Conference Paper

What are the Technical Means the State Prepare for the Regulation of the Cryptocurrencies?

Glotov V. I.[1] and Mihailov D. M.[2]

[1]Candidate of Economic Sciences, professor, academician of the Russian Academy of Natural Sciences, deputy director of the Federal service for financial monitoring, director of Institute for Financial and Economic Security of National Research Nuclear University MEPhI, deputy Chairman of the Board of network Institute in the field AML/CFT, Moscow, Russia
[2]Candidate of Engineering Sciences, associate Professor of BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY, Moscow, Russia

Abstract

The technology of BlockChain and cryptocurrency is an actual topic for humanity today. There are different policies regulating cryptocurrencies, but they are still far from perfect. The difficulty of technical regulation of these systems is beyond doubt, many countries are only at the stage of discussing the status of the currencies, some are extremely supportive of them. However, it is undeniable that more and more countries will introduce regulations in the field of cryptocurrencies, focusing, firstly, on the structure of their own economy.

Keywords: BlockChain, cryptocurrency, Bitcoin, mining.

Corresponding Author:
Glotov V. I.
glotov@fedsfm.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

BlockChain as a technology and cryptocurrencies as a monetary realization of this technology entered the life of the entire mankind very quickly. The enormous boom continues and is extremely hard to control. The very technology of distributed storage and data processing implies the absence of centralized control. Of course, such a position cannot be preferred (though to varying degrees) by governments of the countries that at least want to protect their citizens from scammers and to prevent illegal financing of terrorists, and at maximum do not want unorganized cash flows, financing of illegal organizations in the country.

How to cite this article: Glotov V. I. and Mihailov D. M., (2018), “What are the Technical Means the State Prepare for the Regulation of the Cryptocurrencies?” in *III Network AML/CFT Institute International Scientific and Research Conference “FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies”*, KnE Social Sciences, pages 583–592. DOI 10.18502/kss.v3i2.1593

2. The analytical part

The mechanisms of regulation by the governments of different countries cannot be called perfect yet. Today it is possible to point out a few clearly distinguished regulatory policies.

There exist extremely supportive jurisdictions (Japan, Germany, Switzerland), where cryptocurrencies are absolutely legal means. Cryptocurrencies are placed on the same footing as currencies as such or as a legitimate monetary tool in these countries. The laws are methodically adapted to the requirements of the BlockChain community.

A lot of countries only discuss the status of the currencies yet (Australia, Russia, Canada, France). The regulators of each country are arguing about the status of the currency, about the mechanisms for its regulation and are obviously waiting for the decisions of other countries, collecting the ”best practices”. A number of these countries, India for example, have already established the Association and are actively working on a regulatory framework, but do not introduced it so far.

2.1. Partial regulation

Number of countries begin to regulate only several aspects of the cryptocurrencies (Sweden for example), which decided to introduce regulations gradually. In Sweden the same it is forbidden to pay for scrap metal in the cryptocurrency.

In the United States, there is a tendency for greater regulation in terms of the ICO (Initial Coin Offering), an IPO analogue for ordinary securities, but implemented for attraction of investment by means of cryptocurrencies. The US Securities and Exchange Commission brings ICO transactions and tokens sales under the US securities legislation. The Commission thus wants to protect the market players by using a ”new” method of attracting capital.

In China, trading cryptocurrencies and mining are not prohibited for the citizens of the country, but are prohibited for the banking system.

Representatives of the three largest Chinese cryptocurrencies exchanges BTCC, Huobi and OKcoin are regularly summoned to the People’s Bank of China (PBoC), where they are consulted. The Chinese regulator intends to control all the methods of capital movement, including cryptocurrencies [1]. In fact, Chinese exchanges are forced to verify users and provide information to the controlling bodies of China. Most likely, such countries will gradually continue to impose bans and regulations.

In Vietnam, Thailand, Bangladesh, Bolivia cryptocurrencies are prohibited by law. The motivation in such countries is almost always the desire to protect citizens from speculation and fraud.

Many countries think about their cryptocurrencies, which would be deprived of the advantages of virtual currencies: decentralization and anonymity. Ecuador was the first to follow this path. It should be noted that Ecuador does not have its own currency and uses the US dollars. In 2014, the government of Ecuador officially banned the Bitcoin cryptocurrency and its analogues. Ecuador plans to launch its own cryptocurrency and equate it to the national currency, the next year. It is planned that this currency will be secured by the real assets, although it is not yet clear by which. The monetary and financial Committee of Ecuador will deal with the regulation of the cryptocurrency. Perhaps many countries expect the experiment of Ecuador, for them to follow the example.

It is obvious, that the difference in approaches to regulation is determined both by the cultural aspects, the aspects of the state structure, and by the structure of the country's economy.

A developed securities market in the United States, Singapore, Hong Kong, for example, forced these countries to adopt regulations that protect BlockChain as a system of investments in the securities quite quickly. At the same time, India, for example, is the leader of the global money transfers: most of the Hindus are working abroad. The regulation of the cryptocurrency in this country is designed primarily in order not to harm the cash flow into the country. At the same time, India, with its potential to develop software, can become a world leader in technology, so the regulation is obviously carried out very carefully.

Another reason for regulation may be, for example, the countries where the payments are "leaking out", including the migrants' ones. The simplest example related to India the same: the UAE is the largest source of remittances to India, its share makes up 40%, followed by Saudi Arabia with a 30% share.

Any introduced regulations, especially by the large countries, lead to leaps in the volatile crypto currency.

Thus in 2013, the People's Bank of China banned cryptocurrency transactions for the financial organizations, which led to the collapse of the exchange rate of Bitcoin cryptocurrency. After the IRS ranked Bitcoin to one of the types of property in 2014, the price of cryptocurrency fell by $150. In 2017, the People's Bank of China introduced another ban on the turnover of the cryptocurrency, which affected the Bitcoin exchange rate one more time: the cryptocurrency "dipped" by 30%.

While the cryptocurrencies withstand all the challenges, which proves their viability and makes the yet undecided countries think about the necessary regulations. In addition, the opinion about the regulation of cryptocurrencies within the frameworks of the unions: BRICS, ASEAN, and others arises more often.

Let us consider how states can approach this issue. First of all, it is worth paying attention to the already existing examples in other technologies, since the "precedents" - are the first thing that regulators will pay attention to. The best example that illustrates the fight against technology are the prohibitions and "localization" of messengers. The emerged mobile applications for the exchange of short messages and calls allowed users to go out of sight of the special services. Mass cases of using the messengers by terrorists allowed the states, both legally (in Russia for example) and technically (in Turkey for example) limit the use of these programs. Blocking of messengers, disclosure of keys to secret chats for public authorities (in Indonesia for example) were introduced. China has gone the furthest - it created a national messenger platform: the ideal WeChat messenger (fully accessible to the state) under the interlocking of all other programs of this class it quickly became number one in China and seems to soon become number one in the world. Blocking of programs is carried out at the level of packet filtering, typical for messengers.

The President signed the law on the regulation of messengers in Russia, which obliges to identify users by using a telephone number. In fact, this opens up the possibility for regulation for the state. In the strategy project for the development of the information society for the years 2017-2030, published on the website of the Security Council of Russia, it is expected, to strengthen the legal regulation of messengers in particular.

Any regulation of technological solutions typically has three aspects:

- Legal regulation
- Technical regulation
- Special regulation

Legal regulation is often an aspect of the relevant agencies and parliaments of the countries. In fact, the country should introduce the relevant laws and subordinate acts, by introducing the concept of legality of certain operations, as well as the measures of punishment and control.

Special regulation is the job of the special services. E. Snowden's revelations, Wikileaks publications, scandals with Huawei's "bookmarks" which monitor the users, showed how much the technology is involved in the work of the special services.

For many special services, technologies are the new opportunities. Obviously, special services do not ignore cryptocurrencies.

According to a number of public data and publications, one of the first countries caught for taking an advantage of the cryptocurrencies was North Korea: hackers in the service of North Korea hacked the wallets of many users, primarily of those from South Korea. Bitcoins have become an extremely convenient mean for transferring money into this country, because the world community is very much trying to exclude North Koreans from receiving any kind of financing to prevent the development of a nuclear program [2].

With the growth of the amount of unrecognized states, the role of Bitcoin will also increase. Often, regimes of unrecognized or warring republics are supported from abroad, even at the state level. But direct financing in this case is publicized and can even entail UN sanctions. According to many open sources, it becomes obvious that, with the hidden support of the state, mechanisms for hidden transfers of funds are being created even at the state level. And such a tendency will only grow.

Obviously, many states will try to gain advantages through the penetration or hacking of the BlockChain system. It is necessary to assume that the special services will invest in the development of the school for the study of vulnerabilities cryptocurrencies. If to believe the publications of the hacker groups, the NSA (national security agency of the USA) had unauthorized access to the interbank SWIFT system. That is, the traditional monetary system was subject to hacking by the security services, which used vulnerabilities in Windows operating systems to track the cash flows between the banks in the countries of interest. It is hardly worth considering that the anonymous Bitcoin or any other cryptocurrency will be less interesting for the special services.

Technical regulation is perhaps the most interesting aspect of cryptocurrencies' regulation. How can we technically adjust the technology, which was fundamentally based on the principles of maximum decentralization?

In traditional centralized systems, all transactions, before the execution, are verified on the basis of the information from the central supervisory authority. In decentralized systems (cryptocurrencies) there is always a technical possibility of double-spending. This means that the user can make several payments transmitting the same asset, almost simultaneously. Information about them will immediately not fall into another block and each of the recipients will be sure that they have made a valid operation. Only after one of the transactions (not necessarily the first in time) will be included in the block, the remaining transactions with the same asset will no longer be valid.

But there can be transactions, which will differently define the transaction process in parallel branches for a while.

The probability of the existence of parallel chains of blocks is extremely small and catastrophically decreases with the increasing chain length and the number of independent miners. The control of chains is only possible if the intruder has control over a sufficiently large share of the total mining capacity. In this case, there is a significant probability of hidden formation of long parallel chains of blocks. After their publication, the longest chain will be recognized as the main one, and the real chains will be canceled. If the controlled capacity of mining is less than 50%, then the probability of success decreases exponentially with each confirmation.

Interception of 50% of the miners seems to be almost unreal thing, but nevertheless it can be implemented during the state intervention in the process of mining. Such a method of regulation can be introduced, for example, in centralized China.

Another method of controlling a cryptocurrency may be a quantum computer which will allow to decipher any algorithms of encrypted transactions swiftly, but this scenario will not be considered in this article - as long as quantum computing cannot significantly affect cryptocurrencies.

User wallets are structures for storing crypto currency, that is, virtual money based on BlockChain. The wallet is in fact two figures - the unique identifier of the wallet (the Bitcoin-address to which all the money is tied) and so-called "secret" key.

The existing Bitcoin-address can be dictated to anyone who wants to transfer monetary funds to the wallet, that is, to pay for something on the specified identifier (account). Cryptomoney will be tied to this Bitcoin-address after the transaction [3].

To spend money you need to download special software - so-called software wallet. To send money to this wallet, you will need to enter a secret key. After the secret key is introduced and the amount of the transaction is entered, the funds will be debited from the account.

There exist two types of wallets: a cold wallet and a hot wallet.

Hot wallets are connected to the Internet 24/7, so you can spend cryptocurrency any time. But that is a big disadvantage of the wallet, since a hot wallet may be available for hacker attacks also around the clock.

A cold wallet stores cryptocurrency in the offline mode, that is, a cold wallet is never connected to the Internet. In fact, the "cold wallet" is the address storage place in such a way so that hacker cannot technically access it.

To send money from the ”cold” wallet, you need to import a secret key into the program through which the initiation of the transaction occurs. After this operation, the cold wallet will turn into a hot one.

Hardware wallets are becoming increasingly popular. Such a wallet is a small electronic device, with an autonomous display and power. The device stores secret keys in such a way that they cannot be extracted. The device is connected to a computer with Internet access and monitors transactions.

Since the regulation at the infrastructure level may seem difficult for the state, it is technically easier to control particularly the users' wallets. At least, such regulation can be imposed by the state for any companies that have state accreditation. More and more banks and airlines are accepting cryptocurrency already now. In the case of the introduction of national cryptocurrencies, the state will want to be sure that the currency is safe. At the level of centralization of the currency (as in Ecuador) it can be problematic, but it is easier to oblige users to have certified wallets.

A certified wallet is:

- the identification of the user, and thus removing the possibility of anonymity;
- control and accounting of funds;
- user protection against hackers and hacking.

The first and the second paragraphs actually eliminate the advantages of the cryptocurrency as an absolutely open system, but at the same time reduce the likelihood of money laundering and illicit sales.

User protection against hacking is also important and, probably, the only function of such control accepted by the community.

It is necessary to provide a striking concurrence of the investment growth trends in BlockChain-based projects on the Internet and the growth of cybercriminals' profits over the past year. So, for the year 2017, the volume of investments in BlockChain-based projects has doubled, and, surprisingly, the overall profit of cybercriminals has also increased proportionately. The imperfection of technology protection methods and weak government regulation have obviously reoriented cybercriminals to the BlockChain technology [4]. Almost all attacks of intruders are aimed at hacking wallets.

In general, attacks are committed due to viruses, which, virus Trojan. Coinbitclip for example, by entering the computer monitor when a clip similar to the address of Bitcoin wallet appears on the clipboard. The virus immediately replaces it for its address, money is sent to the intruder. Another popular attack is the one aimed at kidnapping the backup versions of the computers. As a rule, the version of the hot wallet left in the ”backup” has the same password as the new version. After gaining access to the old version, an intruder can easily hack the current wallet. Obviously, the intruders will upgrade all the existing set of ordinary viruses to further steer them to steal cryptocurrencies [5].

The use of a hardware purse can help to effective fight against such attacks. It is impossible to remotely steal the user's cryptocurrency, which is protected by a hardware purse. Herewith, the hardware wallets are not so invulnerable. Vulnerabilities that allow cybercriminals to steal cryptocurrency exist for such devices. To exploit a vulnerability, an intruder needs physical access to the device. It takes intruder only 20 seconds to hack a wallet. Thus, Trezor hardware wallet, for example, automatically downloads its memory (SRAM) where the keys are stored when the power source is connected. Downloading occurs without checking whether the user's PIN is entered or not. If before switching the device on, connect to two contacts inside Trezor directly, then the memory can be simply downloaded and, further, with the help of the special software, published on the Internet by the way, just extract secret keys from it. The same problem exists with another purse manufacturer - Keepkey.

3. Results

For today all hardware wallets on the market are produced by private companies and, of course, are not certified by any country. Security is largely determined by the openness of their architecture and the availability for study by the community. Wallets on delivery have a holographic sticker as a rule. The manufacturer warns that if the sticker is damaged when receiving the device, the user should contact the support service.

Roughly speaking, a hardware wallet is a cryptographic mean of protection of the information. Such means in Russia are subject, for example, to the certification of the FSB. In addition, for a number of classes the Federal Service for Technical and Export Control (FSTEC) may partly be responsible for such certification. The already existing legislation of our country can quite simply be adapted to regulate the cryptowallets as means of protecting information specifically. Certification of the release of hardware wallets can be the first step of the regulation in the field of cryptocurrencies, moreover not only in Russia.

The next step will be the mandatory introduction of such devices for all the government agencies or companies that fall under a specialized order.

It is important that in Russia the production of special equipment and its introduction into the government agencies is already a well-established process, as, incidentally, in the USA and in the EU. Information protection facilities have been certified by FSTEC for a long time in Russia, and the country has an extensive network of laboratories licensed by this service that can certify the solutions.

4. Conclusion

To summarize, we may say that:

- In the near future, more and more countries will introduce regulations in the field of cryptocurrencies, focusing primarily on the structure of their own economy;
- It is highly likely that regulation will begin from the government bodies that will start using BlockChain technologies, where it will be easier to impose requirements;
- Technically, regulation will get through the certification of hardware wallets used for working with cryptocurrencies within different countries. Certified hardware wallets can support multiple currencies and, at some point, can start to support only one of them (with a remote firmware upgrade);
- Most likely, none of the countries will be able to introduce regulation at the mining level (perhaps only China).

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Electronic resource] https://www.dp.ru/a/2017/09/18/Kriptovaljuti_Kitaj_darit

[2] Data analysis company CB Insights "Banking Is Only The Start: 20 Big Industries Where BlockChain Could Be Used," July year 2016. [Electronic resource] https://www.cbinsights.com/blog/industries-disrupted-blockchain/

[3] How many Bitcoins mined to date. Mode of access: https://cryptomagic.ru/kriptovaluty/bitcoin/skolko-dobyto.html.

[4] Data company Accenture ”Join the BlockChain party. How banks are building a real-time global payment network [Electronic resource] https://www.accenture.com/us-en/insight-blockchain-technology-how-banks-building-real-time

[5] Capitalization of the cryptocurrencies market exceeded 200 billion dollars. Accessmode: https://economics.unian.net/finance/2225796-kapitalizatsiya-rinku-kriptovalyut-perevischila-200-milyardiv.html