VIRTUAL CURRENCIES, THEIR TECHNOLOGICAL INNOVATIONS AND CENTRAL BANKING

Bledar Hoda, Research Department, Bank of Albania[1], May 2018

1.WHAT ARE VIRTUAL CURRENCIES?

Cryptocurrencies or **virtual currencies** are digital currencies issued by private individuals or entities that do not have a legal tender granted by a sovereign state or an international institution. Their market value fluctuates as a result of the demand of individuals for transaction or their expectations of potential market price increases in the future. Electronic media uses different terminologies to refer to virtual currencies. In this article, the terms *"cryptocurrencies", "digital currencies"* and *"virtual currencies"* are used interchangeably.

The infrastructure of a *cryptocurrency is a decentralized electronic payment system*, available to the public and regulated by a privately drafted electronic protocol. The acceptance of the regulatory electronic protocol by the agents that operate the infrastructure is regulated through financial incentives granted to the users by the protocol itself. These incentives consist in (i) financial income for the agents operating the system and (ii) the usefulness allowed to individuals by the availability of this payment system. The electronic protocol performs the role that payments guaranteeing central authorities perform in traditional payment systems, like central banks, regulatory authorities or private enterprises like Visa and MasterCard. The blockchain technology underpinning the virtual currencies operates without the need of a central party to authorize these transactions. Also, the creation of money is realized by the same electronic protocol that enables payments' transactions. In this way, the creation of virtual money takes place at a deterministically predictable rate defined by the operating electronic protocol.

The first and one of the most traded virtual currency considered in the paper is Bitcoin. It is the most widespread virtual currency with easily accessible quantitative data regarding transaction value, volume and other trade details. The anonymous author of the cryptocurrency Bitcoin, Satoshi Nakamoto, published the *Bitcoin* electronic protocol documentation and created the first Bitcoin coin of 50 units on 3 January 2009 (Nakamoto, 2008). Electronic money is not an innovation for the economic literature. It has been present at least since the 90s with the massive spread of credit and debit cards or in the M-pesa format (Kaminska, 2015). However, Bitcoin refers also to the technological innovations that its author proposed for carrying out transaction with this currency. In this paper, depending on the context, the term Bitcoin will have the meaning of money, the technology that this currency represents or both.

[1] *This short summary is based on a yet unpublished Discussion Paper originally written in Albanian with the same title at the Bank of Albania and submitted by the author in May 2018.*

Although initially the public was sceptical about *Bitcoin*, the number of electronic transactions carried out in the digital currency Bitcoin increased exponentially. The spread of Bitcoin use has been non-negligible for the financial industry, the public and national and international authorities. At the end of 2011 the number of confirmed transactions denominated in Bitcoin was no more than 5-6 thousands per day. In the last months, before the submission of this paper (October 2017 - February 2018), the number of transfers through Bitcoin fluctuated around 200 - 400 thousands transactions per day. In the same period the value of these transactions reached around USD 1 - 4 billion a day. The amount of income generated by the private agents that maintain the infrastructure of Bitcoin from these transactions reached around USD 20 - 40 million per day. The magnitude of these incomes has prompted other private entities to propose other currencies that operate with similar infrastructure. At the time of writing this paper, the number of virtual currencies in decentralised computer networks amounts to more than 1000.

The attention of the financial industry as well as of academic actors is focused on the infrastructure of Bitcoin. The technological innovation implemented in the infrastructure of Bitcoin transactions is called blockchain. The distributed ledger technology (hereinafter DLT) is a broader term for the blockchain technology that includes modified version of the infrastructure for the needs of various industries. In this paper we will refer to it with the term *decentralized transaction ledger technology (DTLT)*. The function of this ledger is regulated by an electronic protocol drafted by the author of Bitcoin.

The infrastructure of *Bitcoin* is composed by the transaction electronic ledger and by powerful computer units operated by private agents called 'miners', who are financially motivated by an electronic protocol. The private miners may enter or leave this infrastructure maintenance business according to their financial motivations. The ledger is *decentralized* because the miners that maintain the system record the transactions in the only public copy of the ledger, leaving traces only in this unique ledger and not in private ledgers of each miner. Its reliability is granted by the implementation in the electronic protocol of (a) *cryptographic security elements* and by (b) financial remuneration that motivate the miner to maintain the system's (decentralized) infrastructure. Agents' financial remuneration consists in (i) transactions' commissions and in (ii) a subsidy that the electronic protocol allocates by creating new coins *(seigniorage)*. The creation of new Bitcoin money is accomplished by rewarding miners for each finalization of a transaction block. The ledger requires the consent of the agents that maintain the infrastructure of the system. The size of financial remuneration provided in the protocol dictates that consensus is reached in the normal operation of the infrastructure. Two key features, cryptographic security and *decentralisation* of payment infrastructure, make unnecessary the presence of a regulator or authority that guarantees the reliability of the transactions.

Due to these characteristics provided in the electronic protocol, the technological innovation underpinning the ***blockchain infrastructure*** allows individuals some advantages in making payments compared with the current infrastructure monitored or regulated by national or international supervisory authorities. First, the cryptographic protocol elements enable the anonymity of the payments' payers andpayee. This does not prevent the *decentralised transaction electronic ledger* to enable *the registration and tracking of transactions or any change of ownership of Bitcoin* coins. Second, conducting transactions with this technology (the ledger) does not require a central *authority* or *regulator* that guarantees the reliability of the transactions. *Blockchain allows* ***processing*** *and* ***finalisation*** *of* a transaction to be unified in one step. *Fast finalisation* completion allows for a ***reduction in the time*** of performing a transfer and ***minimizing counterparty risk***. Third, the lack of a central regulator, the fast finalisation of a transaction and the subsidy that the electronic protocol provides, allows private agents to ***reduce the financial cost*** of a transfer.

These advantages have prompted a rapid rate of spread of Bitcoin's use, as can be seen by the high number of daily transactions denominated in Bitcoin. The ***blockchain*** technological infrastructure is an innovation that gives a positive impulse to the productivity of private or public enterprise units in almost all areas. Virtually any valuable transaction, action, or objective can be recorded and tracked in such a ledger minimizing the counterparty risk and the financial or time costs associated with the maintenance of the current systems. The high number of other virtual currencies not regulated by the authorities is based on similar technology. Also, the financial and information industries are showing interest in implementing this technology in a new wave of financial products. In this regard, the modification of the electronic protocol enables the formulation of *blockchain* technology according to the needs of public regulatory authorities or private enterprises.

II. THE POTENTIAL IMPACT OF BITCOIN AND OF THE TECHNOLOGICAL INFRASTRUCTURE

The current spread of Bitcoin is motivated by the incentive of individuals to earn quick profits driven by expectations of prices increases, by the anonymity of the parties involved in large volume transactions, by the low cost of transactions, and by the short time of their finalisation. Decentralized payment performance and electronic recording (chain) of transactions makes difficult to monitor the financial transactions denominated in *Bitcoin*. Pre-emptive measures to stop the phenomenon in the form of transaction supervision are difficult due to the anonymity that enables the transactions in *Bitcoin*. **In most developed countries the regulatory and legal authorities are not in a rush to take limiting measures against transaction with virtual currencies.**

A massive hypothetical spread of Bitcoin is not expected due to the conservative and rational behaviour of individuals and the high risk of cash holdings in virtual currencies, Bitcoin or others. The massive spread of Bitcoin as a currency is considered a hypothesis which does not find support in academic

or institutional circles. Likewise, the high price fluctuations of Bitcoin make it a speculative monetary tool.

The monetary authorities of different countries have been careful in their public communications not to stimulate the use of these currencies. Most of them have been short of indicating any signstoward issuing the digital version of national currencies. However, countries such as Sweden, China and a few developing countries have considered the possibility of issuing a national electronic currency to meet the needs of respective nationals for electronic payments. Such an approach provides higher security for citizens in exchange for anonymity. The intention to issue a national electronic currency in these countries is mainly related to the specifics of their own economies. Currently, issuing national electronic currencies is not considered an alternative by most developed countries.

However, the virtual currency *Bitcoin* is considered an innovation, whose infrastructure has served to prompt discussion about the possibility of improving the international payment system between international financial agents.

The efforts of the authorities in various countries are focused on the potential of technological innovation that enables the electronic transaction ledger (blockchain). ***The implementation of the technological infrastructure aiming at improving the existing payment system is the focus of the authorities of many developed countries over a long-term horizon.*** The implementation of the technology is assessed to have an impact on (i) lowering transaction time and financial costs and (ii) further containing liquidity and credit risk. Also, some of the monetary authorities are looking at the possibility of promoting financial technology in the private sector of the respective economies.