JUSTIFICATION OF THE FEASIBILITY OF THE DEVELOPMENT OF FINANCIAL AND LEGAL REGULATION OF THE CRYPTOCURRENCY MARKET IN THE LIGHT OF GLOBALIZATION

Taras Zavada [1]

Received: 2021-11-28
Accepted: 2022-01-17
DOI: http://doi.org/10.46489/gpj.2022-2-1-13

Annotation. The article examines the feasibility of developing the financial and legal regulation of the cryptocurrency market in light of globalization. The author considered the historical and legal context of the formation of the cryptocurrency market against the background of globalization. The author characterized the content of blockchain technology, its features as a subject of financial and legal regulation of cryptocurrency and the content of financial and legal relations arising in connection with the functioning of cryptocurrency markets. The author came to a conclusion that although blockchain technology is able to solve a number of problems related to the functioning of financial markets, it still creates a number of threats to the national interests of the state in the financial sphere. The author substantiates the feasibility of the development of financial and legal regulation of the cryptocurrency market in light of globalization in connection with the spread of threats of fraud, tax evasion, the use of cryptocurrencies to pay for illegal goods and services, and the financing of terrorism.

Keywords: financial and legal regulation, cryptocurrency, cryptocurrency market, financial threats to national security.

[1] Taras Zavada, Institution of Higher Education "Lviv University of Business and Law", https://orcid.org/0000-0003-4321-5987

INTRODUCTION

The practicality of legal regulation of financial and legal relations at the current stage stems mainly from the impossibility of a priori and total observance of the state's national interests by private entities participating in such relations. However, the technical and technological development of the 21st century poses new challenges to financial law in terms of finding ways to regulate specific financial markets, the emergence and development of which are due to technological breakthroughs and the emergence of new financial technologies. One of these directions is the development of the doctrine of financial and legal regulation of the cryptocurrency market.

At first, the cryptocurrency market was seen as a libertarian tool to remove the state from private financial relations between subjects. In the end, however, it turned out that cryptocurrencies not only opened up new opportunities for the liberalization of financial legal relations, but also created threats to the national interests of states in the financial sphere.

In today's conditions of globalization of the world financial system, as well as classic stock and futures markets, the cryptocurrency market has received an impetus for development. Millions of users around the world have access to cryptocurrencies, and this is also possible with the help of a simple smartphone.

A large number of digital and other products in the cryptocurrency industry gives rise to a fairly wide range of relationships with various economic, financial and social consequences. The main reason for the interaction of cryptocurrency market participants is the satisfaction of their interests by obtaining a wide range of services, as well as the possibility of obtaining high incomes in a short period of time.

Roy E. Allen, David Vidal-Tomás, Ana M. Ibáñez, José E. Farinós, and others studied the potential and threats associated with the development of the cryptocurrency market in light of globalization.

The purpose of this article is to summarize the reasons that collectively prove the expediency of national and international financial and legal regulation of the cryptocurrency market in light of globalization.

RESULTS

A financial transaction can be defined as any business transaction in which money changes hands. This action is accompanied by documentation of this event and, accordingly, documentation. Both money and documentation are driven by information technology; therefore, financial market activity is enhanced by advances in technology.

Expanding the use and productivity of electronic and physical mail, telephones, computers, fax machines, imaging devices, communication satellites, fibre optics, the Internet, etc., create better opportunities and increase profits in the field of financial services.

Changes in communications have always affected the structure of finance, but the events of recent decades have determined the truly global nature of today's financial markets. A connection was established between various national and international economic and financial markets. New international opportunities have been emerging for centuries, but only recently has interdependence become so widespread that it deserves the word "global."

The shift of financial markets from paper trading floors to computer screens, as in the case of the US NASDAQ and its connection to the London "stock market", is one example of how new computer technology has stimulated global trade. It was estimated that between $200 and $300 million of foreign stocks changed hands every day on the London over-the-counter market in 1986, when the UK's "Big Bang" occurred, roughly double the level of 1981, with half of this volume coming from US stocks. This level was equal to half the volume on the London Stock Exchange, which also trades a large number of non-British securities.

Over the past three decades, many other new technologies have appeared that have expanded the possibilities of limitless electronic finance: automatic teller machines (ATMs), electronic points of sale, telephone banking, interactive screen communication between financial intermediaries and their wholesale and retail customers, even more, innovative debit, credit and smart cards, as well as electronic wallets. Computer, telecommunication and other "non-banking" firms began to enter these markets. Globalization of plastic payment cards is underway. Nowadays, the globalization of payment systems is moving from plastic to smartphones.

Recently, the blockchain and distributed ledger technology behind decentralized digital currency (cryptocurrency) have been used as databases that are shared by all users rather than by a single entity such as a bank. Central banks of various countries around the world are studying the possibilities of virtual currency supported by these technologies. Due to the "transparency" of cryptocurrencies and infrastructure, this approach makes it possible to save on printing and administrative costs, it will be more difficult to counterfeit, and it will be more difficult to use it for illegal activities [1].

The globalization of the financial system took another leap forward with the widespread use of smartphones and high-speed mobile Internet. The average user has the opportunity to access directly from his smartphone to: cross-border money transfers, banking services, purchase/sale of goods and services, investment and speculative instruments in the classical markets of stocks and cryptocurrencies.

The mass introduction of smartphones and high-speed mobile Internet allowed companies to increase their customer base significantly, and services that were previously unavailable were opened to the average user. Financial processes have been significantly simplified from the point of view of process optimization.

A qualitative leap over the past 30 years (in telecommunications, information, digital and technologies in general) has contributed to the transition from paper media to digital media, which has significantly reduced costs and provided a number of advantages - automation of processes, data segmentation, selection of necessary information, work with Big Data. Despite all the advantages, the human factor remained - software, equipment configured by a specialist (a person who can accidentally or intentionally make mistakes when setting up accounting systems, which affects the final result). These systems cannot be considered completely autonomous, as they require human participation.

Blockchain technology, which is at the origin of most cryptocurrencies, including Bitcoin, is a digital ledger in which all data sorting methods are embedded in software code from the beginning. For the operation of the system (data accounting), human participation, in the classical sense, is not required, and no more changes can be made to the work process (transaction accounting). This is provided for by embedded algorithms. The documentation accounting process is carried out automatically by built-in algorithms. But changes and improvements can already be made to the data processing process to achieve the desired results. If we draw analogies, the blockchain is an archive protected by mathematics, while the work of searching for information in the structure of the archive can be optimized based on tasks.

In addition, cryptocurrencies are based on cryptography, i.e. methods of data encryption, which increases the protection of data against hacking/interception. Unlike centralized financial products that have central servers, blockchain technology implies a distributed data registry on many network machines. That is, hacking one or more nodes will have absolutely no effect, which greatly increases the resistance to failures of such systems and their resistance to hacker attacks.

In February 2016, hackers attacked Bangladesh's central bank and, exploiting vulnerabilities in the global financial system's core SWIFT electronic payment notification system, attempted to steal $1 billion. And although most of the transactions were blocked, $101 million still disappeared. This

heist sent a wake-up call to the financial world that the systemic cyber risks that exist in the financial system have been greatly underestimated.

Today, the assessment that a major cyber attack poses a threat to financial stability is an axiom and a question not of if but when such an attack will be made. However, governments and companies around the world continue to struggle to contain this threat, as it remains unclear who is responsible for protecting the system. More and more concerned key voices are sounding the alarm. In February 2020, the head of the European Central Bank and former head of the International Monetary Fund, Christine Lagarde, warned that a cyber attack could trigger a serious financial crisis. In April 2020, the Financial Stability Board warned that "a major cyber incident, if not adequately contained, could seriously disrupt the functioning of financial systems, including critical financial infrastructure, with wider consequences. for financial stability" [2]. The potential economic costs associated with such events can be enormous and the damage to public trust and confidence significant.

In order to achieve more effective protection of the global financial system from cyber threats, the Carnegie Foundation published a report in November 2020 entitled "International Strategy for Improving the Level of Protection of the Global Financial System from Cyber Threats." This report, prepared in collaboration with the World Economic Forum, recommends concrete measures to reduce fragmentation by promoting closer cooperation both at the international level and between government departments, financial companies and IT firms [2].

However, the report does not provide a definitive solution to cyber threats to the financial system. To solve such a problem, a specific toolkit or technology is needed that can eliminate any threat coming from attackers. Similar technology could potentially be the use of blockchain technology, which is the basis of cryptocurrencies.

In the blockchain, any transaction is tracked from the moment it is created. You can see which wallets had "digital money", so the system is as transparent as possible, which minimizes corruption risks. Also, there are already technological solutions (on individual projects) that allow you to block or burn digital assets that have been obtained through criminal means directly on the wallets of attackers. The improvement of this technology provides tools for the global financial system to counter hacker threats.

The main threats from a global perspective are related to cryptocurrencies – legalization of criminal proceeds, financing of terrorism, etc.

The use of digital currency (bitcoins and altcoins) for criminal activity and money laundering has grown in scope and sophistication in recent years. Tools that facilitate the use of cryptocurrencies are now widely available, and services designed to channel criminal profits are well established. As a result, the criminal use of cryptocurrency is no longer limited to cybercriminal activity but refers to all types of crimes that require the transfer of monetary value.

Regulation of the cryptocurrency environment now requires service providers and platforms to collect more information about users and transactions (AML, KYC) [3], which has improved law enforcement's response to the criminal use of cryptocurrencies.

The proliferation of altcoins includes the emergence of privacy coins. Monero is one of the privacy coins and is often used by criminals. It allows anonymous transactions, hiding the address of sending and receiving, as well as the volume of transactions using different methods and technologies. Although Monero has gained a lot of popularity in recent years, the coin is still far from overtaking Bitcoin.

Many exchanges have now delisted privacy coins following regulatory guidelines. However, these coins have not become as popular as expected, probably because they are not as liquid as Bitcoin and other altcoins and, therefore, more impractical.

Pseudo-anonymity and decentralization create a favourable environment for criminals [4]. It is important to emphasize that cryptocurrencies are not anonymous. Each individual transaction is registered in the blockchain, which is a register of all transactions distributed among all users in the network. Most blockchains are public, allowing transactions to be tracked. However, a number of services and methods can increase anonymity and complicate investigations by law enforcement agencies. Privacy coins can hide parts of their blockchain. The decentralization of this financial system provides additional opportunities, as it allows bypassing the control role of the traditional central authority, as well as geographical limitations. Not only does this enable extremely fast international transactions, but it also makes it possible to exploit regulatory gaps between jurisdictions.

Cryptocurrencies have been adopted as part of money laundering schemes and are particularly linked to several predicate crimes, including fraud and drug trafficking. They are also widely used as a means of payment for illegal goods and services offered online and offline. Money laundering is the main criminal activity associated with the illegal use of cryptocurrencies. The growing popularity and spread of cryptocurrencies have led to their widespread use in money laundering schemes. Other criminal activity that shows the intensive use of cryptocurrencies is related to the use of cryptocurrencies as a means of payment for illegal goods and services, fraudulent investments in cryptocurrencies and cybercrime. In all cases, criminals want to hide the source of illegal assets using cryptocurrencies. A number of indicators show how much fraud criminals rely heavily on the use of cryptocurrencies.

Cryptocurrencies are also the preferred means of payment for criminal goods and services, such as drugs or child sexual abuse material (CSAM), purchased online. This applies, in particular, to listings on darknet trading platforms, where cryptocurrency is the main means of payment. Different types of malware aim to steal cryptocurrency as well as mine coins from the network of unknowing victims. Cryptocurrencies are widely used in extortion schemes carried out by cybercriminals. Digital services and infrastructure used for criminal purposes, such as servers, virtual private networks (VPNs) and hosting services, are mostly purchased in cryptocurrency.

At first, cybercriminals felt safe by simply processing their illegal transactions in Bitcoin. However, soon after, it became clear that Bitcoin was far from anonymous and untraceable when blockchain analysis led to successful law enforcement investigations. Therefore, the criminal use of cryptocurrency must be associated with the use of services that increase anonymity.

The development of specialized cryptocurrency money laundering services has inevitably lowered the level of technical knowledge required, contributing to the widespread use of these methods by many criminal entities and networks.

Cryptocurrency remains attractive to criminals, primarily due to its pseudo-anonymous nature, as well as the ease and speed with which funds can be sent anywhere in the world. However, the use of cryptocurrencies for illicit activities appears to represent only a small portion of the overall cryptocurrency economy and is likely comparatively smaller than the number of illicit funds involved in traditional finance [3].

Threats are outlined, and the grounds for recognizing the expediency of financial and legal regulation of the cryptocurrency market in light of globalization are defined as a whole.

CONCLUSIONS

According to the results of the conducted research, it was proved that the formation of the cryptocurrency market was a consequence of globalization processes in the world financial system, as well as a consequence of telecommunications and other technologies. In parallel with the development of modern technologies, the ecosystem of cryptocurrencies is also developing. New technological solutions (such as stablecoins,

NFTs, and smart contracts) are emerging, and the crypto industry is gradually integrating with the classic ones. Gradually, new users enter the ecosystem and the liquidity of the market increases, and blockchain technologies expand to WEB 2.0, transforming it into WEB 3.0. Thus, the cryptocurrency market not only develops internally but also changes the rules of the game on external platforms. At the same time, the cryptocurrency market is still in its infancy, as evidenced by the extremely high price volatility of both Bitcoin and other cryptocurrencies.

It has been established that there are significant advantages of blockchain technology for certain entities of the cryptocurrency market and even state governments. Nevertheless, related financial and legal threats such as fraud, tax evasion, use of cryptocurrencies to pay for illegal goods and services, and terrorist financing dictate an urgent need to develop an adequate response to the development of sources of financial and legal regulation of the cryptocurrency market.

Referneces

Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. The Financial Crimes Enforcement. 2013.

California State Assembly http://abnk.assembly.ca.gov/sites/abnk.assembly.ca.gov/files/AB_129_0_ABPCA_CX27_Dickinson_RN_SN_20140107_FAROUKMA_20140121_FN_R092121.pdf

AML/KYC. https://exbase.io/uk/free/aml

Global and national security / V..I. Abramov, H.P. Sytnyk, V.F. Smolyanyuk et al. / ed. G. P. Sytnyka. - Kyiv: NADU, 2016. - 784 p.

Kalaida Y.P. the possibilities of blockchain technologies in the investigation of criminal offenses committed in cyberspace. Information and law. No. 4(39)/2021. http://ippi.org.ua/kalaida-yup-mozhlivosti-blokchein-tekhnologii-u-rozsliduvanni-kriminalnikh-pravoporushen-vchinenikh

Splinnyk I., Yaroschuk O. Institutionalization of cryptocurrency: regulation, legal status, accounting and taxation. https://doi.org/10.35774/ibo2020.02.081