European Journal of Sustainable Development (2021), **10**, 4, 304-316 ISSN: 2239-5938
Doi: 10.14207/ejsd.2021.v10n4p304

Criminal Liability for Cryptocurrency Transactions: Global Experience

By Volodymyr Cherniei[1], Serhii Cherniavskyi[2], Viktoria Babanina[3], Olena Tykhonova[4]

Abstract
The article examines the features of criminal liability for transactions related to the circulation of cryptocurrencies. In order to determine the specifics of criminal violations in the field of cryptocurrency circulation, the legal nature of cryptocurrencies is studied. It is concluded that in order to properly qualify criminal offenses related to the circulation of cryptocurrencies, it is advisable to recognize cryptocurrencies as a type of property or money. The article analyzes the global approaches to the legal regulation of relations related to the circulation of cryptocurrencies. Based on the results of this analysis, it is concluded that relations regarding cryptocurrencies in most countries of the world are insufficiently regulated and are still outside of the legal field. This complicates, inter alia, the establishment of criminal liability for transactions involving the circulation of cryptocurrencies. A significant part of the article is devoted directly to the study of criminal liability for transactions involving the circulation of cryptocurrencies in different countries. The norms of the Criminal Codes, which establish liability for criminal violations in the field of cryptocurrency circulation, are analyzed. The measures that need to be implemented to ensure the control of government agencies over the circulation of cryptocurrencies and the security of all operations related to cryptocurrencies are identified.

Keywords: cryptocurrency, criminal offences, transactions, liability, digital asset, security.

1. Introduction

Today, human relations are increasingly moving to the virtual sphere, information technology relations are developing more and more intensively, which is accompanied by the emergence of new phenomena and require the appropriate regulation.
An important feature of modern global processes is the development of the global information society. In this universal process of development of the information society, the question of formation of the international legal bases of regulation of the relations connected with emergence of such phenomenon as cryptocurrency, as well as research of a modern condition and prospects of development of such regulation remain unresolved. Technological innovations in the modern world are associated with the development of distributed registry technology - Blockchain and the emergence of new methods of digital payments, which often use cryptocurrencies. Transactions carried out in the financial sector using cryptocurrency, i.e. various peer-to-peer payment systems that use a certain

[1]Rector of National Academy of Internal Affairs, Doctor of Law, Professor, Kyiv, Ukraine.
[2]Vice-Rector of National Academy of Internal Affairs, Doctor of Law, Professor, Kyiv, Ukraine.
[3]Professor of Criminal Law Department of the National Academy of Internal Affairs, Doctor of Law, Associate Professor, Kyiv, Ukraine.
[4]Professor of Economic Security and Financial Investigations Department of the National Academy of Internal Affairs, Doctor of Law, Professor, Kyiv, Ukraine.

unit of account of the same name and the same protocol of data transmission, are becoming increasingly common in the modern world (Skrypnyk, 2018).

Blockchain technology is widely used worldwide. For example, in the capital of South Korea, Seoul, a "smart city" system has been introduced on Blockchain, so called Blockchain Urban Plan, which includes an archive of vehicle operation, issuance and registration of various permits, as well as a voting system. In Ukraine, this technology is used in the information system of the state land cadastre and the system of electronic trading in seized property "SETAM". Similar Blockchain-based systems operate in India, Sweden, the UAE and other countries. The new technology provides users with security benefits due to the technological principles on which it is based, however, the circulation of cryptocurrencies poses various threats to their participants and society and the state as a whole.

With the increase in the capitalization of cryptocurrencies in recent years, the issue of using Blockchain and cryptocurrencies has ceased to be purely technological, and has become important for the financial system of the world and individual countries. The cryptocurrency market is in the process of formation and development, but the total number of varieties of cryptocurrencies is more than 2000. Although the first of them - Bitcoin - was released in early 2009, the legal status of cryptocurrencies in most countries is not defined. The activity of cryptocurrency exchanges, mining, conversion into fiat money and other financial transactions are mostly not regulated at the state level. At present, these transactions cannot be controlled or tracked, and they are carried out exclusively between two entities without the participation of financial institutions.

The state must clearly define the scope of rights and responsibilities of individuals and legal entities operating in the cryptocurrency market. This will help to improve the existing infrastructure and its integration at the international level. The need to determine the legal status of cryptocurrencies is due not only to the issues of property rights and taxation, but also to counteracting illegal transactions related to the circulation of cryptocurrencies, the number of which is growing daily.

2. The legal nature of cryptocurrency and its delimitation with related categories

Cryptocurrency is a completely new economic and legal phenomenon, different from traditional electronic money. Its main features are: 1) the functioning of the cryptocurrency system is due to its program code; 2) exists in the form of digital code, which is generated according to complex mathematical algorithms; 3) anonymity of operations; 4) accounting for transactions with cryptocurrencies is carried out using Blockchain technology; 5) performs the functions of fiat money; 6) lack of real security (Kaznacheeva & Dorosh, 2020).

Cryptocurrency is based on Blockchain technology. This technology is used by large banks and individual government agencies to simplify the processing of information in transactions.

Cryptocurrencies are represented by transactions recorded in a Blockchain that can be viewed by any user. At the same time, this means that a transaction based on this technology does not depend on government agencies and the official monetary system,

and that the financial transactions of each Blockchain user can be accessed by any Internet user.

Blockchain fundamentally changes the perception of financial transactions, money and business. The authors of the study of Blockchain technology A. Tapscott and D. Tapscott (2017) argue that this system, based on boundless trust, will change the future, affecting all social institutions. As for the Blockchain-based business, there is an assumption that it will be as comfortable and transparent as possible. Blockchain is the trust and security of business, where not only the state can track transactions, but the average citizen as well.

As for the cryptocurrency, the Blockchain means new opportunities for settlements outside the traditional financial system. It is noteworthy that immediately after the creation of cryptocurrency in the first wave of its popularity, users and ideologists (cryptoanarchists) inclined to the philosophical component of cryptocurrency: they justified the meaning of cryptocurrency by the possibility of liberation from state power and traditional financial system. Unlike many other investors, cryptoanarchists did not focus on financial opportunities, but on the socio-political functions of cryptocurrency.

The prototype of the mechanism for creating the cryptocurrency itself was invented in 1997 by Adam Back. He suggested using the Hashcash spam protection system, in which the sender makes many time-consuming transactions, and the recipient very quickly verifies their authenticity (Lukyanov, 2014). Summarizing the various definitions, we can position cryptocurrency as a universal global means of payment, circulation and investment, which exists in the form of software code with a high degree of security and is characterized by a free market rate.

Cryptocurrency systems seek to ensure compliance with several principles: consensus, security and uniqueness, proper verification of transactions. The basis of their implementation in practice is the process of "extraction". The people who provide it carry out expensive computing operations on a competitive basis: the winner has the right to create a new history on the network by updating the "blockchain". In the simplest terms, this term covers the totality of all past transactions, or rather - identification credentials about them. The definition of "block" means current transactions based on supply and demand for cryptocurrency. The set of such "blocks" forms the history of the "blockchain". That is, it is obvious that under such conditions, a return to the previous transaction is almost impossible (Kuznetsov & Yakubov, 2016).

Among the significant number of definitions of this concept, we can highlight the most successful from a legal point of view, such as the following:

1) cryptocurrency is a means of exchange, like ordinary currencies, but designed to exchange digital information, which became possible due to certain principles of cryptography (used to ensure operations and control the creation of new coins) (Nekit, 2018).

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 in them with the monetary system to create a secure, anonymous and potentially stable virtual currency (Shapoval, 2017).

3) cryptocurrency is a type of digital currency based on complex calculations of some function, which is easy to verify by inverse mathematical operations, based on the issue of which is the principle of "Proof-of-work" (Belomyttseva, 2014).

4) cryptocurrency is a fiduciary digital currency, the exchange rate of which is set on the basis of a free-floating regime as a result of demand and supply in the foreign exchange market with a complete lack of control by central banks (Cvetkova, 2018).

Technical, technological and organizational aspects of the use of cryptocurrencies indicate that they are almost identical to the electronic type of non-cash money of their circulation. However, it is wrong to completely identify cryptocurrency with non-cash money in general, and their individual type of electronic money. The similarity is that cryptocurrencies as electronic money are an impersonal payment instrument (i.e. do not require identification of the owner) and circulate outside the banking system in electronic form. If e-money issuers have to work closely with banks to ensure the free exchange of e-money for traditional and vice versa, then cryptocurrencies are not "bank funds", they are not taken into account when calculating monetary aggregates and can not be used for banking services (deposit and issuance) loans) (Petruk, 2017).

The main differences between cryptocurrency and electronic money are as follows:

- access to cryptocurrency is limited only to access to the Internet, while access to electronic money is associated with access to mobile devices and the agency network;
- most countries do not yet have legal regulation of cryptocurrency circulation, electronic money is regulated by an authorized body (most often - the central bank);
- the issuer of cryptocurrency is miners, and the issuer of electronic money is a legally authorized person-issuer;
- cryptocurrency is produced in the mining process, electronic money is issued by order of the authorized body in an amount equal to the mass of fiat money;
- when using electronic money to prevent financial risks, the client identification procedure is required, and when using cryptocurrency anonymity is maintained;
- the value of cryptocurrency is determined by supply and demand, users' trust in the system, and the value of electronic money is equal to the value and quantity of fiat currency;
- cryptographic methods are also used for the circulation and protection of electronic money in conventional payment systems. However, in the case of cryptocurrency without mathematical algorithms, it is a priori impossible to create "coins" and transactions, even if the data did not have to be protected.

Technically, cryptocurrency is a program code that has become a so-called intermediary in financial transactions between the issuer (miner) and the user of this code. It cannot be said that cryptocurrency is a program that has got out of control and is aimed at deforming the world's financial systems. Surprisingly, you can be sure that cryptocurrency is a program code aimed at a qualitatively new formation of a new financial system. Moreover, the appearance of this phenomenon is not strange and unexpected, because humanity has long come to the point of non-cash payments, abandoning cash as a relic of the past. Cryptocurrency is just a programmer's proposal to unify the world currency, which in a decade can move the dollar and the euro and take a prominent place among the methods of calculation.

A cryptocurrency consists of mathematical codes, a special set of letters and numbers, however, it is not a "classic" program code that is the object of intellectual property rights, but a numerical unit that is an "intermediary" between the issuer and the final payment.

Although a crypto unit is a code or sequence of characters, its main purpose is to act as a medium of exchange. Directly as a code, it has no independent value and does not carry any useful properties in itself. However, as a means of exchange accepted by many participants in civil and economic circulation, cryptocurrency acquires significant value.
As a means of exchange, cryptocurrency corresponds to the legal definition of "good", and its lack of material form clearly indicates the intangible nature of this good. However, intangible assets are a generic concept in relation to specific concepts - specific objects of civil rights that are part of this set, and therefore the classification of cryptocurrencies in a broad category of intangible assets can not be considered an exhaustive characteristic.
Given that cryptocurrencies are objects of property turnover, and they are subject to property rights, there are grounds for recognizing cryptocurrencies as property, but the property is also a set of objects, and therefore their attribution to the property requires further detail.
Cryptocurrencies do not fully correspond to any of the currently defined objects of civil rights, and this indicates in favor of their further definition as a separate object of civil rights or as part of a separate group of objects of civil rights, such as a class of digital or virtual intangible assets, which will require the expansion of the classification of intangible assets and their division into property and personal intangible assets.
Intangible assets, which cover virtual assets, including cryptocurrencies, should be recognized as property and property rights (Nekit et al., 2019). In terms of monetary law, cryptocurrencies are not money, although they are able to perform the same functions. However, certain objects become money not because of their nature or internal characteristics, but as a result of recognition. That is, this status is a legal regime rather than a legal nature. Under certain conditions, it is quite possible to assume the recognition of cryptocurrencies as money in the future.

3. Global approaches to legal regulation of cryptocurrencies

Approaches to legal regulation of cryptocurrency and attitudes to it differ in different countries.
In the Republic of Singapore, the circulation of cryptocurrencies and transactions related to this process are not regulated by law. However, the activities of cryptocurrency exchanges in the territory of this state are regulated by law enforcement agencies of state security. Depending on the US state, a cryptocurrency is recognized as a currency or an exchange commodity, and its circulation is subject to licensing, although such transactions are not regulated at the federal level. Nevertheless, law enforcement agencies are working to counter illegal cryptocurrency transactions (Nekit, 2018).
The vast majority of continental European countries and the United Kingdom also did not introduce state regulation of cryptocurrency circulation (European Parliament, 2015). Germany, Sweden and Spain have recognized cryptocurrency as a "private" means of payment. Norway and Finland consider cryptocurrency to be an exchange asset and commodity. Japan fully regulates the circulation of cryptocurrency as a digital asset. The Law "On Currency Regulation" regulates the procedure for cryptocurrency exchanges and mining. Due to the legal and financial status of cryptocurrencies, Japanese law enforcement agencies adequately counter illegal cryptocurrency transactions and ensure the economic

security of not only individuals but also public and private financial institutions (Nekit, 2018). In some countries, cryptocurrencies are forbidden. Thus, cryptocurrencies have been banned in Bolivia, Vietnam, Ecuador, China, Thailand and Turkey.

In Ukraine, the issuance and circulation of any currency other than the national currency and the use of monetary surrogates as a means of payment are prohibited (Part 2 of Article 32 of the Law of Ukraine "On the National Bank of Ukraine") (Verkhovna Rada of Ukraine, 1999). The National Bank of Ukraine considers cryptocurrency as a monetary surrogate that has no security of real value and cannot be used by individuals and legal entities in Ukraine as a means of payment, as it contradicts the norms of Ukrainian legislation. In addition, the use of cryptocurrencies is a high risk factor, in particular due to the anonymity and decentralization of transactions. At the same time, the international distribution of such payments makes this category of services attractive for illegal actions, including money laundering or terrorist financing (National Bank of Ukraine, 2014). The use of cryptocurrencies is illegal in Ukraine, as they are monetary surrogates, and their use is contrary to current legislation.

Despite the legal uncertainty of cryptocurrencies, a number of countries, including the United States, Germany, Japan, Great Britain, Canada, introduce it in various sectors of the economy, recognizing cryptocurrency at the local level (within one industry, law, public sphere, etc.) private money, investment assets, commodities, etc. (Duchenko & Pavlenko, 2018). This allows to tax cryptocurrencies, license activities related to their circulation or mining, recognize the subject of a criminal offense and so on without recognition them officially and determining their status at the legislative level. The local definition of cryptocurrencies is primarily aimed at making a profit by the state and combating crime. However, the existence of certain regulations governing the circulation of cryptocurrencies at the local level creates unjustified conflict and competition of legal norms with state (federal) legislation, which leads to violations of human and civil rights and freedoms that cannot be protected in court.

Currently, cryptocurrencies do not affect national currencies and have the unofficial status of a separate means of payment, which is converted into fiat money (Duchenko & Pavlenko, 2018), and since such activities are not controlled, there are frequent cases of drug and arms trafficking, fraud, money laundering, misappropriation, financing of terrorism or any criminal activity of organized groups and criminal organizations.

Today, cryptocurrency is a means of payment in both legal transactions and DarkNet. And unlike e-banking, which is constantly exposed to danger by attackers, cryptocurrency has a reliable protection in the form of Blockchain technology. That is why banking operations using electronic banking require additional measures to ensure their security, as emphasized by the Basel Committee on Banking Supervision. After all, in recent years, some banks have begun to provide cross-border e-banking services, which has significantly increased the risk of criminal interference in transactions, which necessitates proper risk management in e-banking, first at the domestic level and later at the international level (Tykhonova et al., 2019). Taking into account the increasingly active development of the capabilities of criminals, both technical and intellectual, it is necessary to recognize cryptocurrency as a legal means of payment. This will reduce the degree of riskiness of international financial settlements, as well as allow to recognize settlements in cryptocurrency as those made within the legal field.

4. Peculiarities of criminal liability for transactions related to the circulation of cryptocurrencies and combating criminal offenses in this area

Due to the legal uncertainty of the status of cryptocurrencies at the legislative level in the world environment, the establishment of criminal liability for operations related to the circulation of cryptocurrencies, as well as effective counteraction to criminal offenses in this area remains an urgent issue. International cooperation in the fight against criminal offenses related to the circulation of cryptocurrencies should be carried out on the basis of participation of all states (Cherniavskyi, et al., 2021a). International cooperation should be carried out in various areas and include, first of all, the creation of regulations governing the circulation of cryptocurrency in the world, the development of general recommendations for regulating this issue at the national level, and the introduction of effective models of organizational cooperation between states to combat criminal offenses related to the circulation of cryptocurrencies. Therefore, we should pay attention to the Blockchain Claims Database (BLD), launched by the New York financial law firm Murphy & McGonigle. This commercial project is used by law enforcement agencies to investigate offenses related to the creation of fraudulent ICOs, cryptocurrencies, etc. BLD tracking data includes the total number of fraud cases in this area, their trends, information on criminal or civil cases, generalized circumstances of one or a group of cases that may belong to new startups or projects.

As noted, cryptocurrencies are either a currency or a commodity (property). Given these properties of cryptocurrency, criminal offenses committed with their use can be divided into two groups: 1) "real", i.e. criminal offenses in which the subject of encroachment is cryptocurrency or in which cryptocurrency is used as a means of payment; 2) "virtual", i.e. criminal offenses committed exclusively on the Internet using computer technology, the method of informational influence (Perov, 2017).

In recent years, there has been a clear trend of "merging" of the real criminal world and the so-called "virtual", which contributes to an increase in the number of cases of transnational criminal offenses. This trend eventually allows organized groups and criminal organizations to implement more complex criminally illegal schemes of their illegal activities. As a result, the complexity of detection and investigation of such criminal offenses increases significantly (Cherniavskyi, et al., 2021b), which leads to a decrease in the level of security of human, society and the state.

One of the measures aimed at combating transnational crime is the approval of the UN Convention against Transnational Organized Crime (United Nations, 2000). Such criminal offenses include cybercrime, corruption, terrorism perpetrated by persistent criminal organizations, and the financing of their illegal activities. The international community has obliged all member states to criminalize corruption, money laundering, terrorism and its financing. For some time, such measures have yielded the expected positive results in the fight against transnational crime, but with the advent of cryptocurrencies and distributed registry technology (Blockchain), the detection and counteraction of the above criminal offenses has become much more difficult. This is due, firstly, to the legal uncertainty of cryptocurrencies, secondly, their non-control by government agencies and financial regulators, thirdly, the anonymity of operations related to the circulation of

cryptocurrencies, fourthly, the lack of restrictions (except for the code) and the ability of the cryptocurrency network in terms of the number and volume of such transactions.

The introduction of cryptocurrencies creates additional threats to human security, society and the state, which necessitates the improvement of legislation and the development of new approaches to regulating legal relations in this area, as well as the fight against transnational crime, including cybercrime (Babanina et al., 2021).

One type of cybercrime is the illegal operation of Internet servers, where cryptocurrency transactions are often carried out. The most common Internet sites that use cryptocurrency in criminally illegal activities are Deep web and Mixers. Deep web is an Internet site that stores data not available for public use: information that is a state, corporate or banking secret, information on the sale of drugs and weapons, contract killers, etc. All of the above can be purchased for cryptocurrency. The issue of protection of computer information and information that is a secret protected by law, other similar issues are of serious concern around the world. This is related to ensuring the national security of the state and protection of constitutional human rights (Babanina et al., 2021).

Mixers is an online platform that helps convert cryptocurrency, mostly obtained by criminal means. For example, a person sends a certain amount of cryptocurrency to the specified service, where there is already a cryptocurrency received from other people. It is merged into one anonymous cryptocurrency, and then redistributed among all users. Thus, the person A. receives back the same amount of cryptocurrency, but from a completely different, unknown user. All this helps A. to hide the true path of the cryptocurrency obtained by criminal means, which makes it difficult to identify this cryptocurrency, its origin and owners. There are other online platforms where drugs, weapons, child pornography, and other illicit goods, services, and content are sold primarily in cryptocurrency.

Thus, cryptocurrency is mostly the subject of predicate criminal offenses, i.e. those as a result of which the proceeds were obtained illegally. Such criminal offenses are provided for in the majority of the Criminal Code of foreign states that have ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (hereinafter referred to as Convention). This Convention provides for criminal liability for intentionally committing:

1) the conversion or transfer of property, knowing that such property is income, for the purpose of concealing or masking the illegal origin of property or for facilitating any person involved in a predicate offense;

2) concealment or disguise of the true nature, source, location, condition, transfer, rights in relation to property or ownership of it, realizing that such property is income;

3) acquisition of property, possession or use, realizing that at the time of receipt such property is income;

4) participation in the commission, association or conspiracy to commit, attempt to commit, aiding, abetting, facilitating and advising on the commission of any of the criminal offenses established in accordance with Art. 9 of the Convention (Council of Europe, 2005).

In the Criminal Code of Ukraine, liability for the above acts is provided by Art. 209 "Legalization (laundering) of property obtained by criminal means" and Art. 209-1 "Intentional violation of the legislation on prevention and counteraction to legalization

(laundering) of proceeds from crime, terrorist financing and financing of proliferation of weapons of mass destruction". In Ukraine, cryptocurrency is generally considered to be property reflected in the draft law № 3637 "On Virtual Assets", which states that a virtual asset is a special type of property that is valuable in electronic form, exists in the circulation of virtual assets, and may be involved in civil circulation. That is why cryptocurrency is the subject of criminal offenses under Art. 209 and Art. 209-1 of the Criminal Code of Ukraine.

In the United States, the fight against illicit financial transactions is regulated by a number of regulations (Banking Secrecy, Anti-Money Laundering, Intelligence Reform to Prevent Terrorism, Corporate Transparency etc.), which are included in the Rules for Combating Money Laundering and Terrorist Financing. These laws provide for countermeasures and criminal sanctions for money laundering and terrorist financing. For example, in May 2021, an individual was sentenced to 2 years in prison for money laundering using cryptocurrency. Being a former banking employee and having the skills and abilities, he created the cryptocurrency Herocoin, through which he received a commission for transactions. He also converted Bitcoins and other criminally obtained cryptocurrencies into Herocoin and then into fiat money. By such actions he received from 15 to 25 million US dollars (The Mercury news, 2021).

In Spain, for such acts criminal liability is established in accordance with Art. 301 of the Criminal Code of Spain: possession of assets obtained from criminal activity, transfer, conversion (Part 1); concealment of their illegal origin (Part 2). In this case, all illegally obtained income is confiscated (Art. 127 of the Criminal Code of Spain). Criminal liability has been established for incitement and aiding and abetting money laundering (Art. 304 of the Criminal Code of Spain) (Spain, 2013). Other prohibitions on obtaining illegal income are provided by Royal Decrees and the Anti-Money Laundering Act.

Legalization of proceeds of crime is prohibited in France by the Laws on the Participation of Financial Institutions in Combating Money Laundering from the Sale of Drugs, on Combating Money Laundering and Drug Trafficking, and on International Cooperation in the Seizure and Confiscation of Money and Other Goods material values that are obtained from criminal activity. Criminal liability for various socially dangerous acts related to the legalization of proceeds from crime is provided by Art. 222-38, 324-1–324-9 of the Criminal Code of France. In this case, criminal liability for these criminal offenses applies to both individuals and legal entities (France, 2005).

In the UK, there is a law on criminal finance, which provides measures to combat money laundering and tax evasion. This law provides for criminal liability for a number of offenses related to tax evasion and legalization of proceeds of crime. This law, as amended in 2018, expanded the concept of "cash", which also includes game vouchers, electronic tokens with a fixed value, certificates of game bets. During the investigation of the above-mentioned criminal offenses, law enforcement agencies have the right to seize and confiscate any property or funds obtained illegally or legally in order to ensure compensation for damages caused by tax evasion.

In Germany, for legalization of money and concealment of property obtained by criminal means criminal liability is provided (Art. 261 of the Criminal Code of Germany) (Germany, 1871). Counteraction to illegal activities related to the receipt of money or property, as well

as their concealment, is regulated by the Law on Combating Illicit Trafficking in Drugs and Other Forms of Organized Criminal Activity.

Cryptocurrencies are often used as a means of payment to finance terrorism, purchase weapons, bribe civil servants, pay mercenaries (criminals), and so on. Such socially dangerous acts are committed mainly in the Middle East and West Asia, where various armed conflicts and terrorist acts are ongoing. In Ukraine, criminal liability is provided for such acts: 1) Art. 258-4 of the Criminal Code of Ukraine "Assistance in committing a terrorist act"; 2) Art. 258-3 of the Criminal Code of Ukraine "Terrorist Financing"; 3) Art. 369 of the Criminal Code of Ukraine "Offer, promise or provision of illegal benefit to an official"; 4) Art. 440 of the Criminal Code of Ukraine "Development, production, acquisition, storage, sale, transportation of weapons of mass destruction"; 5) Art. 447 of the Criminal Code of Ukraine "Mercenary" and others.

In France, criminal liability for terrorist financing is not provided by the Criminal Code, but by the Law on Combating Terrorism. Other criminal offenses related to terrorism and the promotion of such activities are provided for in the sections "On Terrorist Acts" (Articles 421-1 – 421-4) and "Special Provisions" (Articles 422-1 – 422-5) of the Criminal Code of France. These norms provide for sanctions not only against individuals but also against legal entities involved in or contributing to terrorism.

Criminal liability is provided for activities related to terrorism in Germany (Articles 129a, 211, 220a, 239a, 239b of the Criminal Code of Germany, etc.). Countering the financing of terrorism and other illegal actions is regulated by the Law on Combating Terrorism. Criminal liability for terrorist financing is provided for in the Criminal Code of Austria (§ 278d) (1974), Bulgaria (Article 162) (1968), Belgium (Articles 137-141) (1996), the Czech Republic (§ 272-292, 309-322, 400-418). (2009) etc. Thus in the Criminal Code of the Czech Republic assistance to terrorism, its financing, mercenaries and other similar criminal offenses are provided in various sections.

This is only the smallest share of criminal offenses committed using cryptocurrencies as a means of payment or the subject of a criminal offense.

The computerized society has long been familiar with criminal offenses committed with the use of computer technology. Nowadays, due to the spread of cryptocurrencies in the world and their high value, new ways of committing so-called "computer criminal offenses" have appeared. The most common way to do this is to create substandard software that illegally uses the computing power of other users' computers to create (mine) cryptocurrencies. The need to combat criminal offenses in the field of information technology, most of which are cross-border, is confirmed by the fact that they have recently become a global international problem (Babanina et al., 2021).

In Ukraine, for such acts, criminal liability is established by Art. 361 of the Criminal Code of Ukraine "Unauthorized interference in the work of electronic computers, automated systems, computer networks or telecommunications networks" and Art. 361-1 of the Criminal Code of Ukraine "Creation for the purpose of use, distribution or sale of malicious software or hardware, as well as their distribution or sale".

The Criminal Code of Germany provides for such acts in the form of qualifiers for various criminal offenses, in particular: 1) § 202c - espionage (interception of data by preparing passwords, security codes and malware for resale or personal use; 2) § 263a - computer fraud (obtaining material benefits through the creation of malicious programs and their

use to influence the processing of computer data, or the implementation of other influences on data processing); 3) § 303a - change of data (illegal erasure or rendering unfit for use of computer data) etc.

The Criminal Code of France establishes criminal liability for: 1) obtaining illegal access to an automated data processing system, which led to the deterioration of the functioning of such a system (Article 323-1 of the Criminal Code of France); 2) obstruction or violation of the normal operation of the automated data processing system (Article 323-2 of the Criminal Code of France); 3) input or destruction of data in the system of automated data processing (Article 323-3 of the Criminal Code of France) etc.

The above criminal offenses, like many other computer criminal offenses, are characterized by complexity, as they require the offender to have special knowledge in the field of information technology, cryptography, financial transactions, etc. (Cherniavskyi et al., 2021b).

When committing such criminal offenses with the help of new technologies and telecommunications, the place of commission of a socially dangerous act, as a rule, does not coincide with the place of actual occurrence of socially dangerous consequences. There may be several such places. They can be at a considerable distance from each other, be in vehicles, various institutions, in areas, including in different states and on continents (Cherniavskyi et al., 2021b).

It is not uncommon to commit criminal offenses related to unauthorized interference with a computer, which blocks its operation and all available information. To restore work and information, criminals demand payment in cryptocurrency. In this case, this requirement is expressed by a corresponding entry on the computer monitor screen, which is displayed to the user when he turns it on.

Another common type of criminal offense is Internet fraud. In most cases, the direct subject of such criminal offenses is money, which due to its special status is of greatest interest to fraudsters. Other items, for the most part, can also be pre-equated to money, because, in the end, after acquiring the right to them, this property is resold (Cherniavskyi et al., 2021b). This also applies to cryptocurrency.

5. Conclusions

Despite the widespread use of cryptocurrencies, they remain outside the legal framework in most countries. The legal uncertainty of the status of cryptocurrencies contributes to the increase in the number of criminal offenses related to their circulation. Such acts are classified in different ways, in particular as: Internet fraud; legalization of proceeds from crime; financing of terrorism and other criminal activities; acquisition of weapons, drugs, pornographic content and other prohibited or restricted items, unauthorized interference in the operation of computers for the purpose of mining at the expense of the computing power of the victim's computer, etc.

The peculiarities of the qualification of socially dangerous acts of a person who commits criminal offenses related to the circulation of cryptocurrencies are that the cryptocurrency should be valued as a means of payment or as a commodity. From an economic point of view, this is not significant, but in criminal law, the status of cryptocurrency affects the correctness of qualifications, the use of certain types of penalties (e.g., confiscation),

measures of a criminal nature (special confiscation or other measures against legal entities), etc.

The question of the expediency of establishing criminal liability for transactions related to the circulation of cryptocurrencies by supplementing the Criminal Code with special rules remains open. The criminalization of socially dangerous acts related to the circulation of cryptocurrencies should be carried out in accordance with the national legislation governing this area of activity. To prevent criminal offenses related to the circulation of cryptocurrencies, it is now necessary to take the following measures:

1) to determine the legal status of cryptocurrencies, cryptocurrency exchanges, mining and other activities related to cryptocurrency at the legislative level;

2) to provide for the rights and obligations of persons conducting transactions with cryptocurrencies;

3) to establish criminal and legal protection of public relations in the field of cryptocurrency circulation.

These measures will help establish government control over the circulation of cryptocurrencies and, as a result, ensure the security of all operations related to cryptocurrencies.

References

Austria. (1974). Criminal Code of Austria. [*Online*]. Available at: https://www.legislationline.org/download/id/8548/file/Austria_CC_1974_am122019_de.pdf

Babanina V., Tkachenko I., Matiushenko O., & Krutevych M. (2021). *Cybercrime: History of formation, current state and ways of counteraction.* Amazonia Investiga, 10 (38), pp. 113–122. DOI: https://doi.org/10.34069/AI/2021.38.02.10.

Belgium. (1996). Criminal Code of Belgium. [*Online*]. Available at: https://www.legislationline.org/download/id/8240/file/Belgium_CC_1867_am2018_fr.pdf

Belomyttseva O. (2014). On the concept of bitcoin cryptocurrency in the framework of the opinions of financial regulators and the context of private electronic money. Problems of accounting and finance, 2 (14), pp. 26–28.

Bulgaria. (1968). Criminal Code of Bulgaria. [*Online*]. Available at: https://www.legislationline.org/download/id/8395/file/Bulgaria_Criminal_Code_1968_am2017_ENG.pdf

Cherniavskyi S., Babanina V., Mykytchyk O., & Mostepaniuk L. (2021a). *Measures to combat cybercrime: analysis of international and Ukrainian experience.* Cuestiones Políticas, 39(69), pp. 115–132. DOI: https://doi.org/10.46398/cuestpol.3969.06.

Cherniavskyi S., Babanina V., Vartyletska I. & Mykytchyk O. (2021b). *Peculiarities of The Economic Crimes Committed with the Use of Information Technologies*. European Journal of Sustainable Development, 10 (1), pp. 420–431. DOI: https://doi.org/10.14207/ejsd.2021.v10n1p420.

Council of Europe. (2005). Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. [*Online*]. Available at: https://rm.coe.int/168008371f

Cvetkova I. (2018). *Cryptocurrencies legal regulation.* Bricks law journal, 18, pp. 129-153.

Czech Republic. (2009). Criminal Code of the Czech Republic. [*Online*]. Available at: https://www.legislationline.org/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf

Duchenko M. & Pavlenko T. (2018). *Influence of cryptocurrencies on the country's economy.* Money, finance and credit, 19, pp. 1002–1009.

European Parliament. (2015). Directive (EU) 2015/849 of the European Parliament and of the council of 20 May 2015. [Online]. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.

France. (2005). Criminal Code of France. [*Online*]. Available at: https://www.legislationline.org/download/id/8546/file/France_CC_am012020_fr.pdf

Germany. (1871). Criminal Code of Germany. [*Online*]. Available at: https://www.legislationline.org/download/id/8253/file/Germany_CC%20am2019_de.pdf

Kaznacheeva D. & Dorosh A. (2020). Cryptocurrency: problems of legal regulation. Bulletin of the Criminological Association of Ukraine, 2 (23), pp. 170–176.

Kuznetsov V. & Yakubov A. (2016). On approaches to international regulation of cryptocurrencies (BITCOIN) in certain foreign jurisdictions. Money and credit, 3, pp. 20–29.

Lukyanov V. (2014). The origin of the cryptocurrency market in the information and network paradigm. Actual problems of economy, 8 (158), pp. 436 - 441.

National Bank of Ukraine. (2014). *On the legality of the use of "virtual currency / cryptocurrency" Bitcoin in Ukraine: explanation of the National Bank of Ukraine dated November 10, 2014*. [Online]. Available at: https://zakon.rada.gov.ua/laws/show/n0435500-14#Text

Nekit K. (2018). World approaches to determining the legal status of cryptocurrencies. Journal of Civil law, 29, pp. 100-106.

Nekit K., Ulianova G. & Kolodin D. (2019). *Website as an object of legal protection by Ukrainian legislation.* Amazonia investiga, 8(21), pp. 222-230. https://amazoniainvestiga.info/index.php/amazonia/article/view/97

Perov V. (2017). *Identification, qualification and organization of investigation of crimes committed with the use of cryptocurrency*. Moscow: Yurlitinform, 2017, p. 200.

Petruk O. (2017). *The essence of cryptocurrency as a methodological prerequisite for its accounting reflection.* Visnyk of ZhSTU, 4 (82), pp. 48-55.

Shapoval P. (2017). Business and bitcoins: how cryptocurrency penetrates the Ukrainian economy. Made for Minds. [Online]. Available at: https://www.dw.com/uk/biznes-ta-bitkoini-yak-kriptovalyuta-pronikae-v-ukrainska-ekonomiku/a-41858072

Skrypnyk V. (2018). The place of cryptocurrency in the system of objects of civil rights. Entrepreneurship, economy and law, 8. pp. 38–43.

Spain. (2013). Criminal Code of Spain. [*Online*]. Available at: https://www.legislationline.org/download/id/6443/file/Spain_CC_am2013_en.pdf.

Tapscott A. & Tapscott D. Blockchain technology. What is driving the financial revolution today. Moscow: EKSMO, 2017, p. 448.

The Mercury news. (2021). California man gets 2 years for laundering millions in Bitcoin and cash. [*Online*]. Available at: https://www.mercurynews.com/2021/05/29/yorba-linda-man-gets-2-years-for-laundering-millions-in-bitcoin-and-cash/.

Tykhonova O., Lytvyn N., Ivantsov V., Chyshko K. & Yarosh A. *Electronic banking as a prospective directive for the financial services market development.* Journal of Legal, Ethical and Regulatory Issues, 22 (2), pp. 182-198.

United Nations. (2000). United Nations Convention against Transnational Organized Crime and the Protocols Thereto. [*Online*]. Available at: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

Verkhovna Rada of Ukraine. (1999). On the National Bank of Ukraine: Law of Ukraine of May 20, 1999. [Online]. Available at: https://zakon.rada.gov.ua/laws/show/679-14/page#Text.