Electronic Money and Payments as Means of Committing Crimes

Andrii A. Vozniuk¹
Andrii V. Savchenko²
Tetiana Yu. Tarasevych³
Olexandr O. Dudorov⁴
Olga A. Klymenko⁵

¹Assoc. Prof., National Academy of Internal Affairs, Kyiv, Ukraine
²Prof., National Academy of Internal Affairs, Kyiv, Ukraine
³Dean, Kyiv University of Law The National Academy of Sciences of Ukraine, Kyiv, Ukraine
⁴Prof., Luhansk State University of Internal Affairs named after E.O. Didorenko, Sievierodonetsk, Ukraine
⁵Interagency Scientific and Research Centre on Problems of Combating Organized Crime under the National Security and Defense Council of Ukraine, Kyiv, Ukraine

DOI: https://doi.org/10.36941/ajis-2020-0069

Abstract

The article deals with the main problems of criminal characteristics of electronic money and payments as instruments of crime. The article reveals the economic and legal nature of electronic money (e-money). The features of e-money and its relation to electronic payments are identified. It is proved that intensive development of the IT sector results in an increasing replacement of cash by cashless methods of payment, and e-money is required for making payments online. E-money is previously created in all cases where they are stored on an electronic device and are used as means of payment, therefore they significantly reduce the level of abuse against property. Criminals in the real estate leasing sector use it as a tool when they commit cybercrime - a new place that has been transformed into a powerful source using for crime. Particular attention in this article is paid to the criminal characteristics of electronic money as an instrument of crime. Electronic money has been updated to account for a significant number of offending characters, while these crimes operate in free currency from a non-supported market and move to electronic services, they are used, and may be joined by warehouse resources, which require a criminal law level. It also indicates that e-money is being received by its billing service, and then can be exploited by attackers to trick owners who have already participated in their work. Through this process, using e-money and electronic payment is almost legal and covers the concept of legality. It is disclosed that the main complexity in detecting malicious tools creates electronic money, which makes it difficult to track the traces of such crime, which uses its delays in cyber space. The author also reveals an accurate view of electronic money resources, such as what is more likely to be abused, which is an additional element of criminal execution qualification.

Keywords: electronic money, electronic payments, cryptocurrency, cybercrime, tools of criminals, criminal characteristics
1. Introduction

The current state of development of IT technologies demonstrates a high level of opportunities for their use in absolutely all spheres of life. This is why online payments are becoming an integral part of the financial sector, and the use of electronic money is accelerating economic processes. E-money is transformed into a powerful investment, payment and wealth redistribution tool. Moreover, the fact that e-money has no material form and in fact only means a price equivalent on the Internet, complicates making it safe by the owner in the context of preventing the unlawful loss of its ownership. Various electronic wallets, payment systems, etc. - all this only creates the illusion of spreading the legal possession of e-money. In fact, they are stored on special platforms and services, and payments are made online far from the boundaries of a person’s physical influence on his property in the form of such payment instruments. This complicates its protection and opens opportunities for fraud with it, misappropriation by third parties. At the same time, the distance and depersonalization of the owner of e-money increasingly makes it a powerful tool and a means of committing crimes. The complexity of the trace examination for electronic trace tracking, as well as the extreme remoteness from the place of commission or preparation of crime in case of the use of e-money makes it a powerful and extremely dangerous means of committing a crime. At the same time, it is necessary to pay attention to the fact that the use of e-money can be an additional qualifying sign of a criminal act that affects the way of committing and the nature of the objective aspect of the crime. Therefore, in order to find out the criminal nature of the use of e-money and payments as means of committing crimes, it is necessary to study:
- the nature, meaning and legal regime of e-money and electronic payments;
- the mechanism of using e-money as a means of committing criminal offenses;
- legal features of regulating the circulation of e-money and the relations built around these payment instruments as separate subjects of relations.

Thus, it is planned to answer the question of how e-money and payments serve as means of committing crimes and what are the ways of countering it. It is also important to provide a criminal-law characteristic of e-money as a potential qualifying feature of a criminal act that affects the final classification of the crime itself.

2. Literature Review

Modern research in the field of legal justification for the use of e-money is reduced to finding ways to minimize their use as a means of committing crimes. Researchers believe that e-money, like electronic payment methods, can be used as tools or objects of crime.

In particular, Armey, Lipow and Webb (2014) investigated the effect of electronic financial payments on crime as a mechanism to increase the secrecy and fouling the trail, due to the electronic nature of means of payment.

Cabrera (2015), Drozdov, Drozdova and Gerelyuk (2018) investigated the nature of Bitcoin as a means of crime, as well as the object to which criminal intent is directed.

Shymon (2015) exploring the nature of electronic money as an object of ownership significantly expands the criminological capabilities of law enforcement agencies. The results of his research made it possible for Crosby et al. (2016) to determine the criminological and criminalistic features of the crime prevention process using Blockchain technologies. Karchevskyi (2017), Grynko (2016) and others investigated the main problems of the criminal law regulation of the use of virtual currency for criminal purposes.

Kirschbaum et al. (2013), Teicher (2018) studied the problems of international legal protection of e-money from criminal violations. They also developed ideas about the need for international cooperation in the field of crime using virtual money.

Nykyforchuk (2018) and Riadinska (2018) analyzed the nature of electronic money as a tool in the field of financial and banking crimes. An important contribution to the development of the
forensic substantiation of methods and tactics in investigations of crime committed by means of electronic money was made by Dorokhina (2016), Berzin and Kutsevich (2013) and others.

3. Methodology

To achieve the result of the study, it was conducted using the synthesis of different methods of scientific knowledge. Particularly important are system analysis, methods of hermeneutics and synthesis, which gradually revealed the features of e-money and electronic payments as means of committing crimes. The final formulation of the criminal law regime of e-money and electronic payments as means of committing crimes is largely due to the formal-logical method, the method of hermeneutics and the like. At the same time, the research algorithm implies the gradual realization of the following scientific objectives: first of all, it requires the determination of the economic and legal nature of electronic money and payments; second, explore the possibilities of using electronic money and payments for criminal purposes; third, it is necessary to establish its unique features that formulate a specific criminal-law characteristic of electronic money as means of committing crimes.

The process of collecting data on the subject of the study - the criminal law characteristics of electronic money - involves the study of the main international legal acts in the field of countering the use of electronic money as an instrument of crime. Special attention will be paid to the international legal regulation of cooperation in efforts to combat cybercrime. The reliability of the data is determined by the relative stability of international instruments. At the same time, it is necessary to understand that the dynamics of the development of virtual technologies and electronic payments with their use significantly increase the variability of the methods of committing crimes.

Such trends are difficult to quickly foresee and ensure in terms of legislative support. At the same time, progressive criminal law research and theories will help significantly expand the perception of electronic money as a means of crime, not just as an object of crime. This will allow the formation of an appropriate platform for further knowledge and the development of forensic techniques to counter such crimes and their detection.

4. Analysis

According to the 2001 Budapest Convention on Cybercrime (Council of Europe, 2001), the following types of cybercrime are established:

1. Crimes against the confidential information and personal data, offenses against the confidentiality, integrity and availability of computer data and systems, including: illegal access; illegal interception; data and system interference; unlawful use of devices;
2. computer-related offenses, including: computer-related fraud;
3. content-related offenses;
4. offenses related to infringements of copyright and related rights.
5. dissemination of racist and xenophobic material through computer systems.

On October 29, 2002, the European Central Bank published a report on Virtual Currency Schemes (European Parliament, 2009), which examined the relevant economic and legal aspects of Bitcoin and electronic money systems, and noted that the 2009 European Directive regulates the use of electronic currencies to harmonize payment methods, increase competition and facilitate market access. This directive demonstrated the possibility of enshrining the following practice – issuing currency in electronic form in exchange for funds to be used as means of payment and identification of persons (Drozdov, Drozdova, & Gerelyuk, 2018). According to European Banking Authority (2013) (EBA), the EU regulatory authority responsible for advising EU institutions on banking, regulating electronic money and payments, has rightfully issued a warning on the risk of transactions such as the purchase, transfer of funds or trading in virtual currencies. The EBA has stated that, because Bitcoin is not regulated, consumers are not protected and risk losing their money, while being responsible for tax evasion when using virtual currencies (European banking authority, 2013). This
opens up a new opportunity to pursue criminal intent through electronic money - tax avoidance and fraud.

The European Union (EU) has not adopted specific legislation on the status of Bitcoin as a currency, although the ECB believes that Bitcoin may fall within the definition of electronic money provided in Directive 2009/110/EC. This Directive defines electronic money on the basis of three criteria: (a) storage in electronic form, (b) issuance upon receipt of funds, and (c) acceptance as a means of payment by a non-issuing legal entity or individual. The report states that Bitcoin meets the first and third criteria, but not the second. Other experts suggest that Bitcoin falls within the definition of payment services provided in Directive 2007/64/EC (European Parliament, 2009). This approach reduces the potential for regulatory impact not only on Bitcoin but also on other electronic money as they are converted to it, as well as other cryptocurrencies, which are however devoid of the unambiguous legal status of means of payment and electronic money. All this leads to the fact that electronic money becomes an important feature as a crime tool, if these crimes occur in the field of withdrawal of currency from the market without taxation and its transformation into electronic means of payment, which can be used to solve much more complex problems of criminal nature.

When identifying electronic money and payments as means of committing crimes, it is necessary to draw attention to an interesting fact - current Ukrainian law does not contain a clear definition of electronic money. That is, its status is undetermined, although the legislation contains separate definitions and categories that give an idea of the nature of the relationship that occurs through or with the use of e-money.

The Regulation on electronic money in Ukraine, approved by resolution of the National Bank of Ukraine defines “the use of electronic money as relations between the issuer, operator, agents, traders and users in the issue, distribution, settlement, exchange, repayment of electronic money and replenishment of electronic devices with electronic money” (Legislation of Ukraine, 2010). The Law of Ukraine “About Payment Systems and Funds Transfer in Ukraine” contains the definition of a means of electronic payment as a payment instrument, which enables its holder to obtain information about the funds owned by the holder and initiate their transfer by means of a payment device (Legislation of Ukraine, 2001). Such definitions indicate that the legislator understands e-money rather as a unit of value, as well as means of payment, as indicated by the wording “electronic money repayment”.

Thus, electronic money acts as a means of payment and the subject of electronic payments, therefore it can be argued that electronic payments in case where e-money is their subject acting as a derived relationship with regard to the provision and execution of the client’s payment order. Although not always electronic payments are made with e-money. Thus, the transfer of funds, which the client of a financial institution places on his account, by electronic means of payment cannot be considered as electronic payment by electronic money, since this money had material realization before it got to the client’s electronic account.

Cryptocurrency is physically a set of data generated on the basis of a complex mathematical algorithm. For example, the Bitcoin payment system is organized on a peer-to-peer (p2p, equal) basis, records for all transactions are distributed among all members of the system, there is no single coordination center of the network, information about all transactions made is freely available. This method of organizing the payment system provides almost absolute protection of transaction information, makes the system stable and reliable (Karchevskyi, 2017). But, despite the fact that electronic money and cryptocurrency act as means of payment, the latter are the so-called “non-fiat money”, that is, they do not express a measure of value, but have some value themselves. Their value as a payment instrument is not secured by anything, and there is no regulator that determines the exchange rate of that currency. Instead, a measure of the value of a cryptocurrency, in particular Bitcoin, is determined by market through establishing demand and supply for them.

But the court practice that has already emerged in Ukraine demonstrates an interesting approach of courts that determine Bitcoin as a monetary surrogate that has no material expression and cannot be considered to be a full-fledged electronic means of payment. Thus, in the Decision of the Darnytskyi District Court of Kyiv (Unified State Register of Judgments, 2016b), as well as in the
Resolution of the Court of Appeal of Kyiv (Unified State Register of Judgments, 2016a), in the same case, it was established that according to Letter from the National Bank of Ukraine 08.12.2014 No. 29-208/72889 concerning the attribution of transactions with virtual currency/cryptocurrency – Bitcoin – to foreign currency trading transactions, as well as the existence of grounds for crediting foreign currency received from Bitcoin sales into a foreign currency current account of an individual, indicated that the issue of Bitcoin virtual currency has no security and legally bound persons under it, is not controlled by the government of any country. So, Bitcoin is a monetary surrogate that does not have a real value security. Buying or selling Bitcoin for US dollars or other foreign currency has the features of functioning of the so-called “financial pyramids” and may indicate potential involvement in the carrying out of suspicious transactions in accordance with the legislation on counteracting money laundering. Thus, the court draws attention to at least the possibility of using cryptocurrency, and therefore electronic money, to carry out “suspicious transactions”. This viewpoint demonstrates the potential for the use of electronic money not only as a means of suspicious transactions but also as a tool for criminal activity.

5. Results

Interesting is the fact that the use of electronic money significantly increases the possibility of their identification as a tool of committing crime. For example, in case of crimes related to illicit gain, money has traditionally been regarded as the embodiment of the object of the crime – illicit gain. At the same time, if we consider electronic money as the object of such a crime, they clearly act as a means of obtaining undue benefits, since in their pure form, their presence in the relations between the party committing the crime and the party which gives undue advantage does not mean that the official receives any benefit. Only using electronic money as a means of payment and using it to make purchases or pay for services results in a person receiving an undue benefit.

Electronic money “emerged as a reaction of the banking services market to the problems of payment card security and the need for a new, more flexible, convenient and secure payment tool to pay for goods and services via the Internet” (Shymon, 2015, pp. 13-16).

Berzin and Kutsevich (2013), determine the following substantive features of electronic money: “by their legal nature, electronic money is a monetary obligation of a particular person carrying out its issue, that is, the debtor’s obligation to pay a certain amount of money to the creditor in accordance with the civil legal transaction (contract) and on certain grounds stipulated by the legislation of Ukraine; their tangible expression is a unit of value stored on an electronic device in the form of a specific technical symbol; electronic money is accepted as a means of payment” (p. 14). Therefore, the use of electronic money is possible solely as a means of payment, although in some cases and countries, electronic money, more exactly some of their forms - cryptocurrency - is recognized as a commodity that complicates their criminal law characteristics as a means of committing criminal offenses.

Drozdov, Drozdova and Gerelyuk (2018) draw attention to the fact that such practice is already known in the practice of criminal prosecution, where in Case # 759/1642/17 and in Criminal Proceedings # 12017100080006346 of July 19, 2017 the law enforcement authorities formulate a position regarding the ban on the issue and circulation of Bitcoin cryptocurrency in the territory of Ukraine, as payment organizations of payment systems, participants of payment systems and operators of payment infrastructure services have the right to operate in Ukraine only after their registration by entering information about them in the Register. On November 30, 2017, the National Bank of Ukraine, the National Securities and Stock Market Commission and the National Financial Services Regulatory Commission made an official statement that the complex legal nature of cryptocurrencies does not allow them to be recognized either as cash or as currency and a payment instrument of another country, or as monetary value, electronic money, securities, or monetary surrogate.

In general, it is traditionally believed that crimes with the use of electronic money are
committed of illegal activity, where they act as a means of achieving criminal interests: the acquisition of certain property whose circulation is prohibited or restricted; payment for services and goods that are directly related to or form an integral part of the criminal result achieved.

In Luxembourg, SnapSwap is licensed to perform Bitcoin payment and exchange transactions and to use them as a tool for transferring funds using current cryptographic technologies and Internet protocols. The German Treasury also resolved that Bitcoin is “private money” through which a wide range of multilateral clearing operations can be conducted (Kirschbaum et al., n./d.). However, given the increased risk and intensity of cybercrime, it seems logical that enshrinement of the possibility of using electronic money at the legislative level, and in particular the cryptocurrency for settlements, demonstrates the objectivity of covering them by the criminal law regime, especially in the context of cybercrime.

It is interesting that in her research Riadinska (2018) also draws attention to the fact that in the EU countries the right to issue electronic money was granted exclusively to banks and credit institutions (Austria, Germany, Spain, Portugal); ban on simplified regime of functioning of electronic money issuers (Italy, Lithuania); requirements for prudential regulation have been toughened (Greece, Sweden). All this means that violations of the electronic money regime, given the existing restrictions on their use, can also have the features of criminal activity, especially if the stability of the financial sector is thus harmed (European Commission, 2006; Bank for International Settlements, 2004).

Dorokhina (2016) also notes that electronic money can be attributed to a special type of non-cash funds, and therefore they can be the object of crime against property. Although it is one of the types of virtual financial instruments, all features of the object of crime against property are inherent in it, namely: physical features are characterized by the ability to measure them in certain units, they can be traded on an electronic exchange, that is, such an item can be withdrawn; in terms of socio-economic component, they have a certain exchange and consumption value, and from the point of view of a legal feature, it is alien property for the culprit (Dorokhina, 2016). In turn, Armey, Lipom and Webb (2014) argue that access to electronic payments can reduce crime rate. Researchers have found that there is a negative and significant statistical link between access to electronic payments and the frequency of economic crimes, such as robbery, while electronic transactions have little effect on reducing the frequency of non-economic crimes such as murder and rape (Armey, Lipom & Webb, 2014). However, this conclusion is more relevant for crimes related to physical violence, robbery, etc., but property crimes committed with the use of electronic money can sometimes even be unsolved on time, due to the specific criminal law regime and the peculiarities of the use of electronic money.

Thus, it can be argued that the development of IT technology contributes to a widespread use of electronic means of payment. Considering the fact that cybercrime is characterized by a relatively high level of anonymity of criminals and the ability to confuse traces and investigations, we conclude that crimes against electronic money are committed much more often because of the relative ease of taking possession of it. Instead, e-money crimes are on the rise. In fact, cash is being replaced by cashless means, and electronic money continues to function as a means of payment. By its legal content, electronic money is a monetary obligation of a certain person who executes their issue, that is, a debtor’s obligation to pay a creditor a certain amount of money in accordance with a civil transaction (contract) on certain grounds provided by the legislation of Ukraine (Nykyforchuk, 2018).

6. Discussion

In our opinion, electronic money is used as a means of committing a crime for the same criminal purposes as conventional traditional money, as a means of payment or as a source of improper benefit, etc. The complexity of using electronic money as a means of committing crime is revealed through the specifics of the features and characteristics of electronic money as special payment instruments:

- first, electronic money is used as a means of payment, and therefore creates a proper
ownership link between the person who disposes of it and the amount of money expressed in the respective payment instrument;
- second, electronic money, by virtue of its complex legal status, especially cryptocurrencies, acts as a means of tax evasion and a way for other frauds in the financial market, as well as a means of manipulation in the financial sector, when acting as a commodity;
- third, electronic money is a means of payment, and therefore the payment of services or goods with it can be used by the offender to double on traces of his/her involvement in a particular crime. In such circumstances, the very process of using electronic payments is legal;
- fourth, electronic money is an intangible form of money, has its value equivalent, and can be exchanged for tangible means of payment, that is, converted into tangible currency, and this gives another opportunity to use electronic money as a means of committing crimes.

Instead, American experts, McMahon (2013), Armey, Lipom and Webb (2014) and others believe that there is a significant and strong relationship between greater access to electronic financial transactions and reduced economic crime rate. Armey, Lipom and Webb (2014) conclude that broad access to electronic financial transactions has the potential to greatly enhance personal security. New electronic payment technologies can solve many industry and trade problems, leading to a significant improvement in living standards. The approach of Wright et al. (2014) and some other researchers that reducing cash flow leads to a reduction in financial crime rates is of interest. Electronic money enhances the transparency of financial transactions, and creates the necessary effect on the stability of payments, since the devices on which electronic money is accumulated and stored belong to the same institutions that conduct electronic payments. However, we cannot agree with this view of the scholars, since there are at least two contradictions in the use of electronic money as payment instruments:
- First, electronic money can be used quite legally, but the purpose of such use may be to avoid tax. For example, the settlements, transfer or conversion of such money is made according to all rules and regulations of national law. However, if such a conversion was made through the acquisition of Bitcoin – in many countries this process makes it possible to use Bitcoin for tax evasion, while the tax burden and liability for the failure to pay remain with the entity/individual;
- Second, the use of electronic money leads to an increase in cybercrime rate in the money acquisition through fraud, while electronic money is acquired either through the use of harmful payment systems and mechanisms, or through breaking of the electronic money storage system’s security mechanisms.

Weibing (2011) points out that the intensification of the use of electronic money has led to a mirror intensification of relations in the sphere of money laundering. The scholar notes that money laundering is realized through e-commerce transactions, provided quick and frequent sales of electronic money and its conversion through the online payment platform. The “self-sale from purchase” commercial account allows transactions consisting of many numbers of payment network accounts united in the process of circulation and gradual laundering of electronic money through (often fictitious) e-commerce transactions. Therefore, e-money laundering is becoming a systemic crime in the financial sphere with the widespread use of the means of electronic payment and e-commerce, which is difficult to track and control.

However, in terms of criminal law characteristics, the additional difficulty arises from the fact that the use of electronic money can at the same time act as an element of qualification of a criminal act, as well as associated with the use of technologies that are difficult to identify and do not subject or partially subject to forensic investigation.

Teicher (2018) claims that electronic money laundering, also known as transaction laundering, is the most common method of money laundering. The principle is simple: an unknown online business uses a seller’s approved payment credentials to process credit card transactions for unknown products and services. For example, there is a common Airbnb scheme. Fraudsters use stolen credit
cards to launder dirty money through the accomplices of Airbnb hosts they meet in backstreet online forums. Once the Airbnb reservation transaction is processed, none is actually left in the advertisement; instead, both parties split the payment and create fake end-of-stay reviews to close the transaction cycle (Teicher, 2018). In this particular example, electronic money and payments act as a means of committing money laundering crimes through the conversion of electronic currency into real money through fictitious electronic transactions.

According to the Center for Strategic Estimates and Forecasts (2005), it is increasingly becoming one of the most common types of financing for the criminal activity of persistent criminal groups and is one of the areas of support for their activity. Against this background, the issue of ensuring the accuracy of the criminal law characteristics of electronic money as a means of committing crimes is topical.

In this context, Grynko (2016) states that “difficulties in obtaining an evidence base; transnational nature of criminal activity; imperfect procedure of international cooperation – all this demonstrates the impossibility of solving the problem at the national level” (p. 110). If national law defines electronic money as a means of payment and the law of another country - as a commodity, a situation is created that renders economic and any other activity regarding the use of such money impossible. Therefore, its use as a tool of committing crimes facilitates criminal activity and complicates the process of qualifying the crime.

“Electronic money is used by criminal groups to carry out a variety of criminal operations. Decentralized electronic money does not depend on central government or financial institutions, but the process of transacting them becomes complicated due to the development of new technologies, which is an advantage for criminals, and vice versa presents difficulties for law enforcement activities” (Cabrera, 2015). Such a conclusion calls for intensifying of, first of all, international cooperation in the field of the least legal certainty of the status of electronic money and their criminal law characteristics as instruments of crime.

But according to Crosby et al. (2016), the very use of blockchain technologies will eventually lead to the minimization of crimes in the sphere of circulation and the use of electronic money. Although the analysis of the research results of scholars shows that the blockchain allows money laundering and their legalization, although it is significantly complicated and it renders sometimes impossible to convert electronic money into nominal.

7. Conclusion

The peculiarities of the legal status of the subjects of relations in the sphere of the use of electronic money, as well as the peculiarities of the legal regime of electronic money, has an effect on its criminal characteristics. So, we come to the logical conclusion that, from the point of view of forensic science, electronic money acts a means and instrument of crime when they are used as an auxiliary tool of criminal activity. At the same time, they have a number of forensic and criminal procedure features, which significantly influences the process of solving crimes committed with the help of electronic money:

- First, the complexity of tracking crimes committed through electronic money is due to a wide range of possibilities of doubling traces in cyber space. The trasology of electronic money is greatly complicated by the complexity of computer code;
- Second, the use of electronic money as a means of committing crimes is an additional element in the qualification of criminal activity. The nature and features of the objective side of the crime depend on the volume and other aspects related to the use of electronic money for committing crimes;
- Third, electronic money is most often the instrument of committing crimes that are aimed at money laundering, tax evasion, fraud by electronic payments. At the same time, the use of electronic money objectively led to a reduction in the level of crimes against property, since the intangible form of electronic money reduces the risks of its misappropriation;
Fourth, the use of electronic money as a tool for committing crime is identified by the features of cybercrime, which has relevant effects determining the specifics of investigating such crimes.

In general, current theorists and practitioners regarding the criminal law qualification of the regime and the legal status of using electronic money and payments as tools of committing crimes noted the complications of the crime solution process, since the establishment of the fact of its commission is quite complex and lengthy.

References


