CRYPTOCURRENCIES: DEVELOPMENT, FEATURES AND CLASSIFICATION

Abstract. The advent of cryptocurrencies and rapid growth of crypto-networks heralded a new era in evolution of financial relations. The main goals achieved by introduction of cryptocurrencies included: a) removal of the third party (the government, banking and financial institutions) from transactions between the parties to a transfer; b) anonymity of the parties; c) transaction security. The governments of various countries of the world have a different stance as regards the use of cryptocurrencies, and in some cases, they consider this medium of exchange illegal. The transnational nature of transactions involving cryptocurrencies and the absence of physical borders for these transactions complicate legislative regulation of the circulation of cryptocurrencies in Ukraine.

The use of cryptocurrencies has significant effect on the economies of Ukraine and other countries of the world due to easy dissemination and popularity of this technology and the growing capitalization of cryptocurrencies. The exchange of cryptocurrencies into fiduciary money and the possibility of gaining substantial profits on a cryptocurrency exchange due to high volatility of cryptocurrencies necessitate development, as soon as possible, of approaches to legislative regulation of both terminological apparatus related to circulation of cryptocurrencies and the exchange transaction procedures, profit taxation, etc. Considering the multisided nature of crypto-networks and the diversity of cryptocurrencies currently existing in the world (over 2000 variants as of today), classification of existing cryptocurrencies and definition of their features represents a contemporary task.

This article characterizes development of blockchain technology that serves as the basis for the functioning of cryptocurrencies, defines their characteristic features, positive and innovative concepts implemented with their advent. Cryptocurrencies were classified based on various criteria (issue type, network decentralization, limitation on issue, controllability of cryptocurrency issue, etc.), and two groups of features typical either for all cryptocurrencies or for their certain variants were proposed. It was proposed to define a cryptocurrency as a variety of e-money used as an alternative additional currency and circulated within global computer networks on the basis of blockchain technology that envisages asymmetrical encryption and the use of various cryptographic protection methods.

Keywords: bitcoins, blockchain, cryptocurrency issue, classification of cryptocurrencies, cryptocurrency, mining, regulation of cryptocurrency circulation.

Formulas: 0; fig.: 0; tabl.: 0; bibl.: 19.
КРИПТОВАЛЮТИ: РОЗВИТОК, ОЗНАКИ І КЛАСИФІКАЦІЯ

Анотація. Поява криптовалют і стрімкий розвиток криптомереж ознамenalви новий етап еволюції фінансових відносин. Основними цілями, які були досягнуті за рахунок запровадження криптовалют, стали: а) виведення третьої сторони (держави, банківських і фінансових установ) за межі операцій, що здійснюються між учасниками переказу; б) анонімність учасників; в) захищеність проведених трансакцій. При цьому використання криптовалют по-різному оцінюються урядами країн світу, а в окремих випадках їх вважають протиправними. Транснаціональний характер операцій із криптовалютами, відсутність фізичних кордонів, при їх здійсненні, обумовлює складність нормативного регулювання їхнього обігу на території України.

Використання криптовалют має суттєвий вплив на економіку України та інших країн світу, що обумовлено легким поширенням цієї технології, її популярністю та зростанням капіталізації криптовалют. Проведення обміну криптовалют на фідуціарні гроші, можливість отримання значного прибутку на криптобіржах через високу волатильність криптовалют зумовлюють потребу в якнайшвидшому розробленні підходів до нормативного регулювання як термінологічного апарату, пов’язаного із їхнім обігом, так і безпосередньо процедур проведення обмінних операцій, оподаткування отриманого прибутку тощо. Ураховуючи багатоплановість діяльності криптомереж, різноманітність наявних у світі криптовалют (наразі більше ніж 2 000 різновидів), актуальним є питання проведення класифікації наявних криптовалют, виокремлення притаманних їм ознак.

Охарактеризовано розвиток блокчейн-технологій, на основі якої функціонують криптовалюти, визначено її характерні риси, позитивні та інноваційні концепції, що були запроваджені з її появи. Проведено класифікацію криптовалют за різними критеріями (тип емісії, децентралізації мереж, обмеженості емісії, контрольованості випуску криптовалют та ін.) і запропоновано дві групи ознак, що притаманні або всім криптовалютам, або окремим їхнім різновидам. Запропоновано визначати криптовалюту як різновид електронних грошей, що використовуються як альтернативна додаткова валюта, обіг яких здійснюється у рамках побудованих глобальних комп’ютерних мереж із застосуванням блокчейн-технології, яка передбачає асиметричне шифрування та використання різних криптографічних методів захисту.

Ключові слова: біткоїни, блокчейн, емісія криптовалют, класифікація криптовалют, криптовалюта, майнинг, регулювання обігу криптовалют.

Формул: 0; рис.: 0; табл.: 0; бібл.: 19.
**КРИПТОВАЛЮТЫ: РАЗВИТИЕ, ПРИЗНАКИ И КЛАССИФИКАЦИЯ**

**Аннотация.** Появление криптовалют и стремительное развитие криптовалют ознаменовали новый этап эволюции финансовых отношений. Основными целями, которые были достигнуты за счет внедрения криптовалют, стали: а) вывод третьей стороны (государства, банковских и финансовых учреждений) за пределы операций, осуществляемых между участниками перевода; б) анонимность участников; в) защищенность проведенных трансакций. При этом использование криптовалют по-разному оценивается правительствами стран мира, а в отдельных случаях — считается противоправным. Транснациональный характер операций с криптовалютами, отсутствие физических границ при их осуществлении обусловливают сложности нормативного регулирования их обращения на территории Украины. Использование криптовалют оказывает существенное влияние на экономику Украины и других стран мира, что обусловлено легким распространением этой технологии, ее популярностью и ростом капитализации криптовалют. Проведение обмена криптовалют на фидуциарные деньги, возможность получения значительной прибыли на криптовалютных биржах из-за высокой волатильности криптовалют обусловливают потребность в скорейшей разработке подходов к нормативному регулированию как терминологического аппарата, связанного с их обращением, так и непосредственно процедур проведения обменных операций, налогообложения полученной прибыли и т. п. Учитывая многоплановость деятельности криптовалют, разнообразие существующих в мире криптовалют (сейчас более 2 000 разновидностей), актуальным является вопрос проведения классификации существующих криптовалют, выделения присущих им признаков. Охарактеризовано развитие блокчейн-технологии, на основе которой функционируют криптовалюты, определены их характерные черты, положительные и инновационные концепции, которые были введены с их появлением. Проведена классификация криптовалют по различным критериям (по типу эмиссии, децентрализации сетей, ограниченности эмиссии, контролируемости выпуска криптовалют и др.) и предложены две группы признаков, присущих или всем криптовалютам, или отдельным их разновидностям. Предложено определять криптовалюту как разновидность электронных денег, используемых как альтернативная дополнительная валюта, обращение которых осуществляется в рамках построенных глобальных компьютерных сетей с применением блокчейн-технологии, которая предусматривает асимметричное шифрование и использование различных криптографических методов защиты.

**Ключевые слова:** биткоины, блокчейн, эмиссия криптовалют, классификация криптовалют, криптовалюта, майнинг, регулирование обращения криптовалют.

Формула: 0; рис.: 0; табл.: 0; библ.: 19.

**Introduction.** Implementation of financial activity of the state occurs in various forms. It is always associated with the turnover of public funds, the mandatory participation of the state or a territorial community in these legal relationships.

Traditionally, within the framework of financial activity of the state there was a movement of fiduciary funds, the value of which is stipulated by the imperative order of the state to use them as a way of payment, and the issuer of which is the state. These relations are properly regulated, but with the advent of cryptocurrency in 2009 which is not emitted by the state but has the certain value, there are more and more issues regarding the regulation of their turnover and the role they can play in the financial activities of the state.

The transnational nature of the issue and the turnover of cryptocurrency, anonymity of transaction participants complicate the legal regulation of their use in different countries. The lack of a normatively-assigned terminology system is largely due to the complexity of crypto-networks, their decentralization, the special way of emission and the execution of transactions without the use of national payment systems. At the same time, the high volatility of this financial instrument allows crypto-market participants to earn significant amounts of money, while the mechanisms of their taxation are still not in the vast majority of countries in the world.
Currently, the main problem in conducting operations with cryptocurrencies is the legal uncertainty of the term «cryptocurrency», the lack of legal regulation of the methodology for accounting crypto-transactions between their participants, the unresolved procedure for determining the tax base when conducting transactions with cryptocurrencies by individuals and legal entities. In this article, was carried out the research of the background and origin of cryptocurrency, the classification is given as well, the obligatory and optional signs of cryptocurrency are singled out, and the peculiarities of their emission are described.

**Research analysis and problem statement.** Significant practices in the research of the designated theme were noted by D. O. Babin, I. V. Greevy, V. V. Korneev, I. A. Kotitsina, M. V. Tarasyuk, E. I. Trubnikov, O. Cheberyako, V. K. Shaydulin and others. At the same time, the novelty of the phenomenon of cryptocurrency and their transnational nature is due to the lack of proper legal regulation of their turnover in Ukraine.

**The purpose of the article** is to determine the economic aspects of the emergence of cryptocurrency, to classify their varieties, to distinguish common and distinct features of cryptocurrencies (according to their individuality, to form the proposals for the legal establishment of the term «cryptocurrency» in Ukraine.

**The result of the research.** The development of technologies leads to changes in many areas of public life. One of the most significant events that had a significant impact on the circulation of finance was the development and implementation of the Bitcoin system in early 2009, which operates on the basis of blockchain technology. Initially, the existence of Bitcoin system network was ensured only due to enthusiasts, but in the fall of 2009, the exchange of virtual currency was made on fiat money, and in 2010 — on real goods (the legendary pizza for 10,000 bitcoins) [1].

Blockchain Technology is a special structure for writing a transaction group in crypto-systems [2]. The transaction is considered completed and credible («confirmed»), when its format and signatures are checked, and when the transaction itself is grouped together with several others and written in a special structure — a block. Block content can be verified, since each block contains information about the previous one [3]. It is worth noting that the blockchain technology came with the bitcoin, but can be used separately as well. In accordance with the concept proposed by blockchain inventor (Satoshi Nakamoto), the basic principles of bitcoin are provided:

- security (each subsequent page- block depends on the previous one, so if someone wants to change the already «sealed» page data, he will also have to change the content and cipher of all subsequent pages, which is impossible due to the use of extremely stable crypto-algorithms);
- anonymity (none of the members of the group knows the personality of others, since even during the transfer of funds member sees only a set of numbers and letters — the address of the wallet in the bitcoin system);
- transparency (all members of the group have access to the database system, note the data of all money transfers occurring inside. Any transaction can be observed at any moment by each participant);
- decentralization (the database is stored in a certain place in a single copy, but in the form of a copy of each user who joined the system);
- security (after a certain time the place for records on a «sheet» (block) ends, then it «seal» with a unique encrypted code, agreed by all the participants, after which the entries on it can only be reviewed, but not changed) [3; 4].

Currently, Bitcoin, Ethereum and Ripple are among the top three of the most capitalized cryptocurrencies. Bitcoin (BTC) is the first of the created cryptocurrencies. [5] This cryptocurrency has the largest capitalization. During its existence, the exchange rate has grown to more than 20,000 US dollars (at the end of 2017) [6]. The basic feature of this cryptocurrency, like many others, is the possibility of separating bitcoin into small parts — the smallest unit of 10-8 bitcoin called «Satoshi.» An electronic payment between the two parties occurs without intermediaries and is irreversible. The system does not have a mechanism to cancel a verified transaction, just as no one can block or arrest funds, even temporarily, except for the private key owner [7].

Ethereum (ETH) — Crypto Currency released in 2015 on the basis of Ethereum technology, is the world’s leading programmable blockade. Unlike other blocking systems, Ethereum is
programmed, which means that developers can use it to create new types of applications that can control digital assets for creating new types of financial applications [8].

Ripple (XRP) — the internal cryptocurrency of the Ripple network launched in 2012. In turn, the Ripple network is used as a crypto exchange platform for payment systems, and is oriented on transactions with currency exchange without refunds [9]. In the Ripple network, users make payments between themselves using cryptographically signed deals denominated in currencies or internal Ripple (XRP) cryptocurrencies. For RIPP nominated in XRP transactions, Ripple can use an internal registry, and for payments expressed in other assets, the Ripple registry only records the amount of debt with assets presented as debt obligations [10].

In addition to the three most highly capitalized cryptocurrencies, about 2200 varieties have been released for this time. At the same time, not all cryptocurrencies are completely decentralized, like Bitcoin. They also have differences of a technical nature, different purposes, application specifics, etc. This necessitates the selection of criteria for which it is possible to classify cryptocurrency. Thus, V. K. Shaidulina proposes to classify cryptocurrencies on the basis of the ICO (the initial presentation of cryptocurrency aimed at attracting investments for its development) and liquidity levels. Consequently, it is proposed to select a group of cryptovaginal tokens received as a result of the Initial Coin Offering (ICO), and other cryptic currencies. According to V. K. Shaidulina’s conviction, the first group of cryptocurrency is used as a way of payment, a way of accumulation (savings), exchange and as an investment instrument (STRAT, IOT, Waves, etc.). Cryptocurrencies of the second group are used as a way of payment, savings (savings) and exchange (Bitcoin, Bitcoin-cash, Dash, Ripple, Litecoin, Etherium, etc.) [11, p. 140].

I. O. Kotitsin offers a more branched classification of cryptocurrencies, which distinguishes several levels, classes and subspecies of cryptocurrencies. In particular, we are invited to divide the cryptocurrencies for: 1) the purpose of creation (target / not targeted); 2) the degree of activity, or the achievement of emission limits (active / not active); 3) the type (original, original, and formation as a result of forks); 4) type of regulation (decentralized / centralized); 5) innovation (created on the basis of existing technologies or new ones); 6) by the method of issue (mining / financial instruments), etc. [12].

In this case, I. O. Kotitsin as one of the grounds for the classification of cryptocurrency distinguishes such a feature as the recognition of cryptocurrency by the state, «... that is, the existence of current legislation, which determines the status of cryptocurrency», and distinguishes: a) regulated cryptocurrency (its status is defined and enshrined in the normative legal acts of the state); b) unregulated cryptocurrency (its status is not defined and not enshrined in state legal acts) [12]. We believe that the recognition by a particular state of one or another cryptocurrency as a legitimate way of payment, for example, can not be used as a classification ground. The fact is that the turnover of cryptocurrency is of an international nature, therefore it is impossible to classify them in the fact of presence or absence of legal regulation of transactions with them in a separate state.

In order to find out the economic essence of the cryptocurrency, it is necessary to determine their characteristics, which are due, above all, to the peculiarities of the technology in which the cryptocurrency functions. In the scientific literature, when describing the cryptocurrency literature, the authors distinguish their various features, including decentralization, emissions through landlining, anonymity of payments, emission limitations, etc. [13, p. 152—153; 11, p. 139]. It should be borne in mind that the cryptocurrencies of various types have a different set of features. In this regard, it seems expedient to determine the main features that are inherent in all cryptocurrency, and additional ones, which characterize the features of their individual groups. Among the main features are: a) the openness of the software code; b) the conditionality of the exchange rate of cryptocurrency by the demand and supply; c) irreversible nature of transactions; d) open access to transaction information; e) anonymity of payment participants; e) saving transaction information for a long time; is) P2P-character of transactions; g) openness to other payment systems. Additional attributes include: a) the absence of a central administrator; b) decentralized emissions; c) limitation of the volume of emission; d) impossibility of forgery.

The overwhelming majority of cryptography is based on open source software that runs a particular cryptographic network. Thereby, the transparency of the system and the possibility of its
improvement by a wide range of specialists are achieved. Open code of software in the economic and legal aspect mean the possibility of attracting a significant number of specialists to increase the efficiency of the use of one or another cryptocurrency with minimal economic costs, as well as the impossibility of the imperative impact of one subject on the functionality of cryptocurrency.

The feature of cryptocurrency, which separates them from traditional fiat money, is the absence of an entity that defines the exchange rate of cryptocurrency and guarantees its liquidity. Cryptocurrencies, unlike fiat money, are not depreciated with anything, they are not used as central banks obligations, and their exchange rate is determined only by the expectations of persons conducting transactions with cryptocurrencies, that is, it is determined by demand and supply.

Transactions with cryptography are irreversible. Transactions can not be frozen, nobody can delay the amount of money, and in case of purchase of goods or services for cryptocurrency, the buyer can not withdraw a payment when he is not satisfied, for example, with the quality of the service or product. There is no third party that could affect the results of the transaction. Another signifies this — P2P-character of transactions (Peer to Peer, from English — equal to [13]), which provides for their exclusively between two persons, without the involvement of banks, financial institutions, etc.

Another feature of all cryptocurrencies is finding information in the open access for all transactions. This is due to the blockchain technology, which involves merging transactions into blocks, and each subsequent block contains information about the previous one. In this case, personal data about the persons who made the transaction is not publicly available. In this way, the anonymity of the transaction is achieved, or rather, pseudo-anonymity, because in some cases, with the use of additional information (for example, tracking the IP address of the participant of the transaction), it is possible to find out the physical location of the computer from which it was conducted, and identify a particular individual. In the future, it is not difficult to trace all the operations with this cryptocurrency, which person pursued.

The distinctive feature of cryptography is to store information about all transactions throughout the lifetime of one or another cryptocurrency network. This is also due to the blockade technology. Storing this information is a prerequisite for the existence of a network. Also, all operations with cryptocurrency transactions are in non-cash form.

Another feature of cryptography is the openness of the corresponding crypto-exchange systems to other payment instruments. It is about the possibility of exchanging cryptocurrency for other currencies — such as fiat (dollars, euros, hryvnia, etc.) and other electronic ones (QIWI, WebMoney, etc.). Such an exchange is in practice carried out on cryptoexchanges or with the use of electronic exchange points. Currently, the legal regulation of such activities in different countries is significantly different, and the common feature is the presence of a large number of gaps. Not completely resolved remains the issue of cryptocurrency taxation as market participants, which carry out exchange transactions, as well as organizers of the respective platforms.

The additional feature of cryptocurrencies is the absence of a central administrator, but this sign is not absolute. It is not right to assume about the absolute decentralization of cryptocurrencies, since it can indirectly be carried out at three levels: centralization of development management; centralization of wallets (services); centralization of mining [15].

At the development management level, centralization can be indirectly impacted by the impact on the staff involved in the improvement of the program code. This process involves developers who, of course, can not work for free. Thus, the organization (or organizations) that fund the development and improvement of the relevant crypt-exchange platform has an impact on its program code. In addition, cryptography needs to be stored, which is used for so-called hot (funds are stored online with the involvement of a third-party service) or cold (located on the user’s computer) wallets. In the latter case, of course, centralization does not occur — each user has its own wallet and does not affect other participants in the cryptocurrency network. However, treating blockheads requires significant computing power, which creates inconvenience for a simple user. That is why users frequently resort to organizations that handle cryptocurrencies on their powerful servers (for example, http://blockchain.info/, https://www.myetherwallet.com/, etc.). In fact, such organizations manage the funds of their clients.
The vast amount of cryptocurrency is characterized by decentralized emissions, which is typical for those types that are emitted due to the mining (from English, «mining» — a process in which transactions are checked for various forms of cryptocurrencies and added to the block book’s digital book) [16]. Centralization of mining is carried out by combining the capacities of miners into groups (pools) for more efficient landing and issuance of the corresponding cryptocurrency [17]. The idea of the creator of the cryptocurrency is to complicate with each of the found blocks of the achievement of the subsequent led to the ineffectiveness of personal property, so the managers and grouped together. By the way, the legal regulation of the activity of such pools also needs to be improved, since in fact it is a matter of the kind of entrepreneurial activity, but due to the lack of regulation of the basic concepts and categories, it is difficult to determine the peculiarities of its taxation at this time.

Decentralization of emissions — a feature that is not common to all cryptocurrencies. There are several types of cryptocurrencies emissions: limited disposable; limited controlled; unlimited controlled. In the first case, the entire volume of the corresponding cryptocurrency is issued immediately (Ripple — 100 billion coins, NEM — 9 billion, Cardano — 45 billion). In the process of functioning of these systems, in the future, their number does not change, the growth of coins does not occur, which is embodied in the concept of these cryptocurrencies. Limited controlled emissions were the first, and now under this scheme the emission of an overwhelming amount of cryptocurrency is carried out. New coins in this case come in turn gradually, and their total number can not exceed a certain threshold (BitCoin — 21 million coins, Litecoin — 84 million, DASH — 19.8 million, etc.). Limitation of volume and control over emissions significantly affect the exchange rate. Typically, coins with this type of issue are turned over through mining. Unrestricted controlled emissions are inherent in such cryptic currencies as Ethereum, Dogecoin. These systems are characterized by fast transactions [18; 19].

Conclusions. Thus, currently, cryptocurrencies transactions are not limited to the physical boundaries of one state, therefore their regulation should take place simultaneously with the provisions of the law of the countries in which the participants of transactions are located. Signs inherent for all cryptocurrencies are: open source code software; the exchange rate is crippled by demand and supply; irreversible nature of transactions; open access to transaction information; anonymity of payment participants; saving information about transactions for a long time; P2P-nature of transactions; openness to other payment systems). With regard to the benefits of limited controlled emission of cryptocurrencies, they consist of: a) the gradual appearance of coins, which, combined with a constant increase in the complexity of the estate, contributes to the growth of their course; b) through the application of regulatory instruments and the limitation of the final volume of coins, the demand and supply are at the same level or the first exceeds the latter; c) Coins with this method of emission are prone to deflation.

Литература
8. Ethereum official site [Electronic resource]. — Available at : https://www.ethereum.org/beginners.
References


The article is recommended for printing 16.09.2019 © Kucheryavenko M. P., Dmytryk O. O., Golovasheych O. O.