

Conference Paper

Perspective Methods of Regulating Crypto-Currency Based on Blockchain Technologies in the Modern Economy

Fedorov N. M.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

Nowadays almost every advanced user who pays a little attention to the development of the financial market aware of crypto currency. The novelty of this technology, due to its features such as transparency and decentralization, has demonstrated a completely new approach to the notion of a payment system. But at the same time, this development has brought problems, that may pose a threat both to the financial system and to the AML / CFT sphere. In this article, I propose to consider on one of the most effective, in my opinion, method of regulation in order to eliminate the shortcomings – blockchain.

Corresponding Author:

Fedorov N. M.
 fedonick@mail.ru

Received: 11 December 2017

Accepted: 20 January 2018

Published: 13 February 2018

Publishing services provided by
Knowledge E

© Fedorov N. M.. This article is distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use and redistribution provided that the original author and source are credited.

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

1. Introduction

The development of information technology is now gaining new scales, and what was recently considered as a distant future, nowadays seems quite ordinary. New fundamental technologies are widely implement into global spheres and the functioning of socially important areas such as health care, education and state regulation cannot be imagined without hi-tech technologies. The same is for the global economy. Information and communication technologies are entrenched in this sphere and are an indissoluble in maintaining the working capacity of the world market. Nowadays, the functioning of any financial services occurs only with using information technology. Due to such tools it became possible to make international transactions transferring money from one point of the planet to another. But this is just a modernization of the mechanisms that have already been existed, while truly innovative ideas are only just developing.

If you think about the direction in which the financial market is developing now and what can really be called the future of the financial system, most appropriate variants are "bitcoin", "crypto-currency" and "block", which are written by various economic

 **OPEN ACCESS**

publishers and Internet forums. Offering a completely new range of possibilities, such technology can be considered innovative and replace the current financial system.

2. Crypto currency

In 2009, a group of hackers named "Satoshi Nakamoto" develops one of the first payment crypto-exchange systems - bitcoin. The appearance of such currency did not cause an interest boom but the concept of such virtual monetary unit introduced a lot of problems for financial regulators. The principle and basis of the technology on which the exchange of such currency was based was a decentralized system of circulation of funds, together with the openness of transactions and the absence of a single bank. Initially, the crypto currency was used in the shadow network and was intended for use to exchange illegal goods. But, years later, people have appreciated the advantage of the new technology and the crypto industry has gone beyond the shadow sector. The advantages of such payment system were obvious - while supported and regulated by central banks the national financial mechanisms became more expensive, the use of crypto currency guaranteed the security and speed of transactions without attracting third parties for making transfers. The head of the Financial Times, Julio Faura, believes that, in view of the labor-consuming nature of trade between different financial institutions, the use of crypto-currency brings rationalization and makes this process much more efficient.

The problem is, that no matter how well experts talk about the advantages of crypto currency, society should understand that the anonymity of the user himself, when he makes transfers, will not be the same positive side as they believe. Obviously, the need to hide their incomes is inherent in people who commit unlawful acts rather than ordinary users. As example, at this summer, a virus WannaCry had infected computers of some government agencies and companies. To retrieve an access to stored files a virus-extortionist required payment of money on hacker's bitcoin-wallets. In total, this scheme brought about 130 thousand dollars to its creators, while tracking down the recipients of funds and finding out hackers had failed, despite the fact that the information about the transactions was publicly available. Of course, most of this amount was lost in mixing, but some cash hackers were managed to receive, which clearly shows that such schemes are working and are dangerous.

It is obvious that countries cannot allow their citizens to pay anonymously and transfer currency because it can lead to money laundering, that is the basic task of

state bodies as fighters against money laundering and terrorist financing will disappear, because it will not be possible to determine either the source of the transfer, the beneficiary and target of received data. Moreover, it turns out that any activity of financial regulators will be excluded because there will be no mechanisms for controlling the release or devaluation of the crypto currency. If such a payment system operates around the world, then the market itself will have to agree on how much currency it is necessary to issue.

Despite that fact the attempts are being made to limit the use of crypto currency, experts believe that it is much more effective and more rational to convert crypto currency technology to a model which will be met with the requirements of state bodies, adding mechanisms that provide monitoring of using such currency in a fraudulent and illegal sphere. In fact, developers themselves takes such steps. For example, the creators of the RSCoin were able to resolve the issue of controlling in monetary security and solve the problem of high volatility.

But I think it's much easier to solve such a problem with existing mechanisms then adding some new features to the crypto currency technology in case of building a system that meets the necessary requirements. Obviously, this problem can be solved with the help of the technology in which bitcoin and other crypto currencies were made i.e. blockchain.

3. Blockchain

Formally, blockchain is a secure database that records the exchange of the stored information. The most important advantage of such database is, that the records about them are publicly available, but they cannot be deleted in any way, without making changes to the previous blocks of the chain. The security of such system is provided by a set of two keys, the first of which is publicly available, and the second one is available only to the person who completed the data transfer process. Blocking algorithms allow user to combine crypto currency transactions into blocks, and then add them to the chains of existing blocks, using a cryptographic signature.

Despite the fact that the block is open to everyone and anyone can look at the purse what amount of money is being transferred, attackers can use so-called "mixers" that mix dirty money with clean ones, gradually laundering them. The possibility of using such scheme directly follows from the anonymity of the address of the owner. And it is obvious that if this will not be eliminated, then there will be more such schemes.

One of the ways to regulate was implemented by the banks of Barclays and Goldman Sachs in order to reliably consolidate the market of crypto currency, without risking their capital. Their consortium has successfully use the technology of a controlled version of block-based ledger to provide bonds sale. The distributed ledger, in fact, is the same database obtained by blocking, but at the same time technology allows you to determine the personal data of users who used the ledgers. Of course, such access is controlled and is simply not accessible to data, but at the same time there is no absolute anonymity. This technology has already been actively used by a number of countries to optimize the health care system and state management. So, using ledgers, state bodies are able to issue and receive documents from citizens, as well as control the collection of taxes and the issuance of pensions. Such technology can really affect on the opinion of financial and government institutions about using a crypto currency.

Although, it is clear that the ledgers used for data exchange more than for currency. But they can be used in creation of blockchain model based on KYS principle. The development of such model assumes the creation of additional databases, which will link digital signatures of users with their real personalities, while at the same time setting restrictions on access to stored information. The introduction of the described scheme carries a number of positive things: such model will be able to store structured data about users that can be replenished, access will be made using cryptographic methods and it will be easier to submit customer data to the relevant authorities. Moreover, the financial institutions will be able to provide the channel for client information on a temporary basis, which means if a certain government body needs to check the tax documents, in addition to the fact that other documents will be restricted to access, also the time, for which the admission is granted, will be limited.

The need for such model is explained by the fact that it can become a solution responding to the aspects on which the crypto currency has been developed and the requirements for regulating its turnover. On the one hand, the desire of financial institutions to regulate the confidentiality of data will be met, and on the other hand, ordinary users will not be afraid of the fact that someone can illegally use information about them.

Such a model can make the process of exchanging data on customers between bank branches or other credit organizations and units engaged in AML / CFT activities many times faster and more efficiently. However, at the initial stage, such models, of course, will take a lot of time and besides, they will need legal support from the government.

If, legally, the state does not create an appropriate legal framework that will include certain norms and restrictions that ensure the stability of such a system and, most

importantly, eliminate opportunities by which this technology can be used for illegal purposes, such crypto currency payment system will not be able to perform its functions normally.

In 2017, the People's Bank of China banned Chinese exchanges of crypto-currency, citing violations of the law on money laundering. Such measures, the Central Bank of China has adopted to develop rules according to which exchanges, according to the requirements of certain authorities, will disclose information about their customers. This practice is now used by the United States. As we can see, the relevant bodies, first of all, need to resolve this problem legislatively. It is expected that financial regulators will sooner establish some legal restrictions than will develop such mechanisms by which the crypto currency will retain its advantages over conventional money and at the same time will meet the security concerns that society and the state; require, although the second option is significantly would accelerate the process of using the crypto industry as a payment system.

4. Conclusion

Summarizing all of the above, although the crypto currency really has the potential of a fundamentally new payment system, offering openness and lack of centralized management, there are also problems that needed to be solved. The system has drawbacks. The absence of real mechanisms to regulate such payment system forces the governments and financial regulators to look with caution and limit its use, instead of achieving a mutually beneficial position.

Due to these points, the main problem of AML/CFT sphere, of course, is the opportunity to launder money using this technology. The method described above is quite capable of eliminating this flaw with proper conception and proper implementation. It is possible that in the near future there will be new ways of regulating. However, governments may legislatively prohibit any activity related to the crypto currency until appropriate mechanisms are developed. But the problem is, that as a result of such prohibitions the entire crypto industry will have to return to the "gray" market.

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] Taya Arianova, The history of bitcoin: A short excursion into the past and future of the crypto-currency, <https://ru.insider.pro/investment/2017-09-08/istoriya-bitkoina-kratkij-ekskurs-v-proshloe-i-budushee-kriptoalyut/>
- [2] Mikhail Overchenko, Four leading world banks create a crypto currency, <https://www.vedomosti.ru/finance/articles/2016/08/24/654293-chetire-banka-kriptoalyutu>
- [3] Morgen Peck, Blockchains: How They Work and Why They'll Change the World, <https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world>
- [4] Hon Matt Hancock, Ed Vaizey, Distributed ledger technology: beyond block chain, <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain>
- [5] KYC and blockchain, <https://www.finextra.com/blogposting/13903/kyc-and-blockchain>
- [6] Dmitry Yakovenko, Bitcoin, young and uncontrollable, <https://stimul.online/articles/science-and-technology/kriptoalyuty-priglasenie-v-belle-epoque-ili-izderzhki-tsifrovoy-ekonomiki/>
- [7] Why should banks, regulators and payment systems have their own crypto-currencies, <https://habrahabr.ru/company/itinvest/blog/308738/>