DOI: https://doi.org/10.34069/AI/2021.42.06.17
How to Cite:
Panova, L., Tsurkanu, S., Synieokyi, O., Dilna, Z., & Prymachenko, I. (2021). Liability in the field of digital payment systems and cryptocurrencies: mission is (im)possible? *Amazonia Investiga*, *10*(42), 186-195. https://doi.org/10.34069/AI/2021.42.06.17

Liability in the field of digital payment systems and cryptocurrencies: mission is (im)possible?

Юридична відповідальність у сфері цифрових платіжних систем і криптовалюти: місія (не)можлива?

Received: May 13, 2021 Accepted: July 3, 2021

Written by:
Liydmyla Panova[75]
https://orcid.org/0000-0002-1393-8626
Siuzanna Tsurkanu[76]
https://orcid.org/0000-0001-5851-5996
Oleh Synieokyi[77]
https://orcid.org/0000-0002-1419-4964
Zoriana Dilna[78]
https://orcid.org/0000-0002-6066-1279
Ivan Prymachenko[79]
https://orcid.org/0000-0003-1908-4278

Abstract

An electronic payment system is a system of settlements between different organizations and Internet users when buying or selling goods or services over the Internet. The relevance of the research topic is that electronic payment systems are used widely at the present stage of the development of society. This area has not escaped criminal activity. Penalties for digital payment systems and cryptocurrencies should be commensurate with the level of damage caused. The article analyzes the international legal establishing liability for this type of crime. At the instant, it remains an open question for further study of the legal status of cryptocurrency in different countries and the settlement of penalties for violations in the field of digital payment systems and cryptocurrency. Research methods: comparison, observation, analysis, synthesis, analogy, the system method, generalization method, and formal-legal method. According to the results of the study, the international comparative aspect of the types of liability for offenses in the field of

Анотація

Електронна платіжна система являє собою систему розрахунків між різними організаціями та Інтернет-користувачами під час купівлі-продажу товару чи послуги через мережу Інтернет. Актуальність теми дослідження полягає в тому, що на сучасному етапі розвитку суспільства широко використовуються електронні платіжні системи. Цю сферу не оминула злочинна діяльність. Покарання за правопорушення у сфері цифрових платіжних систем та криптовалюти повинно відповідати рівню завданої шкоди. У статті проведений аналіз міжнародного законодавства, що встановлює відповідальність за даний вид злочину. Наразі залишається відкритим питанням для подальшого вивчення саме правовий статус криптовалюти у різних країнах та врегулювання покарання за порушення у сфері цифрових платіжних систем і криптовалюти. Методи дослідження: порівняння, спостереження, аналізу, синтезу, аналогії, системний метод, метод

[75] Ph. D., Associate Professor of Civil Law Department, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
[76] Ph. D., Associate Professor of Department of International Law and Comparative Law, International Humanitarian University, Ukraine.
[77] Doctor of Social Communications, Professor of the Department of Philology and Publishing, Faculty of Law, Humanities and Social Sciences, Kremenchuk Mykhailo Ostrohradskyi National University, Ukraine.
[78] Ph. D., Associate Professor of the Department of Criminal-legal Disciplines of Lviv State University of Internal Affairs, Ukraine.
[79] Candidate of Economic Sciences, Associate Professor of the Department of National Economy of National University "Odesa Law Academy", Ukraine.

digital payment systems was analyzed; the issue of criminal liability for offenses in the field of digital payment systems and cryptocurrencies, as a key punishment for these actions; identified means of protection of payment systems; the issue of legal regulation of cryptocurrency in different countries.

Keywords: legal liability, offenses, digital payment systems, cryptocurrency, cybercrime.

узагальнення, формально-юридичний. За результатами проведеного дослідження проаналізовано міжнародний компаративістський аспект щодо видів відповідальності за правопорушення у сфері цифрових платіжних систем, було досліджено питання кримінальної відповідальності за правопорушення у сфері цифрових платіжних систем та криптовалюти як ключового покарання за вказані діяння, виокремлено засоби захисту платіжних систем, проблематику правового регулювання криптовалюти у різних країнах світу.

Ключові слова: юридична відповідальність, правопорушення, цифрові платіжні системи, криптовалюта, кіберзлочинність.

Introduction

Today, there are a large number of payment systems that differ in different countries. Payment systems are the central means by which shocks are transmitted in domestic and international money and other markets. If the risks that may arise during the operation of the payment system are not averted, a crisis may occur that threatens the stability of these markets. Therefore, efficiency, effectiveness, and security are the main requirements for both the payment system of an individual country and the global financial system as a whole. These requirements can be met by electronic payment systems that use the latest advances in technology.

Currently, most commercial transactions have moved to the Internet. Relevant changes in economic relations have led to the formation of a new sphere of public relations – e-commerce. Experts attribute the emergence of e-shops and a new form of payment – e-money – to its appearance.

The specifics of this area of public relations have caused a number of problems that need to be addressed. In particular, the question of the legitimacy of electronic money and payment systems, in which they are used as a means of payment needs to be clarified.

Offenses in the field of digital payment systems and cryptocurrencies belong to the field of cybercrime. Today, many foreign countries have a system of cooperation, due to the need to share experiences at the international level. The COVID-19 pandemic with its risks of restricting human rights (individual) has become a challenge, necessitating more attention to defining a person's status as an individual and ensuring his or her rights (Kharytonov, Kharytonova, Kolodin, & Tkalych, 2020).

These issues are coordinated by each country in accordance with the developed and current cybersecurity strategy: The United States and most EU member states in their strategies put the fight against cybercrime at the forefront. The United States was the first country to pass a law and create a National Cyber Security Strategy (Petrovsky, & Livchuk, 2019).

Foreign countries use the following main areas of crime control: the creation of political programs to combat crime; regulatory regulation of the information sphere; establishment of criminal liability for cybercrime; international cooperation in the field of combating cybercrime; creation of special bodies for the prevention and detection of cybercrime.

Liability for digital payment systems and cryptocurrencies is a pressing issue around the world, as evidenced by the numerous cases of such crimes. In particular, it is possible to give the following examples of offenses:

- in 2018, one of Japan's largest digital currency exchanges, Coincheck, reported losing a cryptocurrency worth about $ 534 million due to a hacker attack on its network. As a result, Coincheck has temporarily suspended deposits and withdrawals for all cryptocurrencies except bitcoin (BBC. News Ukraine, 2018);

– one of the world's largest cryptocurrency exchanges Binance reported a "large-scale hacking" by hackers and theft from its platform for more than $ 40 million. To steal these funds, hackers used phishing, virus attacks, and other techniques to steal bitcoins. The hackers managed to obtain valuable data from a large number of customers, including two-factor identification codes (Economic truth, 2019).

The study aims to analyze the types of liability for offenses in the field of digital payment systems and cryptocurrency in the international comparative aspect.

Theoretical Framework or Literature Review

During the study, articles, monographs, textbooks, and regulations were analyzed.
For comprehensive disclosure of the topic of the article used the work of scientists who formed the theoretical basis of the main material. These include Alekseev (1999), Serdyuk (2010; 2011), Zaychuk and Onishchenko (2008), Rabinovich (2007), Berlach (2012), Skakun (2001), Lipinsky (2004), Ivanenko (2007), Azemsha (2012), Lukyanets (2004), Shemelynets (2017), Musatkina (2006), Romanyuk (2019), Grin and Donchenko (2015), Dmitriev, Polyansky, and Trofimov (2008), Zayats (2012), Vovchak, Shpargalo, and Andriykiv (2008), Spindler and Summers (1994), Usoskin and Belousova (2010), and Pyrih (2008).

The topic of legal liability in the context of this study needs to be disclosed as a fundamental category. Among the scientists who studied the essence of legal responsibility, it is possible to Alekseev (1999), Serdyuk (2010; 2011), Zaychuk and Onishchenko (2008), Rabinovich (2007), Skakun (2001), Lipinsky (2004), and Ivanenko (2007). Thus, based on their work, approaches to understanding legal responsibility, its understanding in general, were analyzed.

Regarding the separation of types of legal liability, this element of the study was analyzed based on the works of Azemsha (2012), Lukyanets (2004), Shemelynets (2017), Musatkina (2006), Romanyuk (2019), Grin and Donchenko (2015). This issue is a pluralism of opinions, which expands the possibilities for a comprehensive analysis of the types of legal liability in legal doctrine.

As for the issues of legal regulation of digital payment systems and cryptocurrency in different countries of the world, it was necessary to refer to the regulatory framework of European Union organizations dealing with payment systems and cryptocurrency, namely to the European Central Bank (Kokkola, 2010) and the Payment and Settlement Systems Committee of the Bank for International Settlements (Committee on Payment and Settlement Systems, 2003).

To analyze the legal regulation, including liability for violations in the field of digital payment systems and cryptocurrency, electronic resources were analyzed, which contain, in particular, information on innovations in countries related to the legal regulation of cryptocurrencies. These appeals are appropriate in this research topic, as cryptocurrency is a new phenomenon, and the world is undergoing constant changes in its functioning. Also, the international aspect of the study of liability for offenses in the field of digital payment systems and cryptocurrency has been studied by such scientists as Golubeva (2017), Yushchenko, Savchenko, Tsokol, Novak, and Strakharchuk (1998), Lapta (2017), Orlov and Onishchenko (2014), Bilobrov (2020), in particular, Golubeva (2017) studied the essence of cryptocurrency on the example of bitcoin in such countries as Denmark, China, and other countries; Bilobrov (2020) and Orlov and Onishchenko (2014) investigated the responsibility for violations of digital payment systems and cryptocurrencies on the example of international experience, etc.

Despite the extensive system of scientific papers on cybercrime, the topic of diversification of liability for offenses in the sphere of digital payment systems and cryptocurrency, their legal regulation, and protection need further detailed study.

Methodology

The methodological basis for the study of types of liability in the field of digital payment systems and cryptocurrency in the international comparative aspect is a set of methods and techniques of scientific knowledge, the use of which is due to the legal regulation of digital payment systems and cryptocurrency in different countries.

Following the goal in the research process, the following general scientific methods were used:

1) system method. This method was used to study the practice of legal regulation of

digital payment systems and cryptocurrencies in the United States, Britain, France, Germany, Denmark, Russia, etc. This allowed to form an idea of the legal regulation of cryptocurrency activities and payment systems in the world;

2) comparison method. To compare the experience of foreign countries in regulating digital payment systems and cryptocurrency, it was necessary to identify the general principles of the legal status of the subject of study, which allowed to find a general algorithm in building a system to combat cybercrime and punishment for such crimes;
3) method of observation. This method is used to comprehensively characterize both the theoretical and practical side of the object under study, which manifested itself in its active perception, during which results are obtained on approaches to its understanding, essence, and content;
4) method of analogy. With the help of this method, it became possible on the example of Ukrainian civil law to distinguish civil liability for offenses in the field of digital payment systems and cryptocurrency;
5) synthesis method. Its use allowed from all the variety of doctrines about the nature and content of digital payment systems and cryptocurrencies to distinguish the content that contributed to the establishment of their functions, means of protection, etc.;
6) method of analysis. This method contributed to the detailed disclosure of the specifics of the research topic by identifying certain parts of the field of digital payment systems and cryptocurrency, namely the practical and theoretical side;
7) generalization method. This method was utilized to identify key elements in the study, and by summarizing international experience, problematic aspects in the legal regulation of digital payment systems and cryptocurrencies were clarified;
8) formal-legal method. The use of this method allowed to establish the need to improve the legislative regulation of public relations that arise in the operation of digital payment systems and cryptocurrency, and;
9) method of ascent from the abstract to the concrete. This method helped to solve the problem of a small number of doctrinal teachings in the field of studying liability for offenses in the field of digital payment systems and cryptocurrency.

Results and Discussion

In the scientific legal literature, there is no single approach to the definition of legal liability. Scholars are divided into two camps: supporters of the monistic and dualistic approaches.

The first approach is characterized by the understanding of legal responsibility only in the negative (retrospective) aspect, excluding lawful conduct from the institution of legal responsibility. Thus, according to Alekseev, legal liability should be understood as the application to the guilty person of measures of state coercion for the offense (Alekseev, 1999); russian lawyers Senyakin and Chernykh expand the interpretation of legal liability by highlighting the legal relations arising from the offense between the state in the person of its appropriate bodies and the offender, who is obliged to suffer appropriate deprivation and adverse consequences for the offense, for violation of the requirements contained in the law (Serdyuk, 2010); according to Serdyuk (2011), legal liability can not be associated only with law enforcement relations, as it can also be carried out within the regulatory relationship, which is characteristic of the branches of private law. Additionally, statements about the monistic understanding of legal responsibility are shared by Rabinovich (2007).

The dualistic approach is characterized by the presence along with the retrospective aspect of the prospective, i.e. one that is characterized by positive legal responsibility. Positive legal responsibility can be interpreted as responsibility, which is defined by incentives, positive consequences in the form of, for example, a cash prize, promotion, announcement of gratitude (Berlach, 2012). Proponents of the dualistic approach are Skakun (2001), Lipinsky (2004), Ivanenko (2007), and Onishchenko (2008).

In the context of this study, it is advisable to use the division of legal liability into types by industry. Thus, according to this criterion are criminal, administrative, civil, constitutional, and international law (Azemsha, 2012). Lukyanets (2004) divides administrative responsibility into financial, transport, and economics.

Table 1.
The division of legal liability into types. Information provided by Shemelynets (2017), Musatkina (2006), Romanyuk (2019), Grin and Donchenko (2015), Dmitriev, Polyansky, and Trofimov (2008), Zayats (2012), Gashchin (2021), Koverznev and Koverzneva (2016), and Tkachenko (2013).

Type of responsibility	The most characteristic features
Financial	public-law nature; occurs for violation of financial legislation; application of measures of financial and legal coercion, the external form of expression of which are financial and legal sanctions; the subjects are the offender and the state represented by the competent authorities
Criminal	the legal form of criminal liability is a court conviction; entails the application of a specific measure of criminal law influence provided by the law on criminal liability; occurs for violation of criminal law grounds for the occurrence-administrative offense;
Administrative	has a public state-binding character; manifested in the imposition of certain types of administrative penalties on violators; the subject composition is characterized by relations of subordination
Civil-legal	compensatory nature; aimed at the property of the offender and does not affect his status; occurs only for violation of civil rights and obligations
International-legal	grounds for occurrence – international offense, the presence of international legal regulations; Occurs as a result of illegal behavior (non-compliance by state bodies with its international obligations, which manifests itself in violation of the rights of other states, international organizations, individuals, or legal entities) provided by the coercive force of the state; availability of special sanctions (for example, early reform or disbandment of the controlled body);
Constitutional	most of its manifestations take place in the political and legal sphere of society; the legal grounds for its occurrence are contained in the constitutional legislation; the onset of consequences for its subjects is aimed primarily at protecting the constitution, constitutional order, fundamental rights, and freedoms of man and citizen

To ensure the most complete disclosure of the research topic, it is advisable to determine the essence of digital payment systems and cryptocurrency.

At the international level, the payment system is interpreted as a tool or set of procedures that allow the transfer of funds from the payer to the payee (European Central Bank) (Kokkola, 2010), a set of payment instruments, banking procedures, and, as a rule, interbank funds transfer systems. provides money circulation (Committee on Payment and Settlement Systems of the Bank for International Settlements) (Law 4/26, 2013).

There is a large number of opinions in the scientific literature on the essence of payment systems. Vovchak, Shpargalo, and Andriykiv (2008) gives the following definition of the payment system: a set of payment instruments, banking procedures, and, as a rule, interbank money transfer systems, the combination of which provides money circulation together with institutional and organizational rules and procedures governing the use of these instruments and mechanisms. Usoskin, Belousova, and Spindler reduce the essence of the payment system to a set of specific tools that serve the efficient functioning of the country's economy (Spindler, & Summers, 1994; Usoskin, & Belousova, 2010).

With the development of Internet technologies and a wide range of subjects of its use, electronic (digital) payment systems are emerging. Among them, it is possible to single out the most famous:

- E-Gold;
- PayPal;
- PayCash;
- WebMoney;
- CyberPlat;
- Systems that use Smart-card (Mondex and VisaCash).

The functions of electronic payment systems are as follows (Pyrih, 2008):

- the ability to open and maintain virtual customer accounts;
- the client's ability to withdraw funds from the payment system in cash;
- transactions between customer accounts, storage of transaction data;
- ensuring the protection of customer information and account security;
- advisory customer support, etc.

Electronic payment systems are based on a new form of money – the so-called "electronic money", which is a monetary value that is stored electronically on a technical device and can be used to make payments. 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 a monetary system to create a secure, anonymous, and potentially stable virtual currency (Popov, 2017).

Legal regulation of cryptocurrencies in different countries is not the same, which can be explained by a relatively new phenomenon for payment systems.

In the United States, some bodies regulate and control cryptocurrency activities: the Financial Crimes Enforcement Network – manages all issues except tax. It is this body that issues licenses for cryptocurrency transfer activities; the US Internal Revenue Service - regulates taxation (Eurasian Commission, 2017).

Cryptocurrency in the UK is currently still considered a unique combination of numbers, which is the result of complex mathematical calculations and algorithms. Therefore, cryptocurrencies do not fall under the financial legislation of the United Kingdom. However, Her Majesty's Revenue and Customs (HMRC) defines cryptocurrencies as assets or private money. Moreover, HMRC may levy several types of taxes on transactions involving cryptocurrencies (Perma.cc, 2018).

Moreover, cryptocurrency is not yet used in any way in Russian law. The country has been found to be illegal, but there are some precedents where the use of cryptocurrency is seen by law enforcement as an illegal legalization activity (CryptoMagic, 2018).

In 2013, in Denmark, the Financial Supervision Authority (FSA) stated in an official statement that such a cryptocurrency as bitcoin is not recognized as a currency and, in this case, there is no need for its legal regulation (Golubeva, 2017). India wants to ban cryptocurrency ownership and trading at the legislative level. Such actions are subject to criminal liability (Kunytskiy, 2021).

In China, bitcoin is considered a commodity, not a currency. Bitcoin transactions are prohibited for banks but allowed for individuals (Golubeva, 2017).

Uncertainty of the legal status of cryptocurrency in the legislation of many countries makes it impossible to protect it from the state and establish responsibility for the relevant offenses.

In the specialized literature, there are methods of protection of the rights of users and owners of the payment system (Yushchenko, Savchenko, Tsokol, Novak, & Strakharchuk, 1998); Tchaikovsky, 2006). Thus, it is possible to single out the following:

- legal – measures that regulate the functioning of payment systems and establish liability for their violation;
- moral and ethical measures – norms of behavior of participants of calculations and service personnel;
- administrative measures – measures of an organizational nature, which regulate in detail the process of functioning of the payment information processing system, the use of its resources, staff activities, etc.;
- physical measures – protection and bypass mode of buildings in which the central computer equipment is located; protection of payment system key generation and certification centers; physical protection of payment system service personnel and creation of safe working conditions.

Illegal seizure of cryptocurrency in the way of hacking cryptocurrency exchanges and hacking attacks on cryptocurrency wallets is a cybercrime (Koziy, 2018).

The United States is considered one of the most computerized countries in the world. Accordingly, the development of information technology has also contributed to the emergence of cybercrime.

Crimes related to cryptocurrency include a hacker attack on the Bitfinex exchange in the summer of 2016, which resulted in the theft of 119,756 bitcoins from customer accounts, which at that time amounted to about 70 million US dollars, as well as hacking in June 2018 cryptocurrency exchange in South Korea, Bithumb, which stole $ 32 million in cryptocurrencies.

In 1979, the United States passed the Protection of Computer Systems Act, which established liability for entering intentionally incorrect data into a computer system, illegal use of computer equipment, making changes to the process of information processing or violation of these processes, theft of funds, papers, services, property, valuable information, conducting using computer technology or computer information. An improved act in the form of § 1030 in Title 18 of the U.S. Code is currently in force. Thus, according to this act, criminal liability is provided for trade in stolen or counterfeit means of access that can be used to obtain money, goods, or services (Law 4/26, 2013). To combat such offenses in the United States in 2016 adopted the National Cybercrime Plan and Presidential Policy Directive-41 (PPD-41), which defines the Federal Bureau of Investigation (FBI) a key role in combating cyber threats (Lapta, 2017).

As for the European Union, the EU Cyber Security Strategy was adopted in 2013, covering various aspects of cyberspace, including the internal market, justice, domestic and foreign policy. Moreover, it is worth to note the problem of corruption in this sphere. To prevent this problem, UN Convention against Corruption (United Nations, 2003) was adopted in New York on October 31, 2003. It establishes the necessary international legal framework to combat corruption offenses, in particular, identifies vectors of theoretical and practical developments in combating corruption (Kolomoiets, Tkalych, Melnyk, Panchenko, & Tolmachevska, 2021).

The shortcomings of the system for combating digital payment systems and cryptocurrencies in the EU member states are the lack of a single European system for responding to cyberattacks, differences in cybersecurity standards in different countries, low level of information exchange on cyber incidents between member states, etc. (Petrovsky, & Livchuk, 2019).

In 2015, France adopted a National Information Security Strategy. It aims to support the transition of French society to digital technologies and to address the new challenges posed by the changing use of digital technologies and the threats posed by them. It identifies five areas of work: ensuring state sovereignty; effective response to malicious actions in computer systems and networks; informing the general public; transformation of information security into a competitive advantage of French enterprises; increasing the influence of France in the international arena (Bilobrov, 2020). In 2008, the two special services of the Central Directorate of General Intelligence and the Directorate of Territorial Surveillance were merged. As a result of their unification, the Central Directorate of Internal Intelligence was created, one of the functions of which is the fight against cybercrime (Orlov, & Onishchenko, 2014; Shulga, 2013).

In the United Kingdom, the Organized Crime Agency has been set up to fight cybercrime, which includes the Cybercrime Unit. It should be noted that offenses related to the misuse of computer technology are punishable in the UK, imprisonment for a term of 10 years (Orlov, & Onishchenko, 2014).

In Germany, the fight against cybercrime is carried out by the Federal Criminal Police, as well as the National Center for Cyber Defense, which is responsible for the timely detection and prevention of hacker attacks (İCT NEWS, 2011).

If we talk about cryptocurrency as an object of civil rights, liability for offenses related to its operation can be considered by analogy with the mutual liability of the bank and the depositor. Civil liability arises in case of late crediting to the account of funds received by the client, their unreasonable write-off by the bank from the client's account or violation by the bank of the client's order to transfer funds from his account, the bank must immediately after detecting the violation credit the appropriate amount to the client's account or the appropriate recipient, pay interest and reimburse damages, unless otherwise provided by law (Article 1073 of the Civil Code of Ukraine Law No. 435-IV, 2003)). Therefore, it is a question of full responsibility for the commission by the bank of the specified infringements. However, it should be noted, that the legislation contains rules that indicate that, in some cases, the principle of full responsibility does not apply.

Given the above types of legal liability, it should be noted that such types as constitutional, administrative, international, financial liability are not used in the legislation of foreign countries.

Criminal liability as the most severe type of punishment in retrospect corresponds to the consequences of the offense in the field of payment systems and cryptocurrency, which is applied, in particular, in countries such as the United States, France, Britain, and Germany.

Conclusions

According to the results of the study, it is possible to draw the following conclusions:

- Offenses in the field of digital payment systems and cryptocurrencies should be classified as cybercrime. According to the theoretical analysis of legal liability in general and its practical side, which is manifested in the onset of criminal liability for violations in the field of digital payment systems and cryptocurrency, countries such as the United States, Britain, France, and Germany have a system for combating cybercrime has been created, which consists in the functioning of specialized bodies: the Federal Criminal Police and the National Center for Cyber Defense (Germany); the Cybercrime Unit of the Organized Crime Agency (UK); General Directorate of Internal Intelligence (France); Federal Bureau of Investigation, Financial Crimes Enforcement Network (USA);
- by analyzing the legal regulation of cryptocurrency in the United States, China, Russia, India, Denmark, Great Britain revealed the uncertain legal status of cryptocurrency, which makes it impossible to unify the international experience of liability in this area.
- security measures for users and owners of payment systems were identified: legal, administrative, moral-ethical, and physical.

For further research, it is important to analyze the issues of institutions that prevent and combat payment system offenses, as well as to analyze in more detail the issues of digital transformation of payment systems in the context of the Covid-19 pandemic.

Bibliographic references

Alekseev, S.S. (1999). Law: Alphabet - Theory - Philosophy: The Experience of Complex Research. Moscow: Statut. Recovered from http://lawlibrary.ru/izdanie20682.html

Azemsha, I.B. (2012). Features of formation of institute of legal responsibility in Ukraine. Journal of Kyiv University of Law, 2, 44-47. Recovered from http://kul.kiev.ua/images/chasop/2012_2/44.pdf

Bank for International Settlements. (2003). Committee on Payment and Settlement Systems. A glossary of terms used in payments and settlement systems. Recovered from https://www.bis.org/cpmi/glossary_030301.pdf

BBC. News Ukraine. (2018). Japan has the largest digital currency theft in history. Recovered from https://www.bbc.com/ukrainian/news-42847803

Berlach, N.A. (2012). Prospects for the development of positive legal responsibility in a democratic society. Forum of Law, 1, 77–81. Recovered from http://nbuv.gov.ua/UJRN/FP_index.htm_2012_1_13

Bilobrov, T.V. (2020). International experience in combating cybercrime by cyberpolice bodies. Law and society, 3, 96–102.

CryptoMagic. (2018). Legal regulation of cryptocurrency in Russia - what awaits us in 2018? Recovered from https://cryptomagic.ru/regulirovanie/kriptovalyuta-v-rossii.html

Dmitriev, Yu. A., Polyansky, I. A., & Trofimov, E. V. (2008). Administrative law of the Russian Federation. Moscow: Garant. Recovered from https://may.alleng.org/d/jur/jur489.htm

Economic truth. (2019). Hackers stole more than $ 40 million from the Chinese cryptocurrency exchange. Recovered from https://www.epravda.com.ua/news/2019/05/8/647630/

Eurasian Commission. (2017). Regulation of cryptocurrencies. Study of the experience of different countries. Recovered from http://www.eurasiancommission.org/ru/act/dmi/workgroup/Documents/digest/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%20%D0%B2%20%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B0%D1%85%20%D0%BC%D0%B8%D1%80%D0%B0.pdf

Gashchin, V. (2021). Basic concepts, features and forms of civil liability. Ternopil: Ternopil Ivan Puluj National Technical University. Recovered from http://elartu.tntu.edu.ua/bitstream/123456789/13764/2/VseukrStud_20121v2_Hashchin_V-Osnovni_poniattia_osoblyvosti_134.pdf

Golubeva, N. Yu. (2017). Cryptocurrencies: legal nature and regulation. Judicial-legal newspaper. Recovered from https://sud.ua/ru/news/blog/110210-kriptovalyuty-pravovaya-priroda-i-regulirovanie

Grin, O.D., & Donchenko, O.I. (2015). Criminal liability as a kind of legal responsibility. Legal state, 19, 129-135. Recovered from http://nbuv.gov.ua/UJRN/Prav_2015_19_27

İCT NEWS. (2011). The National Cyber Defense Center opened in Germany today. Recovered from http://www.ictnews.az/read-561-news-3.html

Ivanenko, O.V. (2007). The essence of legal responsibility and the role of law enforcement agencies in its provision (doctoral thesis). National Academy of Internal Affairs, Kyiv. Recovered from http://www.lib.ua-ru.net/diss/cont/243974.html

Kharytonov, E., Kharytonova, O., Kolodin, D., & Tkalych, M. (2020). The Covid-19 Pandemic and the Rights of the Individual in Terms of Private and Public Law. Ius Humani. Law Journal, 9(2), 225-250. Recovered from https://doi.org/10.31207/ih.v9i2.253

Kolomoiets, T., Tkalych, M., Melnyk, P., Panchenko, B., & Tolmachevska, Y. (2021). Combating Corruption in Sport: Legal Aspect. Retos, 41, 746-755. Recovered from https://recyt.fecyt.es/index.php/retos/article/view/86975

Kokkola, T. (Ed.). (2010). Payments, securities and derivatives, and the role of the eurosystem. Frankfurt am Main. European Central Bank. Recovered from https://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf

Koverznev, M.S., & Koverzneva, G.P. (2016). Responsibility in International Law. Almanac of International Law, 13, 49-56. Recovered from http://inlawalmanac.mgu.od.ua/v13/8.pdf

Koziy, V. (2018). Responsibility for illegal seizure of cryptocurrency in Ukraine. Scientific Journal of the National Academy of Prosecutors of Ukraine, 2, 69-82. Recovered from http://www.chasopysnapu.gp.gov.ua/ua/pdf/2-2018/kozij.pdf

Kunytskiy, O. (2021). India plans to ban cryptocurrencies. Forbes. Recovered from https://forbes.ua/ru/news/indiya-planue-zaboroniti-kriptovalyuti-zakonoproekt-peredbachatime-kriminalnu-vidpovidalnist-za-mayning-torgovi-operatsii-i-volodinnya-kriptoaktivami-reuters-15032021-1160

Lapta, S.P. (2017). FBI in the fight against cybercrime. Kharkiv: National Academy of Internal Affairs. Recovered from http://univd.edu.ua/science-issue/scientist/78

Law 4/26, Computer Crimes Law. Chief Information Security Officer, Texas, USA, 2013. Recovered from https://security.utexas.edu/policies/computercrimes

Law No. 435-IV, Civil Code of Ukraine. Bulletin of the Verkhovna Rada of Ukraine, Kyiv, Ukraine, January 16, 2003. Recovered from Recovered from https://zakon.rada.gov.ua/laws/show/435-15#Text.

Lipinsky, D.A. (2004). General theory of legal responsibility (doctoral thesis). Samara Humanitarian Academy, Saratov. Recovered from https://www.dissercat.com/content/obshchaya-teoriya-yuridicheskoi-otvetstvennosti

Lukyanets, D.M. (2004). Typology of legal responsibility. Legal Ukraine, 3, 4-10.

Musatkina, A.A. (2006). Legal relationship of financial responsibility. Jurisprudence, 3, 100-107.

Onishchenko, N.M. (2008). Legal responsibility: theoretical analysis and practical measurements. State and Law. Jurid. and flight, 42, 3-11. Recovered from http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=S&I21DBN=REF&P21DBN=REF&S21FMT=JwU_B&S21ALL=%28%3C.%3EU%3D%D0%A500

2.8$%3C.%3E%29&Z21ID=&S21SRW=dz&S21SRD=DOWN&S21STN=1&S21REF=10&S21CNR=20

Orlov, O.V., & Onishchenko, Yu. M. (2014). Generalization of the international experience of creating a state system of prevention and prevention of crimes on the Internet. Theory and practice of public administration, 2, 212-219. Recovered from http://nbuv.gov.ua/UJRN/Tpdu_2014_2_32

Perma.cc. (2018). Advarsel mod virtuelle valutaer (bitcoin m.fl.). Recovered from https://archive.org/details/perma_cc_UZ2E-G7S7

Petrovsky, O.M., & Livchuk, S.Yu. (2019). Problems of combating cybercrime: international experience and Ukrainian realities. A young scientist, 12(1), 55–59.

Popov, V. (2017). What is a "cryptocurrency"? Radio Svoboda. Recovered from https://www.radiosvoboda.org/a/details/28742278.html

Pyrih, S.O. (2008). Payment systems. Kyiv: Center for Educational Literature. Recovered from https://www.studmed.ru/pirg-so-platzhn-sistemi_305a094.html

Rabinovich, P.M. (2007). Fundamentals of the general theory of law and the state. Lviv: Krai. Recovered from https://lvivpravo.at.ua/_ld/3/312__.-2007-_____-2.pdf

Romanyuk, Y. (2019). Financial responsibility as a category of financial law. Entrepreneurship, economy and law, 2, 231-235. Recovered from http://pgp-journal.kiev.ua/archive/2019/12/44.pdf

Serdyuk, I.A. (2010). Fundamentals of the theory of law enforcement relations. Dnepropetrovsk: Lira LTD.

Serdyuk, I.A. (2011). Methodological analysis of modern interpretations of the concept of "legal responsibility". Bulletin of the Ministry of Justice of Ukraine, 1, 30-35. Recovered from http://nbuv.gov.ua/UJRN/bmju_2011_1_6

Shemelynets, I.I. (2017). On the question of classification of types of legal liability. Transcarpathian legal readings. Irpin: Dumka. Recovered from https://dspace.uzhnu.edu.ua/jspui/handle/lib/13419

Shulga, M.V. (2013). Features of legal responsibility in land law. Kharkiv: National Academy of Sciences of Ukraine. Recovered from https://dspace.nlu.edu.ua/handle/123456789/7200

Skakun, O.F. (2001). Theory of State and Law. Kharkiv: Consum. Recovered from http://www.dut.edu.ua/uploads/l_948_39072050.pdf

Spindler, J.E., & Summers, B.D. (1994). The Central Bank and the Payment System. The Payment System: Structure, Governance, and Control of the IMF. Washington: Lei.

Tchaikovsky, J.I. (2006). Payment systems. Ternopil: Carte Blanche.

Tkachenko, Yu. V. (2013). Features of constitutional and legal responsibility Law Forum, 3, 652-656. Recovered from https://dspace.nlu.edu.ua/bitstream/123456789/5151/1/Tkachenko.pdf

United Nations. (2003). Convention against Corruption. Retrieved from https://www.unodc.org/unodc/en/treaties/CAC/.

Usoskin, V.M., & Belousova, V.Yu. (2010). World trends and development of payment systems. Money and Credit, 11, 39-48. Recovered from https://www.imemo.ru/publications/info/global-trends-payment-systems-development

Vovchak, O.D., Shpargalo, G.E., & Andriykiv, T. Ya. (2008). Payment systems. Kyiv: Knowledge.

Yushchenko, V.A., Savchenko, A.S., Tsokol, S.L., Novak, I.M., & Strakharchuk, V.P. (1998). Payment systems. Kyiv: Lybid.

Zayats, R. Ya. (2012). The concept and signs of administrative responsibility. Scientific notes of Lviv University of Business and Law, 8, 17-20 Recovered from http://nbuv.gov.ua/UJRN/Nzlubp_2012_8_6

Zaychuk, O.V., & Onishchenko, N.M. (Eds.). (2008). General theory of state and law. Kyiv: Jurinkom Inter.