PROBLEM OF PROTECTION AGAINST CYBER CRIMES IN THE FIELD OF CRYPTOCURRENCY CIRCULATION

Kateryna Chyzhmar, Institute of Law and Postgraduate Education of the Ministry of Justice of Ukraine
Oleksandr Yunin, Dnipropetrovsk State University of Internal Affairs
Iryna Paterylo, Oles Honchar Dnipro National University
Ihor Alieksieienko, Oles Honchar Dnipro National University
Serhii Shevchenko, Dnipropetrovsk State University of Internal Affairs

ABSTRACT

In the course of the study, cases of interaction of a cryptocurrency system with external subjects were identified. Such connections are manifested mainly in the protection of rights of participants in the cryptocurrency market in the event of an offense, respectively, the issue of punishment of offenders, taxation issues, as well as the performance of the cryptocurrency as a medium of circulation outside the cryptocurrency market. Due to the misregulating of the algorithm of such relationships at the legislative level, many violations of the rights and interests of both the participants of the cryptocurrency market and these very external actors arise. The way to resolve problematic issues is to develop a legislative framework. First, since each state at the national level regulates the process of cryptocurrency circulation in its own way, and the cryptocurrency market covers the whole world, it becomes necessary to establish common rules, as well as to develop a conceptual and categorical apparatus at the international level. Such an act can even be documented as a legal custom, such as Incotermsю After determining the main points regarding the circulation of cryptocurrency in the world at the international level, each state will be able to develop norms at the level of national legislation on some basis. Today it is very important to realize that the emergence of a cryptocurrency (digital money) is a globalization phenomenon. Cryptocurrency is a class of financial assets that is developing and gains popularity more quickly than others and is both a prospect and a threat to the entire global financial system. Therefore, it is necessary to take control of this phenomenon in advance in order to be ready for its appearance in the financial markets.

Keywords: Cryptocurrency, Fiduciary Digital Currency, Phishing, Clickjacking, Payment Portal.

INTRODUCTION

The 21st century is the age of information technology. Globalization, the dynamic growth of the Internet market, the development of information technologies-all these processes contribute to the emergence of new institutions, financial instruments and new forms of interaction in society.

Today, the Internet is an integral part of modern daily life. Many products, also services can be purchased through online services. It is very convenient and saves a lot of time for both consumers and sellers, many of whom use electronic wallets to make the appropriate payment.

In addition, over the past 10 years, the system of circulation of monetary units in the world has been showing its instability. Some economic and regional communities think about creating their own currency. Today, many international associations plan to issue their single currency. For example, the Customs Union of Kazakhstan, Russia, Belarus, the countries of South Asia, and the countries of the Bolivarian Alliance in 2010 for the first time used a collective currency - sucre.

The pegging of the domestic market of states to world currency has become unfavorable for some countries, and therefore certain groups of countries are working to create their own monetary system. In addition, these circumstances contribute not only to the creation of new monetary systems, but also new currency forms.

Today, one of these new currency forms is cryptocurrency. The facts evidencing the popularity and convenience of the new settlement system speak for themselves, and the cryptocurrency generation system may arise as an alternative to the world monetary system on the principles and forms of money circulation.

Today, cryptocurrency is a new evolutionary stage in the development of the market for currency circulation. The concept of electronic money with its independent from anyone emission and decentralized system of activity is gaining popularity every day.

REVIEW OF PREVIOUS STUDIES

The concept of "*cryptocurrency*" was first given publicity in 2009, when the first bitcoin appeared (Boes & Leukfeldt, 2017). At that time, bitcoin cost only ten cents, today-more than six and a half thousand dollars.

Over time, along with bitcoin, we can see many other types of cryptocurrency (more than 400 types). In addition, there are a large number of cryptocurrency exchanges that are constantly growing (as of the end of 2018 there are more than 500) (Boister, 2018). Therefore, we can confidently say that cryptocurrency is the beginning of a new history in the use of the monetary system by mankind, this is a new stage of its existence on high-tech basis.

However, unfortunately, today in the world there is no single, clear approach to the definition of the term "*cryptocurrency*" either from an economic or a legal point of view, which causes the existence of major problems in the legal regulation of cryptocurrency circulation (Miquelon-Weismann, 2017). Therefore, it is conceptually important to define what the term "cryptocurrency" means.

Among the significant number of definitions of this concept, we can single out the most successful from a legal point of view, for example the following:

1. Cryptocurrency is a medium of exchange, like ordinary currencies, but aimed to exchange digital information, made possible by certain principles of cryptography (used to secure operations and control the creation of new coins) (Hilorme et al., 2019).
2. Cryptocurrency is a type of digital money that uses distributed networks and publicly available transaction logs, and the key ideas of cryptography are combined with the monetary system to create a safe, anonymous and potentially stable virtual currency (Drobyazko et al., 2019).

3. Cryptocurrency is a type of digital currency based on complex calculations of a certain function that can be easily verified by reverse mathematical operations, on the basis of the issue of which is the principle of the "*Proof-of-work*" (Ivanus & Iovan, 2017).
4. Cryptocurrency is a fiduciary digital currency which exchange rate is set on the basis of a freely floating regime as a result of supply and demand on the foreign exchange market with complete lack of control by central banks (Jhaveri et al., 2017).

METHODOLOGY

The methodological basis of the study is a set of methods and techniques of scientific knowledge, the use of which is due to the peculiarities of the legal regulation of the cryptocurrency circulation process in the world. In the process of the study, the following general scientific methods were used: the system and structural method. This method was used in the study of the practice of legal regulation of the process of cryptocurrency circulation by foreign countries: analysis of legal acts, business practices, etc. This made it possible to form an idea of the state of legal regulation of cryptocurrency activities in the world, to determine the main approaches to such regulation.

Synthesis Method

This method was used in formulating the definition of the concept of "*cryptocurrency*", namely, on the basis of a study of the characteristics of a cryptocurrency, a corresponding definition was formed containing all the studied characteristics,

Abstraction Method

This method was used in the study of relations with third parties which are not participants in the cryptocurrency market in the process of cryptocurrency circulation.

Also, in the process of the study I applied such special methods as system and functional, comparative and legal, formally dogmatic, classification method, method of documentary analysis, logical and semantic and logical and legal methods.

RESULTS AND DISCUSSIONS

The system of protection of rights of participants in cryptocurrency relations as such is absent. Today, in no country there is a legal act that would accurately define the rights and obligations of participants in cryptocurrency relations, there is not even a accurate definition of cryptocurrency at the legislative level. Trying to protect their interests, the persons subjected to their violation have nothing to rely on. Similarly, the judiciary does not have the opportunity to make the only correct decision, since there are no substantive law, on the basis of which it would be possible to resolve the dispute.

Cryptocurrency legal relations are close to civil, economic and legal relations, respectively, the protection of the rights of participants in these relations shall provide for various ways.

Participants in cryptocurrency relations are assigned with certain rights and certain responsibilities. Along with this, there are often cases when such rights are violated. In recent times, cybercrime activities has become quite common in this area.

With the appearance of cryptocurrencies, cybercriminals have new motives for their activities on the Internet.

Moreover, the growth of the types and number of cryptocurrencies has led to the creation of new types of criminal activity. Examples of cybercrimes in the field of cryptocurrency activities are:

Clickjacking

It is a criminal offense when a special code is entered on a website on the Internet with which you can generate a cryptocurrency using the power of the central processor of site visitors.

Hacking of Payment Portal

Even a real payment portal today can cause a loss of a cryptocurrency. The first such crime was committed in 2014. A well-known case is the case of July 2017, when from the Ethereum Classic, one of the most popular cryptocurrency web wallets, which was located at the address https://classicetherwallet.com/, suddenly cryptocurrency began to be stolen from users' electronic wallets. The hackers used social engineering methods and assured the hosting provider that they really were the owners of the domain (web pages, simply put). Having thus gained access to the domain, they began to intervene in the financial transactions that took place there. However, since the theft of a cryptocurrency started immediately and in fairly large amounts, this criminal activity was quickly discovered. At that time, there were stolen cryptocurrencies at the total amount of three hundred million US dollars. If the hackers had paused and had been stealing the cryptocurrency more slowly and in smaller amounts, the losses would be much greater.

The largest amount that was stolen in this way was five hundred million US dollars. Change of payment details. In fact, this is a banal theft. The principle of committing this crime is that when transferring a cryptocurrency from one wallet to another, a virus is launched that replaces the address of the wallet to which the transfer is made. Not every market participant re-verifies the correctness of the copied e-wallet address. Thus, the cryptocurrency gets to the wrong electronic wallet, but it’s impossible to identify the owner.

Phishing

The concept of this crime is that the participant of the cryptocurrency market is “*sucked*” to a fake website, where he uploads his e-wallet himself and enters his password. Thus, these data fall into the hands of criminals who carry out further theft of the cryptocurrency available on the electronic wallet.

More than half of all crimes committed in the field of cryptocurrency occur in the United States. Russia and China are in the top three after the United States.

The number of cybercrimes in Russia increased in the first quarter of 2018 by 32%. At the same time, the share of attacks aimed at infecting computers with a hidden mining cryptocurrency virus has also increased-23% of malicious software exploit the power of a PC to mine a cryptocurrency.

Today, cybercriminals in this area have stolen about 1.2 billion US dollars. Due to the widespread of such cases, more severe safety standards are being established worldwide.

The European Commission intends to introduce new penalties for cybercrimes related to the cryptocurrency. The executive body of the European Union expressed its intention to submit a new directive aimed at preventing crimes on the Internet. The plan includes the establishment of a European Cybersecurity Agency, which in the future will assume the role of the governing body in regulating this issue.

According to the EU's proposed plan, penalties for cybercrimes will be tightened. Today, the EU reports that the existing provisions of the current regulations on cybercrime activities do not apply to crimes in the field of cryptocurrency activities:

> *"The existing rules, according to which the activities in the field of non-cash payments can be recognized as illegal, have been established by the Council Framework Decision 2001/413/JHA of 2001. It became obvious that these rules no longer correspond to reality and do not allow to adequately confront new challenges related to virtual currencies and mobile payments".*

RECOMMENDATIONS

The important aspects that are recommended to be settled at the international level are: preparation of a basic single conceptual and categorical apparatus; creation of supreme state bodies to protect the rights of participants in cryptocurrency relations; creation of bodies that at the international level will coordinate cryptocurrency relations (setting rules and standards, quality control, setting permissions and bans); development of international legal acts regulating the cryptocurrency circulation process.

CONCLUSIONS

One of the main problems is the problem of security. At the moment, there is an acute issue about the safety of using blockchain technology. It provides a high level of protection on the network, making transactions anonymous, but it also creates risks for the use of cryptocurrency for criminal purposes.

In addition, the technologies underlying the functioning of a cryptocurrency, like any other information systems, are subject to various types of vulnerabilities.

Weak point in the chain of cryptocurrency circulation is a link where cryptocurrency is exchanged for traditional money. Since this happens on the newly unregulated exchanges, they often become the object of hacker attacks.

There are other traps in the cryptocurrency market. For example, due to the rapid emergence of new cryptocurrency exchanges, it becomes difficult to determine their historical performance and just hope for their reliability. There are "*gray*" stock exchanges, which at any time may suspend their activities, having previously withdrawn assets.

For many governments, the most important security issue is the use of a cryptocurrency to launder money or finance terrorism. The Japanese government, ministers of finance and heads of central banks of France and Germany propose to make cryptocurrency regulation international to prevent money laundering using virtual currencies.

The IMF also takes the view that international legislative regulation of the digital currency market is necessary.

Also, the problem is the protection of the rights and interests of participants in the cryptocurrency market. Today it is quite difficult to do this, because the system of such protection does not exist. Courts quite ambiguously resolve disputes in this area, since they have

nothing to rely on. And the protection of rights in this area, as in any other, is a very important aspect that guarantees its reliability.

All these problems described above arise from the fact that neither in the international market nor within countries, their solutions are not provided. Moreover, not only their decisions are not provided for, but even conceptual aspects, that is, the rules for their functioning, the conceptual and categorical apparatus.

REFERENCES

Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. In *Cyber-Physical Security* (pp. 185-203). Springer, Cham.

Boister, N. (2018). *An introduction to transnational criminal law.* Oxford University Press.

Drobyazko, S., Hryhoruk, I., Pavlova, H., Volchanska, L., & Sergiychuk, S. (2019). Entrepreneurship innovation model for telecommunications enterprises. *Journal of Entrepreneurship* Education, *22*(2), 1-6.

Hilorme, T., Perevozova, I., Shpak, L., Mokhnenko, A., & Korovchuk, Y. (2019). Human capital cost accounting in the company management system. *Academy of Accounting and Financial Studies Journal, 23*(SI2), 1-8.

Hilorme, T., Shurpenkova, R., Kundrya-Vysotska, O., Sarakhman, O., & Lyzunova, O. (2019). Model of energy saving forecasting in entrepreneurship. *Journal of Entrepreneurship Education, 22*(SI1), 1-7.

Hilorme, T., Zamazii, O., Judina, O., Korolenko, R., & Melnikova, Y. (2019). Formation of risk mitigating strategies for the implementation of projects of energy saving technologies. *Academy of Strategic Management Journal, 18*(3), 1-6.

Ivanus, C., & Iovan, S. (2017). Cybercrime in the European Union. Annals of Constantine Brancusi University of Targu-Jiu. *Social Sciences Series, 22*(3), 187-192.

Jhaveri, M.H., Cetin, O., Gañán, C., Moore, T., & Eeten, M.V. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys (CSUR),* 49(4), 68-89.

Miquelon-Weismann, M.F. (2017). The convention on cybercrime: a harmonized implementation of international penal law: what prospects for procedural due process?. In *Computer Crime* (pp. 171-204). Routledge.