which show that Ukraine entered the top ten of the European states on the number Internet users. The Indicator for Ukraine is 22 million people, who have access to the World Wide Web (59% of the total number of users).

Today, cybercrime is one of the most dynamic groups of socially dangerous attacks. This is caused by the quick development of science and technology in computerization, on the one hand, and by the constant increasing of computer equipment use, on the other hand. In the period of 2009-2018, 8438 cybercrimes were registered but the number of such kind of crimes is steadily increasing because of the open access to the World Net in various fields of activity and the number of the Internet users which is greater than before.

On-line services and electronic wallets are the most vulnerable in the bank sector and the most attractive for cyber criminals. That's why the incidents of stealing money from the clients' bank accounts are not decreasing. Here is the list of actions used by cybercriminals:

• using accounts opened for lost or forged documents;

• opening an account, including cards for low-income citizens and shell enterprises;

• using international payment systems (electronic payments);

• the chain of financial flows through several bank accounts with the help of remote access;

• electronic funds and cryptocurrencies;

• using figureheads.

It is necessary to pay attention to such ‘instrument’ of cybercriminals as cryptocurrency. Since the last year cryptocurrency has gained the interest not only of people but of the whole countries that have begun to use such kind of money in their everyday life. Cryptocurrency transfer is carried out with the help of block chain technology when each transaction must be approved by five different clients of the system who are financially rewarded for that. One can trace all transactions from one wallet to another one through the block chain, i.e. we can speak about the high level of cryptocurrency anonymity.

The block chain technology also provides the real decentralization of data saving because the transaction base is divided among all the units of the system. Thus, we can say about providing protection of information against external influences and force majeure.

Taking into account all the facts mentioned above we can say that cryptocurrency has the following main peculiarities:

- limitation use which prevents from cryptocurrency inflation;
- data protection from the external influences and attacks as one should destroy more than twelve units in order to damage the cryptocurrency system;
- users’ anonymity;
- transactions transparency, the information is accessible from any unit of the system;
- absence of commissions for transactions among the countries;

- absence of transaction control from banks, tax authorities or other supervisory authorities.

Cryptocurrency has taken its place in modern financial system because of its advantages mentioned above and such reasons as lack of trust to the current financial market, instability of exchange rates and financial assets.

Nowadays total capitalization of the local market is estimated at between $ 160 million and $ 177 million. According to Roni Moas, the founder of Pointpoit Research, and some other analysts it will have risen up to $ 2 trillion for the next 10 years. The world daily turnover in the top cryptography rounds will be $ 4 billion. What is behind this growing market?

Cryptography experts explain that the main difference from the ordinary national currency for cryptocurrency is decentralization and lack of state control. In particular, the emergence of this independent center with no digital payments management shows how public confidence to the state and the financial system worldwide is diminishing every year. However, this does not mean that the state should not regulate this turnover, since lack of cryptography control opens up great opportunities for frauds, management of shadow business, financing military conflicts, etc. That is why some countries try to regard them as the objects of civil law relations, the other ones try to forbid them. Bolivia and Ecuador decided on direct bans while most EU countries, Great Britain, Switzerland, the US federal government, Canada, Japan and Southeast Asian countries took the policy of observation with cautious optimism. In most developed countries, financial law has been adapting to the problem of cryptographic regulation, so this problem will soon be resolved in one way or another.

Ukraine is in the TOP-10 countries on the number of Bitcoin users. The Kuna Bitcoin agency, being the largest one in CIS, carries out its activity in Ukraine and has the Cryptocurrency Exchange. The use of decentralized technologies is being planned and has been partially implemented at the state level: e-Auction 3.0, e-Vox, E-Ukraine. There is also a very developed cryptocurrency society in Ukraine. In

December 2016, the Ukrainian Stock Exchange became the world's first trading venue for Bitcoin derivatives.

Frauds offset many of the benefits of digital assets. They use viruses and phishing sites that fake wallet addresses and completely copy the interface of the exchange or any other cryptocurrency site. Careless users regularly fall victim to fraudsters and get rid of their assets.

Список використаних джерел

1. Офіційний сайт Кіберполіції України. URL: https://cyberpolice.gov.ua/results/2018/
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. URL: bitcoin.org.https://bitcoin.org/bitcoin.pdf.
3. Dr. Robby Houben, Alexander Snyers. Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion. *Policy Department for Economic, Scientific and Quality of Life Policies*, 2018. URL: http://www.europarl.europa.eu/cmsdata
4. Josias Dewey. Blockchain & Cryptocurrency Regulation, 2019 URL: https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf