CRYPTOLIABILITY

DSc. Denis A. Pechegin
The Institute Of Legislation And Comparative Law Under The Government Of The Russian Federation, Russia

ABSTRACT

Funds are the core of the financial system of any modern state. Initially, the money comes from private funds; however, the development of the economy and other factors at the time led to the abandonment of private money and the establishment of a unified monetary system in most countries. Despite this, the development of Internet technologies and trading techniques in real-time has led to the revival of the idea of private money.

In accordance with official forecasts of the development of the domestic economy (development Concept and Security Strategy), the imbalance in world trade and capital movements will continue and may increase in the coming years, which will contribute to changes in the exchange rates of world currencies.

The topic is crucial today, because no one in the whole world wants to consider the question of liability in the cryptosphere. Thus, the draft Federal law "On amendments to the Federal law "On the development of small and medium-sized businesses in the Russian Federation" and the draft Federal Law "On amendments to the Federal Law "On digital financial assets" provides for the formation of special platforms (crypto-exchange, operators, etc.). However, they do not regulate the liability of professional participants of the emerging new crypto market.

This paper is prepared on the basis of a legal and technical analysis of legal norms, as well as comparative legal and formal-logical methods; i.e., the method of systemic analysis. The goal of this paper is to consider this problem and to suggest possible solutions, including in the field of criminal, tax and budget legislation.

Keywords: cryptocurrency, cryptosphere, liability, cryptocurrency exchange market, cryptorisks.

INTRODUCTION

Currently, both professional and non-professional market participants are increasingly discussing various aspects of the use of cryptocurrency in a particular country [12]. There are draft laws on regulation in the cryptosphere, organised lectures, and conferences. Meanwhile, in pursuit of "new thrills," we've forgotten about the flip side of the coin. It is necessary to understand clearly who will be responsible for illegal activity in the area under consideration.

The unregularised status of cryptocurrencies; the lack of a uniform international practice [5] and judicial protection of the issue being analysed; the

instability of pricing in the cryptosphere; and so on. – Collectively, this comprises the core facts that today constitute a threat to national security [5].

DISCUSSION

Russian judicial practice on this highlighted issue is based on the fact that until the due legal settlement of all key issues in the cryptosphere is achieved, neither individual persons nor legal entities will be able to find protection in the face of governmental enforcement authorities.

The lack of clarity among approaches in law enforcement practice prevails among foreign jurisdictions. So, according to one court US decision, bitcoin is recognised as legal tender (http://cdn.arstechnica.net/wp-content/uploads/2016/09/murgio-order.pdf). Relying on the principle that, in the absence of regulation a contractual term is to be understood in its literal sense, one US court concluded that bitcoin is a form of money, since it acts as a universal monetary equivalent and is used to acquire things. In another decision, bitcoin was not recognised as money (https://forklog.com/sudya-iz-majami-otkazalas-priznat-bitkoin-dengami/).

This latter decision contradicts other judicial acts of 2013 and 2014 on similar issues (https://forklog.com/sudya-iz-majami-otkazalas-priznat-bitkoin-dengami/). Moreover, in the US, the Federal tax service's interpretation is that cryptocurrency is property, whereas FinCEN's interpretation is to recognise cryptocurrency as a form of currency [8].

It seems that one should not impose full responsibility for the commission of various divergent actions in the cryptosphere on the user – an ordinary citizen who, in the current world economic situation, sees in virtual currency the sole real opportunity for garnering income without using banking services that would be, in his opinion, unnecessary.

Although, in comparison with 'fiat' money, cryptocurrency is used for criminal purposes less often [7], nevertheless, according to Positive Technologies (https://www.kommersant.ru/doc/3566894), fraudsters stole USD300 million through ICO's in 2017. At the same time, in the vast majority of cases, the attackers sought to gain control of the platform itself in order to replace the address of the organizers' cryptocoin cache with their own [13]. Another example is development by the cyber criminals of miners' programs [3], which deliberately blocks other miners' programs that were installed on that computer [2].

However, more "classical" (*mala in se*) crimes are also committed in the cryptosphere [14]. For instance, very commonly encountered of late is a scheme whereby a seller of cryptocurrency meets with a buyer in a restaurant to exchange digital for fiat money. The buyer shows the seller the money and the seller transfers the cryptocurrency. But at this point, powerful people show up who claim that the seller did not receive any money, because the buyer must first come to terms with them.

The above-indicated situation emphasizes the urgency of introducing liability (including even criminal) in the cryptosphere. In one manner or another, those market participants who decide on an ICO (financing recipients) seek to raise money through special websites or crypto-exchanges. It would seem that establishing the responsibility of such a platform (exchange) for information provided thereon to market participants as well as the responsibility of financing recipients would significantly reduce the number of potential fraudulent actions in this area and ensure greater stability at the national level. At a minimum, such a platform should analyse the activity of one legal entity against the activity of another legal entity, in arbitration and civil proceedings to which it is a party, on net profits (not information about assets) for the previous year, and so on. There are ways out of this situation.

Option 1: The recipient of financing must maintain a separate account with the bank, provide data on expenses therefrom in a restricted access mode (login, password) to financing participants, and agree that the bank shall have the right at any time to freeze funds on this account until certain specific circumstances are clarified; in any situation where funds from such an account are spent not in accordance with the stated goals of the legal entity's fundraising by way of the ICO, such information is placed on the fundraising platform, with simultaneous notification of the Internet platform (crypto-exchange).

Option 2: The activity described at Option 1 is carried out by the Internet platform itself (crypto-exchange). In other words, the financing recipient does not receive any "hard cash;" rather, it is all located on a digital account opened with the crypto-exchange. At the same time, information about the expenditure of funds is provided by the Internet platform (crypto-exchange) to financing participants in closed access mode (login, password).

Then the system will be able to provide financing participants with a certain level of guarantee, which will increase the attractiveness of this new sphere and attract new investors, including those from abroad.

Possible objections to this proposed approach are understandable. Neither the companies, nor the crypto-exchanges, nor the banks today would choose to conduct their activities under such "strict" regulation because of their desire to obtain easy and fast profits. On the other hand, if a financing recipient behaves in good faith and achieves its goal as the result (honest implementation) of the project, then what should it be afraid of?

It is quite possible to build a new system within the existing legal framework, as evidenced by the experience of several countries – in particular, the Republic of Belarus. Foreign companies can form subsidiaries in the Hi-Tech Park of the Republic of Belarus [1].

According to the statement of V. Zuercher, the main problem of cryptocurrencies is that, in the vast majority of cases, no one can take the proceeds from the sale of a cryptocurrency at an increased exchange rate (compared with the exchange rate when purchasing crypto-currencies) as money to the Bank.

In our opinion, a way out of this situation (given, also, the goal of preserving the current financial system and the proper order for monetary circulation) would be to exchange cryptocurrencies for 'fiat' money by reference to crypto-exchanges accredited by the state and functioning with large (reputable) banks, whose activities would be subject to compulsory insurance (crypto insurance).

In other words, crypto-exchanges would act as a kind of filter in this new sphere of activity for national governments, which would minimise the risks in constructing a new financial turnover algorithm, thereby ensuring consensus among all market participants.

A system thus described, in our opinion, would serve to minimise cases of improperly granting legal rights of possession, use and disposal of money or other property acquired by persons as the result of their commission of crimes, including by means of transactions or financial operations with such money or other property. In this regard, it would be possible to adjust the scope of articles of criminal law on money laundering, since under contemporary circumstances these acts can be committed not only through transactions or financial operations, but also by other means [6]. An example would be the experience of Switzerland, which intends to regulate cryptocurrency operations with existing legislation. In particular, it is envisaged that all tokens would be classified into payment, utility (affording access to the resources of special crypto-platform) and asset tokens.

Accordingly, it might be assumed that utility tokens should not fall under the legislation on the anti-money laundering of funds due to the fact that such tokens only provide access to the relevant resources (https://crypto.whenspeak.ru/rooms/3840/). However, this approach cannot be deemed successful, since utility tokens can in fact be transferred to other persons or exchanged for other tokens – including payment tokens – exchanged for currency, and so on. Therefore, the risk of the use of tokens in the Swiss jurisdiction for purposes of money laundering cannot be considered adequately mitigated.

It is noteworthy that the idea of creating a national crypto-exchange has already been raised in China. Wang Pengjie has suggested that the People's Bank of China, in cooperation with the China Securities Regulatory Commission, can create its own platform for authentic blockchain technology with a special system of verification and a national crypto-exchange (http://bitcom.blog/member-chinas-main-political-advisory-proposes-national-crypto-trading-platform/?i=3).

It is rather easy to envision a crypto-exchange more tangibly if we consider official applications for modern smartphones that allow downloading and installing of programs and games (AppStore and Google PlayMarket). Yes, you can download a program from the Internet to your phone (especially easily, as this can be done on any phone with the Android platform); but in this case, you will not be immune from fraudsters and cyber criminals, who insert special scripts into "free" software that is hosted on the Internet allowing them to download information from your phone; to send SMS messages; to identify the level of your savings in the bank; to steal money; or to install a permanent task in your phone

to engage in undetected mining of the Monero cryptocurrency, etc. [15]. Similarly, today, with the independent purchase of cryptocurrency, no one is immune from phishing sites, scam sites, mirror sites of official foreign exchanges, etc. It seems that the accredited crypto-exchanges would minimise the risks currently existing in the crypto-sphere.

Such an approach would also help to build a system in which the state, along with the "classic" budget, would be able to formulate in tandem a crypto-budget. In science, for example, it is proposed to introduce an elective tax on anonymity for a transaction in which at least one party is known [10]. In Brazil, a capital gains tax of 15% is payable to the state at the time of the sale of cryptocurrency, and the holder of the cryptocurrency worth more than 1,000 reals must declare such information in his declaration [9].

After all, the financial resources of the country are different flows (municipal, public finance, household finance), which are not separated by an impenetrable wall, but rather interconnected [4]. In this case, the state, according to some forecasts, would also be able to transfer the accumulated cryptocurrency to fiat currency and replenish the "classic" budget; and the level of the country's budget would always be above 100%.

CONCLUSION

This study shows how it would be possible to integrate the latest developments in the field of Finance in the legal sphere of monetary circulation.

A way out of this situation (given, also, the goal of preserving the current financial system and the proper order for monetary circulation) would be to exchange cryptocurrencies for ‘fiat’ money by reference to crypto-exchanges accredited by the state and functioning with large (reputable) banks, whose activities would be subject to compulsory insurance (crypto-insurance).

This would minimise the risks in constructing a new financial turnover algorithm, thereby ensuring consensus among all market participants.

In this case the state would be also able to create its own cryptobudget and the level of the country's budget would always be above 100%. In addition, by applying to the crypto-exchange, the courts would be able to impose a penalty on the cryptocurrency of citizens and law firms, etc.

A private citizen should not have fear that a transfer of funds to an Internet platform (whether *de jure* or *de facto*) would be equated with their unconditional loss. Financial security should correspond to the real development of monetary relations and be adapted to modern conditions; and the state’s monetary system should be flexible in relation to new challenges and threats.

REFERENCES

[1] Alejnikov D., Regulirovanie blokchejn-ehkonomiki: opyt Respubliki Belarus', First international law forum «Cryptosreda», Russia, URL: https://crypto.whenspeak.ru/rooms/3840/resources, 2018;

[2] Cimpanu C., Coinminer Comes with a Process «Kill List» to Keep Competitors at Bay, URL: https://www.bleepingcomputer.com/news/security/coinminer-comes-with-a-process-kill-list-to-keep-competitors-at-bay/, 2018;

[3] Dowd K., New Private Monies: A Bit-Part Player?, Institute of Economic Affairs Monographs, Hobart Paper 174, England, pp 52, 2014;

[4] Dzhumov A., Nalogovye dohody byudzheta kak glavnyj sistemnyj integrator finansovyh resursov, Nalogi, Russia, 2007, vol. 6, pp 18-20;

[5] Ehlektronnaya valyuta v svete sovremennyh pravovyh i ehkonomicheskih vyzovov: sb. materialov Mezhdunarodnoj nauchn.-prakt. konferencii [ed. A.S. Genkin, E.L. Sidorenko, O.I. Semykin], Russia, pp 360-369, 27, 2016;

[6] Esoimeme E., The Money Laundering Risks and Vulnerabilities Associated with MMM Nigeria, Journal of Money Laundering Control, Great Britain, 2017, vol. 21, issue 1, pp 112-119;

[7] Francis E., Bitcoin: Not So Scary, pp 1-5, URL: https://ssrn.com/abstract=2600344, 2015;

[8] Khisamova Z., Ugolovno-pravovie meri protivodejstviya prestupleniyam, sovershaemim v finansovoy sfere s ispolzovaniem informacionno-telekommunikacionnih tehnologiy, Dissertaciya … PhD, Russia, Krasnodar, pp 166, 2016;

[9] Oblachinskij I., Bitkoin: zarubezhnyj opyt, EHZH-Yurist, Russia, 2014, vol. 23, pp 8;

[10] Omri M., A Conceptual Fremework for the Regulation of Cryptocurrencies, 82 University of Chicago Law Review, USA, 2014, vol. 53, pp. 53-68;

[11] Petrov I., Kriminal'nyj bitkoin, URL: https://iz.ru/684876/ivan-petrov/kriminalnyi-bitkoin, 2017;

[12] Popper N., Cifrovoe zoloto: neveroyatnaya istoriya Bitkojna, Russia, 2016, pp 11-12;

[13] Sidorenko E., Criminal Use of Cryptocurrency: International Assessments, Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yusticiya, Russia, 2016, vol 6, pp 8-10;

[14] Trautman L., Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?, Richmond Journal of Law and Technology, 2014, vol. 20, pp 4;

[15] Vovnyakova A., Ostorozhno: Android-virus atakoval tysyachi bankovskih kart, URL: https://hi-tech.mail.ru/news/virus-obokral-tysyachy-kart/, 2018.