VIRTUAL CURRENCY AND GLOBAL BUSINESS - THE NEW TREND IN THE NET-ECONOMY

Cătălin DUMITRESCU, PhD Lecturer
Athenaeum University, Bucharest, Romania
catalindumi@yahoo.com

Matei DUMITRESCU, BA Student
Department FABIZ, University of Economic Studies, Romania
mateidumi7@gmail.com

Abstract: *The rapid development of information technology has made generating cryptocurrencies and fast, cheap and uncontrollable transactions using virtual space possible. Among virtual currencies, Bitcoin is considered to be a major challenge for traditional financial operations, and especially for the fight against money laundering and terrorist financing. This article presents the following points of discussion: the spectacular appearance of Bitcoin, its exponential evolution, its popularity, its growing demand, lack of anonymity and predictability, the cross-border nature of transactions.*
Keywords*: Blockchain, Ledger Technology, Bitcoin, ETH, cryptocurrency, cryptography, technology, digital*
JEL Classification : *C23, C26, C38, C55, C81, C87*

Introduction

Lately, the crypto economy has come out of the shadows and started to be discussed publicly, but even now few understand its meaning and capabilities. Being a trend of the 21st century, it is already difficult to ignore this phenomenon. Since 2016 various banks, organizations, and parliaments are discussing the crypto economy and its effects. What is the crypto economy? How do cryptocurrencies work? It is a completely new scientific issue, not only nationally but also internationally. Current literature in the field of economics

describes no work that explores the essence and operational mechanisms of electronic means of payment based on cryptographic solutions. However, progress and, in particular, the development of virtual communities based on new technologies have generated new forms of transactions and methods of regulating them, far exceeding the knowledge and existing legal framework. Therefore, the purpose of this research is to present the essence and capabilities of cryptocurrencies from an economic point of view.

Bitcoin is an innovative payment system and a peer-to-peer digital currency that works online, essentially like money. Its creation is based on an open source encryption protocol. Since its appearance in 2009 by an unidentified programmer Satoshi Nakamoto (Nakamoto, 2008), Bitcoin has gained in popularity. There are now approximately 1.8 million users of the Bitcoin system worldwide. In recent years, the currency has grown exponentially in visibility and has seen acceptance by suppliers and buyers, as well as fluctuating prices.

The current capitalization of the Bitcoin economy is estimated at more than $7 billion, both real goods and online services being sold. Bitcoin has become "convertible" into US dollars, Euros, Japanese yen, Russian rubles, etc. with trading sites offering these trading services. Blockchain technology is commonly known as the technology behind Bitcoin. Although Bitcoin was indeed the first practical application of blockchain technology, its features make it flexible enough to be used in various fields - from medical to governmental services. Moreover, the financial services industry is among the strongest candidates for the development of solutions based on distributed ledger technology. Within the Net-Economy and the financial services industry, there are different possible applications for the blockchain. Thus, it is necessary to understand the impact that these applications will have on the management of the Net-Economy, but also for the management of transactions by financial institutions.

1. Ledger Technology - Blockchain

Crypto-economics is the use of incentives and cryptography to design new types of systems, applications and networks. As the crypto-economy grows, governments and financial institutions must apply well-established government regulations and practices. Currently, the lack of regulations prevents governments from adopting the Net Economy. Crypto-economics is not a subsector of economics, but an area of applied cryptography that takes into account economic incentives and economic theory. Bitcoin, Ethereum, Zcash and Blockchain are just a few crypto-economic products. Blockchain is an unquestionably ingenious invention. But since its inception, it has evolved into something larger

and the common question is: How does this technology work? To understand its operation and functionality, it is necessary to first begin with the definition of technology.

At the basic level, a blockchain is an accounting system - a registry. Blockchain is a distributed digital register that records transactions in which values are exchanged. The distribution is validated by the existence of several copies of the transactions. The ledger is distributed among several participants, called nodes, on a Peer-to-Peer (P2P) network (Figure 1). Nodes are the equivalent of the servers in the example above. Nodes perform three main types of functions; sending and retransmitting transactions, updating the blockchain new blocks related to the transaction (consensus) and retransmitting transaction blocks (Tapscott & Tapscott, 2016).

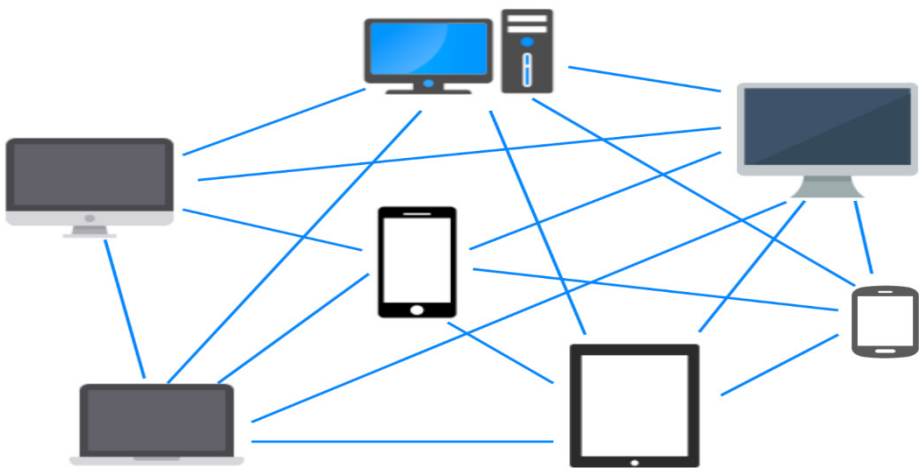

Figure 1: Peer-to-peer (P2P) network.

Blockchains can be classified into different subcategories, depending on the authorization required for network nodes to act as verifiers and whether access to blockchain data (blocks) is public or private (Peters & Panayi, 2016). The first category of authorization addresses the process of verification and consensus with or without permission:

- Blockchain without permission - anyone can configure a node, connect to the network and participate in the verification process.
- Blocked chains allowed - mining privileges are delegated by a central authority or consortium.

The second classification refers to access to public or private data:

- Public blockchains are blockchains in which anyone can obtain a copy of the register and initiate transactions.
- Private blockchains are blockchains in which permission is restricted to users within an organization or entity.

On public blockchains, users can connect to one or more nodes and broadcast (initiate) a transaction. When a user makes a transaction, each receiving node transmits the transaction interface to its connections until all nodes finally have a copy of the transaction. New blocks are created when certain nodes, or all nodes, assemble transaction blocks in time stamped („block creation time"), which are transmitted over the network. Consensus is established when all nodes or a majority of nodes have received a valid block of transactions that is appended to previous blocks in the blockchain. Each block is digitally signed and includes the signature of the previous block. The associated digital signatures guarantee the integrity of the transactions registered in the blockchain and it is not necessary to maintain a centralized copy (Egilsson & Valfells, 2017). The time interval between newly created blocks is called „block creation time".

Bitcoin System Features

Decentralized system. Bitcoin is the world's first complete decentralized digital payment system, in the sense that there is no denomination in a known currency, national or regional (Dollar, Euro, Yen, Pound etc.). On the other hand, currency generation cannot be located in a certain country, but in any country from where the computer is operating on the network. Being located on the Internet, transactions are transnational because The Internet itself is a transnational space.

Until the advent of Bitcoin, electronic transactions could only be completed with the existence of a third party, holder of a transaction log, to prevent the expense of the same amount twice. For example, entity A that sends money electronically to another entity B needs the services of a third party, such as a credit card issuer. In return, the third party keeps a record of all transactions and balances of all account holders: the money will be deducted from A's account and added to B's account. With the Bitcoin system, all digital transactions on the network are centralized in a public register, observable by any user on the network - a complete database, called blockchain, which is constantly growing, because it contains the complete record of each exchange, from the beginning of Bitcoin. Through an algorithm, the task of validating each

transaction is randomly distributed on the network (proof-of-work algorithm). To ensure their correctness, new transactions are checked against the blockchain database. As such, the third party is made up of thousands of users involved in validating the same transaction. In this way, the major technological problem that Bitcoin has solved is the ability to prove the transfer of ownership without the need for a third party. Currently, confirming a transaction takes an average of 8 minutes.

Double money spending avoided: The global Bitcoin system ensures single money spending through distribution validation activity. Users provide computing resources to validate Bitcoin transactions and maintain the registry Bitcoin public transactions. As an incentive for their work, when validation takes place, they sometimes receive bitcoins and a fee also expressed in bitcoins (actually, in fractions of bitcoins). In this way, some of the users they are „miners", similar to gold mining workers. All transactions and thus the transfer of Bitcoin property, are registered, marked with the date of execution, displayed in a „block" of the blockchain and validated. Therefore, the issue of double spending is resolved without the intervention of a third party.

Traceability and lack of anonymity. Each transaction is potentially tracked in its evolution, because it is permanently signed and visible on the blockchain (Bitcoin Price Index 2018). But the anonymity of the addresses is still a questionable issue. Within the system, users are identified only by public keys. But an analyst in the field of cryptography, which seeks to de-anonymise users by associating them with a real identity, could make this through a network analysis and the association of other information external to the system. Other researchers consider that the addresses are pseudonyms and the real identity of the users is easily detectable, unless specialized anonymization software has been implemented.

Open market, volatility. Although transactions are denominated only in bitcoins, the US dollar value of a Bitcoin is established on open markets, just as the exchange rate of other currencies is established, so it derives from the value that the market assigns to it.

Control. Who owns the technology behind an email? No one. Similarly, control being distributed across the network means that no entity or person controls the system; Bitcoin has been designed so that only cryptography can control its creation and management. Users around the world are "controllers". Even developers cannot impose a change in the Bitcoin protocol, just as no one can impose a certain software or version on regular users of computers or mobile phones. But a user who wants to be compatible with others, in order to benefit from the perks of the community, must implement software with the same rules as the entire community.

Limiting money supply and storing value. The Bitcoin system was designed to provide a limited, predictable amount of money: 21 million. By 2013, half of the total amount was generated; by 2017, three quarters were generated. The money supply limitation hypothesis is included in the algorithm for creating and managing the Bitcoin system. He has the ability to automatically reduce incentives for "miners" as more and more enter the community. This limitation of Bitcoin currency mimics the world's gold reserves there is a limited amount of gold on earth and miners are looking for it until it probably runs out. But the attribute of gold is that it stores value, even if the limited quantity is ignored, while the Bitcoin value is only conventional and extremely volatile.

The advantages of technology and mathematics. Decentralization and mathematics, specifically public key cryptography, have eliminated the risk of not controlling transactions. Public key cryptography is an asymmetric scheme that uses two encryption keys: a public one, which encrypts the data, and an appropriate private key, for decoding. Each node of the network is assigned a public key, which can be seen by anyone and a private one, kept secret by the user. Anyone who owns a copy of the user's public key (or node) can encrypt information on which can only be seen by the user. The two keys are mathematically related, but it is very difficult to deduce the private key starting only from the public key. A criminal who attacks the network and wants to deduct the private key from the public key needs immense computing power and time. As for the keys are longer, the more secure the message, the shorter the key, the faster it can be applied, this being the well-known difference between security and functionality.

A transaction consists of a message containing the recipient's public key, „signed" with the sender's private key, registered, marked with the date and time, and validated on the network as a blockchain. Transaction validation ("mining") requires time and computing power, as the entire history of that specific Bitcoin sent or generated it must be reviewed and verified from its origins. In this context, mining is a mathematical process, such as finding prime numbers: it is easy to find small prime numbers, but it is difficult to detect large ones (consisting of dozens of digits). To find bigger and bigger prime numbers, advanced computers are used and finding a new big prime number is considered a scientific achievement. Similar principles are applied when a series of data (a block) matches that of the „miner" for the certification of the transaction. The miner obtains a bitcoin allowance and a fee when the transaction is certified. The allowance is getting smaller and smaller as more bitcoins are mined around the world.

2. The dark side 0f Bitcoin

The Internet can be divided into surface web (common users), deep web (connoisseurs) and dark web (Dark Web) for illegal transactions. The surface web, or public web, is the Internet, as most of us know it. The public web includes any common search engine, such as Google or Yahoo. However, the deep web is all that a common search engine cannot find. The deep web is assumed to be 400-500 times larger than the surface web. So, most of us have used only a small portion of the Internet (BrightPlanet, 2014). The Dark Web is a very small dimension of the deep Web. The Dark Web is only accessible through a special web browser called the Torr browser. Using the Torr browser, you can access the Torr network, which is an anonymous network. The Torr network was developed by the US Department of Defense and was intended (in the first phase) for intelligence agents („The Deep Web vs. The Dark Web," 2015).

The Dark Web is now well known for its illicit activities, black market business in the field of crime. Licensed users use the dark web to buy and sell drugs, hormones, children, child pornography, counterfeit currency, identity theft, illegal sale / purchase of weapons, acts of terrorism, money laundering, hacking attacks and malware attacks. What is the preferred currency for all these illegal activities? Bitcoin. Bitcoin is the main currency of the dark web; therefore, we can say that most Bitcoin transactions, which are currently carried out, are related to illegal activities. This is facilitated by the fact that the Bitcoin currency is not tracked in relation to other currency units, being easy to trade for illegal business. Initially, Bitcoin was not conceived as a currency of criminals, but, over time, it became the main currency for criminal activities. Because Bitcoins continue to be used in this way, financial institutions are very unlikely to be willing to use Bitcoins as their trading currency. Financial institutions have guidelines to follow, such as anti-money laundering regulations and anti-terrorism legislation. In the future, Bitcoin coin-generating networks could be banned internationally and the Dark Web banned. Financial institutions will most likely use another cryptocurrency or even create their own cryptocurrencies, using regulated Blockchain ecosystems.

3. Risks

A comprehensive risk analysis was conducted by the European Banking Authority (EBA) in a study published in July 2019 (European Banking Authority 2019). Risks are classified according to their origin and intensity.
Comparing conventional payment systems, used in barter transactions or

clearing systems, with Bitcoin (or other virtual currencies), the EBA highlighted the following:

1. Governments have a fundamental role to play in providing currency and control monetary arrangements, including quantity of money from the channels of circulation of the economy. In this matter they have a monopoly. Behind Bitcoin is a mysterious man or group of people. Bitcoin creation is based on complicated math and algorithms, allowing anyone to extract virtual currency through computing power of the computer.

2. Conventional currency flows are tracked by use of a reliable international reporting system. The size of virtual currency systems is difficult to be assessed in view of the lack of reporting of data sources.

3. The supply of conventional money originally appeared in the cause of the needs of the real economy. The desire for virtual currencies arose due to demand from members of the virtual community, such as players on computer, to have a fast and cheap way "Appropriate to the system" of financial trading among users and for rewarding winners.

4. Transactions are under strict and vigilant control at national and international level in accordance with the provisions of the legislation on money laundering. Criminals are able to launder money because they can deposit and transfer quickly, globally, irrevocably and under the protection of a pseudonym. Transactions can be pursued.

Bitcoin Regulations

There are debates at various levels about some open issues: is Bitcoin a currency and if so no, how can he be treated? As software, asset, property? The same features that make up the Bitcoin attraction as a method of payment allow users to evade tax, launder dirty money, sell illicit goods (drugs, weapons, criminal charges). Governments and legislators have been constantly concerned about the evolution of Bitcoin, as well as of the "anonymity" of the transactions or, more precisely, their pseudonymous character (Ometoruwa, 2018). Australia, Germany, Finland and Canada were among the first countries to officially accept Bitcoin. They held several international conferences especially in the European Union, the United States, Japan and Australia which addressed the essential levels of the revolutionary new payment system: technological, economic, security and legality. There are many enthusiasts and even "evangelists" of Bitcoin, who have adopted it as a currency of payment or exchange, but after the discovery of use for criminal purposes and the fall of several companies,

both the use and the value of Bitcoin have decreased. An informative website has been created to update the evolution Bitcoin regulations. More and more companies around the world, including Romania, are accepting payments in Bitcoin instead of cash and consider it a legitimate source of funds.

The role of Bitcoin in money laundering

Bitcoin networks have offered a new "tool" for money laundering, due to the three functions of the network - decentralization, the impossibility of identifying partners who establish a transaction and the ease of transactions. First, the decentralized way in which the Bitcoin network is built allows users to transfer their financial value to each other without the involvement of a third party.

A key strategy in the fight against money laundering regulations is to monitor intermediaries between buyers and sellers, in order to limit their ability to transfer values without control. Second, even if each transaction is stored and can be tracked in the blockchain, no connection can be established with the individual or organization behind that transaction. The Bitcoin ecosystem only reveals the arbitrary sequence of numbers which is the public key, while the private key is kept hidden, which makes the link between the real identity and the public address of Bitcoin extremely difficult to find (Cascarilla, 2015). This problem is exacerbated by the ease with which a user can have more e-wallets, giving them more public addresses, which leads to the limitation of methods to combat money laundering. Finally, the speed and ease of transactions in Bitcoin, make this network a much more practical method for money laundering, compared to the traditional method, cash payment. As with money laundering (Fiat Money), it is difficult to quantify how much money is actually laundered through Bitcoin. The FBI, the European Banking Authority and the G7 Financial Action Task Force all recognize the role of Bitcoin ecosystems in money laundering.

Conclusions

Blockchain has great potential. It provides a huge amount of data in a short time and it reduces costs by diminishing operational risks and by simplifying the system transmission of information. Evolution of technology can help us take an important step towards limiting the boundaries with the digital (virtual) world, and cryptocurrencies could be the first real experiment.

Blockchain technology offers us the following prospects for its implementation in the Net-Economy:

- The emergence of Bitcoin and other cryptocurrencies is a consequence

of the rapid development of the digital economy. Currently considered a technological experiment, the Bitcoin system has the potential to disrupt current financial operations and, in addition, long-term institutional structures. Bitcoin inflation can be controlled and known by any user.

- On the other hand, with the current (non) existing regulations, the system can be diverted to illicit trade, robbery and criminal activities. New international regulations are needed for virtual currency systems, due to their global nature and completely decentralized way of generating money.
- International transaction fees can be much lower than those of conventional bank transfer services. However, regulation in this context is very likely to increase the costs of Bitcoin payments. These costs could be passed on to customers by charging them higher.
- To become usable, a critical mass of consumers willing to pay with digital currency should be created. In order to achieve this, consumers could be encouraged to pay with digital currency by the considerable number of merchants that would eventually adopt this system

References

Bitcoin Price Index - Real-time Bitcoin Price Charts. (2018). Retrieved from https://www.coindesk.com/price/

BrightPlanet, 2014. *Clearing Up Confusion - Deep Web vs. Dark Web*, 2014, March 27. Retrieved April 11, 2018, from https://brightplanet.com/2014/03/27/clearing-confusion-deep-web-vs-dark-web/.

Cascarilla, C. G. (2015). Bitcoin, Blockchain, and the Future of Financial Transactions. In *CFA Institute Conference Proceedings Quarterly* Vol. 32, No. 3, pp. 18-24. CFA Institute.

Egilsson, J. H., & Valfells, S. (2017). *Blockchains and the future of financial services*. Retrieved from *Monerium* Website: http://monerium.com/content/monerium-reportweb- 2017-07.pdf.

European Banking Authority. (2019). *EBA at a glance*. Retrieved July 20, 2019, from https://eba.europa.eu/about-us/eba-at-a-glance.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system. Network Effect.* (2010, June 28). Retrieved February 24, 2018, from https://www.investopedia.com/terms/n/network-effect.asp.

Ometoruwa, T. (2018, May 16). S*olving the Blockchain Trilemma: Decentralization, Security & Scalability.* Retrieved May 17, 2018, from https://www.coinbureau.com/analysis/solving-blockchain-trilemma/.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239-278). Springer, Cham.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. New York: Penguin Random House

The Deep Web vs. The Dark Web. (2015, May 6). Retrieved May 7, 2018, from http://www.dictionary.com/e/dark-web/.