

VIRTUAL CURRENCIES, A NEW BUSINESS DEVELOPMENT MODEL

Scientific Researcher Cătălin DRĂGOI

“Victor Slăvescu” Centre for Financial and Monetary Research, Romanian Academy, Romania
E-mail: icfm01@icfm.ro; hipercub@gmail.com

Abstract: *On the background of the development and maturity of virtual currency markets a new type of business or company emerged. The classic method by which a company becomes public by winning funds from individual investors is by selling shares in an initial public offering. What is called "initial coin offering" is in the area of cryptocurrency equivalent to an initial public offering in the world of the main investments, the initial offer of the currency acting as a collector of funds. Most often, initial coin offerings are used by new companies to circumvent the rigorous and regulated process of capital increase demanded by investment funds or banks. The paper aims to analyse how virtual currency work, what their characteristics are, and whether they can be an economic development factor.*

Key words: *virtual currency; initial coin offerings; business model.*

JEL Classification: *E40, M13, O16.*

1. Virtual currency

Shortly after the collapse of the American bank Lehman Brothers, which triggered the financial crisis of 2008, a new, it appeared a previously unknown economic phenomenon called the "virtual currency". The term "phenomenon" is not exaggerated because the existence of virtual coins implies a new environment, exclusively virtual with specific rules of issuing, holding and trading of the currency. The first virtual currency was the bitcoin, and his architect has remained so far shrouded in mystery, giving rise to many speculations about the intention behind the creation and development of virtual coins. Even though at the beginning the Bitcoin has lived in almost anonymously, its popularity has begun to grow slowly. Then, many other virtual coins appeared, so that after 10 years on the trading platforms over 1600 virtual coins were registered, many of them trying to attract investors' attention through new features different from others.

Since virtual currency demand has steadily increased since the emergence of bitcoin in 2009, concerns have arisen that the use of virtual coins unregulated in the global economy can become a threat to society, crypto coins being compared to pyramid schemes and economic bubbles. Transactions that occur through the use and exchange of these instruments are independent of the official banking systems and therefore simplify tax evasion as well as the financing of illegal activities. It has been said that the use of virtual coins is an index of money laundering and that it shows how large is the money laundering demand in the world.

As bitcoin is the best known virtual currency, the most transacted one, we will explain the features of the virtual currencies analysing the bitcoin. It was the first such currency, the subsequent ones having, more or less, similar features.

Created rather recently, in 2009, bitcoin is a decentralized electronic payment currency, without a financial institution or central bank, and without being regulated; its purpose is to ensure the financing and protection of business and investments without any constraint.

At the same time, the use of bitcoin term also refers to the distributive, peer-to-peer sending of data, and to the open source operation program, available to anyone.

The asymmetric cryptography, thus called because it uses two different encrypting keys, plays an important role in setting the basic functions of the bitcoin currency, ensuring its security of possession and spending (for instance, the bitcoin can be used only by the rightful holders and spent just once). Public and private, at the same time, the asymmetric cryptography uses the pair of asymmetric keys both for encrypting and for decrypting.

Bitcoin encrypting is done using the public key, but decrypting is done only using the private key that corresponds to the public key. The private key also provides, besides decrypting the text, a digital signature which allows checking by anyone, by access to the corresponding public key.

Cryptography makes the bitcoin anonymous, confidential for holding and transacting. It is deposited in the computer of a holder in a money purse file; it can be sent to any holder of a bitcoin address. The amounts are transferred between the public accounts through the public cryptographic keys; the transactions are confirmed, which prevents the repeated spending of bitcoins.

The incapacity of a central authority to manipulate the bitcoin, for instance to create more bitcoins than produced and held in the peer-to-peer network, averts the bitcoin from inflation.

Nevertheless, the bitcoin is highly volatile, which is why even the websites that accept bitcoin payments, actually accept this currency only for the transfer of funds at the current rate.

The long-term holders evaluate the bitcoin as a currency that will take the place of the other currencies, but the short-term holders consider the bitcoin just a speculative investment.

Furthermore, next to the disadvantage of a high volatility, the bitcoin has a rather slow system of processing and confirming transactions compared to the Master Card and Visa systems.

It seems that the underground, illegal, black and grey economy, seem to use rather well the bitcoin for transactions of guns, drugs, traffic of people, etc. however, the legal business also seem to need the bitcoin for a rather cheaper transfer between incompatible information and financial systems; for instance, the transfer between two currencies can be done, under particular circumstances, easier through the cryptocurrency (in countries such as Russia, India, China etc.).

Although the bitcoin requires important computing resources, the cost of each transaction is below 5 cents per transaction.

The bitcoin relies on the concept of blockchain, a network of knots (each knot being a computer, implicitly an internet used that validates and retransmits the transactions). Each knot receives a copy of the blockchain, each modification being perceived instantly by the knot, as it is connected to the network.

Blockchain decentralisation is relevant because, being a digital registry, it encrypts the information in mathematical formulations on the basis of other encrypted data, forming a network. Besides checking the authenticity of transactions at any moment, the knots also compete in solving computing problems and earning bitcoins.

In the case of the bitcoin, the blockchain contains data referring to transactions (receiver, sender and number of bitcoins). The blockchain has some kind of unique fingerprint, hash, which identifies a block and its content. The hash function is a mathematical function which, when applied on the input data, produces output data of a pre-set size. The blockchain hash is calculated once a block appears in the chain and the hash changes at the first transaction within the block. Besides, the blockchain also contains the hash of the previous block.

Every bitcoin holder has available a copy of the blockchain; at each newly created block, each of the network participants receives the block which, after being checked by all the network participants, and after the unanimous validation, can be introduced within the chain.

Those who participate in encrypting the data within the blockchain are called miners, because the bitcoin was designed as a limited resource (similar to the gold), whose

exploitation is done with great effort and consumption of energy. The terms mining and miner, although used both in English and in Romanian, in the field of cryptocurrencies, are somehow improper; I think that the terms of encrypting and encrypter define better the activity of encrypted writing of the transactions within the blockchain, and the person doing this. In order to have success in mining, which presumes competition, only the first one that is successful in registering in the blockchain, the miners pool their computing capacity, and in case of success, each participant in the pool is rewarded proportionally to the percent of the total computing power cumulated for the accomplishment of that blockchain.

2. Initial coin offering (ICO)

For the traditional companies, there are some ways to raise the funds necessary for development and expanding.

A company can start only with the funds brought by the company founders, and grow as its profit allow, remaining only at the company owners, but they have to wait for the funds to accumulate.

Another way, is that the company turns public, raising funds from individual investors, by selling shares in an initial public offering (IPO).

The initial coin offering (ICO) is, in the field of cryptocurrencies, the equivalent of IPO in the mainstream investment world. The initial offering (IO) acts as fundraiser. A company that wants to create a new coin, an application, a good or a service, launches an ICO.

The investors purchase the offering either with fiat coin, or with tokens (particularly bitcoin or ethereum). In exchange for their support, the investors receive a new symbol of the cryptocurrency specific to ICO. The investors hope that the token will work in the future, providing a good return on their investments.

The company that has the ICO uses the funds from the investors as means to continue its goals, to launch the product, service or digital coin.

The ICO are used by new enterprises in order to avoid the rigorous and regulated process of increasing their capital, demanded by the investment funds or by the banks.

The investors purchase the tokens launched by the ICO hoping for a fast and strong return for their investments. The most successful ICO of the recent years give the investors reasons to maintain this hope, because of the huge profits, in some cases. However, this enthusiasm of the investors may also cause losses. Because most of them are not regulated, the ICO became a space for fraud, where some issuers are trying to deceive the over trusting and uninformed investors.

When a company wants to raise funds by an initial coin offering, it develops a business plan that describes the project, as clear as possible, what need will the project ultimately fulfil, how much money it has for this project, what type of money it accepts and how long will the ICO company function. During the ICO campaign, the investors and supporters of company initiative buy some of the cryptocurrency distributed against fiat money or virtual coin. These coins are called tokens, and are similar to the shares of a company sold to the investors in IPO transactions.

If the collected money is not enough for the minimal funds required by the company, the supporters are refunded, and the ICO is considered a failure. If the money requirement is raised within the specified term, the collected money is used either to start the new system, or to complete it.

The ICO are similar to the initial public offering and with the crowdfunding. As with the initial public offering (IPO), a part of the start-up of company is sold to make money for the operations of the entity during an ICO operation. However, while the initial public

offering gathers investors, the ICO gathers supporters who want to invest in a new project, similar to a crowdfunding event.

There are structural differences between the ICO and IPO. The ICO are decentralized (no governing authority), the ICO are largely unregulated, which means that the governmental bodies do not monitor them, and the ICO are laxer in terms of structure, than the IPO, due to the decentralization and lack of regulation.

The ICO can be organised in several ways. In some cases, a company sets a specific purpose or limit for its funding, which means that each token sold within the ICO has a pre-set price and that the offer of the total token is static. In other cases, there is a static offer of ICO tokens, but a dynamic objective of funding, which means that the distribution of tokens by the investors will depend on the received funds (and that the higher are the funds received within the ICO, the higher will be the value of the token). Some ICO have a dynamic offer which is determined by the value of the received funding. In these cases, the price of a token is static, but there is no limit to the total number of tokens, except for some parameters, such as the length of ICO period.

In an IPO, the investor receives shares of a company in exchange for his/her investment. In the case of ICO, there is no share to talk about. For ICO, in most cases, the investors pay in a popular token, such as the bitcoin or ethereum, and receive in exchange a corresponding number of tokens.

The initial coin offering usually has three stages of token purchasing and reaching the targeted level of capitalisation.

There are two levels of the capital collected by an initial coin offering. The minimal level of capital, which most ICO reach easily (the softcap), and the targeted level of capital (the hardcap). The first stage – “private sales”. Negotiations take place between the team launching the virtual coin and specific investors that can receive preferential prices. The second stage is the “pre-sales” stage, in which any natural person or company can reserve a specific number of coins, in an escrow account. The third stage, the actual sale, also called Crowdsale, in which anyone can buy tokens; this is the moment when the ICO is actually launched.

Usually, the investments in the initial coin offerings are done in other virtual coins, most often bitcoin or ethereum. There are few ICO that allow investments directly in fiat coin. The ICO function on smart contract basis for the ethereum, which means that when the coin is launched, the investors from the first two stages automatically receive tokens of the newly launched coin, in exchange for the invested amounts.

Between the launch of a virtual coin and its listing on the exchange platforms, there is a period necessary for the growth of that coin. For most investors, the ICO proved to be the most profitable ways of investing in the cryptocurrency market.

According to statistics, the ethereum was launched at a price of 0.314 USD, the yield of the investment reaching 340,000% two years later. NEO, another cryptocurrency, was launched at the price of 0.03 USD, reaching a yield of 425,000%.

The investors in ICO operations before the launch of the coin are motivated to buy tokens in the hope that the virtual coin will be successful after its launching. If this happens, the value of the tokens bought during the ICO will go higher than the price set during the launching of the coin and will therefore get higher gains.

This is the main benefit of an ICO: the potential for huge profits. Thus, in 2017, there were 435 successful ICO, each of them gathering in average 12.7 million USD. The total amount for 2017 was 5.6 billion USD, the biggest 10 projects taking 25% of this total. Furthermore, the token purchased during the initial offering returned, in average, 12.8 times the initial investment, in terms of USD. In the first quarter of 2018, ICO brought funds worth of 6.3 billion USD, already exceeding the total amount of 2017.

Are the Initial Coin Offerings legal?

In the United States, there are no specific regulations for the ICO; however, according to the classification of the digital currency, it may fall under the jurisdiction of the Securities and Exchange Commission (SEC). The regulatory authority has to monitor the transactions with various financial products. If SEC considers that, a currency is the equivalent of a security, then the company behind it might have to register with the regulatory authority.

In Europe, the European Securities and Markets Authority (ESMA) launched, last year, directions regarding the ICO. The regulatory authority said that the initial offerings that qualify as financial instruments might fall under the incidence of the relevant laws regarding money laundering or investments.

Last year, the People's Bank of China declared the ICO illegal, warning the people against the risks of investing in them. Shortly after, South Korea followed, by banning fundraising through virtual currencies.

3. Frauds and dangers of the ICO

„ICO actually are start-ups; exactly as in the real world, 18 out of 20 will fail.¹”

Investing in ICO is a risky business for several reasons. Often, people invest money in products that do not yet exist. Although this would not seem different from investing in other start-ups, the people betting on ICO usually are simple investors.

These projects also have high rates of failure. Already, hundreds of coins “passed away”, which means that the projects behind them were scams, or did not materialise. Dead Coins is a website presenting all the cryptocurrencies that fall within this category, counting until now, over 800 digital tokens which it considers “dead” (see the name of the website).

Because of the lack of regulation, the frauds are rather spread within the industry. This opens widely the gate for the Ponzi schemes and cheatings, phantom companies appear and ask money from users seeking substantial gains. Recently, SEC, the institution regulating the US capital market, announced that it identified such an operation, which gathered, fraudulently, 600 million USD.

One of the problems of the system is exactly the ease of creating new tokens. There are online services that allow the generation of cryptocurrency tokens in a few seconds. ICO administrators generate tokens in agreement with ICO terms, receive them and distribute them as they please, transferring them to the individual investors.

4. Conclusions

There are many companies that have succeeded to launch goods and services through the initial currency offer. However, the easiness with which anyone can create a coin (tokens), makes many of the ICO to be thought as scams from the very beginning. That's why in order that this kind of fund-raising that is conducive to business and economy development to be successful, it would be necessary to have methods and authorities to monitor companies, to analyse companies' guarantees for launching an ICO and underwriting for it.

Even if crypto coins would disappear, technological gain is considerable for mankind. If we take into account that thousands of IT, banking, capital market specialists have been involved in the creation of thousands of virtual coins, we can assume that some of the innovations of the crypto currencies' environment will be taken over by other areas, creating points of technological inflection, the rapid development of some domains and

¹ <https://www.businessmagazin.ro/cover-story/tehnologia-care-ar-putea-schimba-lumea-16977439>

implicitly material well-being. (I would mention only two examples of the "smart contract" automated technology developed for the ethereum currency and the transfer technology of the ripple coin that is so fast and it allows large volumes of data so that Western Union wants to take it over).

As a first step, the regulation of crypto coins and their classification as securities represent an important step in reducing their volatility, but an international effort is needed to find all the legal levers to bring to light the role, purpose and their operation mechanism.

References:

1. Ciutacu, A., 2018. Ce sunt criptomonedele și cum poți să cumperi Bitcoin, Ethereum, Ripple sau alcoins. Tot ce trebuie să știi despre criptomonede, ICO și portofele electronice și cum transformi monedele virtuale în bani adevărați. *Ziarul Financiar*, 23.01.2018 [online] Available at: <<https://www.zf.ro/eveniment/criptomonedele-poti-cumperi-bitcoin-ethereum-ripple-altcoins-tot-stii-criptomonede-ico-portofele-electronice-transformi-monedele-virtuale-bani-adevarati-16953234>> [Accessed 2 March 2019].
2. Clayes, G., Demertzis, M. and Efstahiou, K., 2018. *Cryptocurrencies and monetary policy*. [online] Available at: <<http://bruegel.org/2018/06/cryptocurrencies-and-monetary-policy/>> [Accessed 2 March 2019].
3. Dobrescu, E.M. and Dobrescu, E.M., 2017. Future of virtual currency. *Journal of Financial and Monetary Economics*, 4(1), pp.118-124.
4. Fernández-Villaverde, J., 2016. *Cryptocurrencies: Some Lessons from Monetary Economics*. [pdf] Available at: <<https://www.sas.upenn.edu/~jesusfv/Cryptocurrencies.pdf>> [Accessed 2 March 2019].
5. Frankenfield, J., 2019. *Initial Coin Offering (ICO)*. [online] Available at: <<https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>> [Accessed 2 March 2019].
6. Marinelweb, 2018. *Înțelegerea valutei criptate (Bitcoin). Cum funcționează, ce o conduce, ar trebui să o cumperi?* [online] Available at: <<http://www.marinelweb.com/intelegerea-valutei-criptate-bitcoin-cum-funcioneaza-ce-o-conduce-ar-trebuie-sa-o-cumperi/>> [Accessed 2 March 2019].
7. Roubini, N., 2018. *The big blockchain lie*. [online] Available at: <<https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10>> [Accessed 2 March 2019].