

RESEARCH ISSUES REGARDING THE BITCOIN AND ALTERNATIVE COINS DIGITAL CURRENCIES

Alexandru PÎRJAN ^{*1}

Dana-Mihaela PETROȘANU ²

Mihnea HUTH ³

Mihaela NEGOIȚĂ ⁴

ABSTRACT:

In this paper, we research and analyse the main characteristics, the evolution of the Bitcoin and of the Alternative Coins (Alt-Coins) digital currencies, their numerous applications and ramifications. We make an in depth analysis of the Bitcoin digital currency and of the most significant Alternative Coins, taking into account their technical characteristics, their main advantages and limitations. Just as it happened in the past decades with the personal computers and Internet, the impact of these digital currencies will gradually increase in the future, leading to major changes in our lifestyle, redefining our everyday life, economy and society.

Keywords: digital currency, Bitcoin, Alternative Coins, electronic payments.

1. Introduction

The digital currency (also known as digital money) represents an online mean of payment that differs significantly from the classic means of payments such as cash, cheque, credit, debit or bank transfer. The digital money preserves a series of properties from the physical currencies, having the advantages of allowing instant transactions and transfers to be made. Similar to the classic means of payment, the digital currencies can be used to pay for a wide range of goods and services.

From a historical point of view, the digital money have emerged consequently to the development of the cryptography. Obviously, when a sequence of bits becomes a digital representation of a monetary value that can be used for paying different goods or services, users might have their own doubts regarding the security of their money and of the associated transactions. Even the most secure cryptographic algorithms can be attacked [1]. For example, the users might be concerned to find out if the digital money is genuine or if they risk having their money stolen and used by others, one of the most widely known problems being the so-called "double-spending issue".

In the case of the classic printed money, problems related to their counterfeiting occur frequently, the methods and technologies used for their counterfeiting becoming

¹ *Corresponding author. PhD Lecturer. Faculty of Computer Science for Business Management, Romanian-American University, 1B, Expozitiei Blvd., district 1, code 012101, Bucharest, Romania, E-mail: alex@pirjan.com

² PhD Lecturer. Department of Mathematics-Informatics, University Politehnica of Bucharest, 313, Splaiul Independentei, district 6, code 060042, Bucharest, Romania, E-mail: danap@mathem.pub.ro

³ Romanian-American University, 1B, Expozitiei Blvd., district 1, code 012101, Bucharest, Romania, E-mail: huth.cf.mihneacristian4@student.rau.ro

⁴ Romanian-American University, 1B, Expozitiei Blvd., district 1, code 012101, Bucharest, Romania, E-mail: negoita.m.mihaela4@student.rau.ro

increasingly advanced. However, in this case, if conventional money is being used directly when conducting transactions, the risk of the "double-spending issue" is easily solved because the physical banknote cannot be in more places than one at a given moment of time. In certain cases, the conventional money is being stored and transmitted digitally, thus raising the two problems mentioned above: the risk of counterfeiting and of the "double-spending". In both of the cases, the problems are handled by the intervention of the central authorities that have access to general information regarding the users' accounts, their transactions and the cash flows.

In the case of digital money, the cryptography offers guarantees towards the legitimacy of a user. Specifically, the cryptographic digital signature allows a user to sign a digital asset or transaction, thus confirming the ownership of the asset. The "double-spending issue" can also be solved by means of digital signatures [2], [3].

In the late 1980s, as cryptography evolved and became more accessible, several researchers became interested in using the cryptography for developing digital currencies. They have succeeded to issue digital currencies that had coverage in national currencies or even in precious metals [2].

Even if the early versions of digital currencies were implemented, they posed the main disadvantage of being centralized and consequently became vulnerable. The first digital currencies used a system similar to the one used in traditional banking, where the settlement of all the transactions took place at regular intervals, through a centralized system. Unfortunately, in most of the cases, these initial digital coins were disavowed at first. Afterwards, the concerned governments challenged them and some of the digital currencies have failed when the parent company suddenly went bankrupt. In this context, it became obvious for the researchers that in order to obtain a digital currency that is robust against attacks, the currency must be decentralized, thus eliminating the existence of a vulnerable centralized system.

Nowadays, the most popular digital currency in the world is Bitcoin, an online payment system developed by Satoshi Nakamoto. He published the details of his invention in 2008 and afterwards, in 2009, he released it as an open-source software. In the case of Bitcoin, as for all the current digital currencies, no central organization, control point or person is involved in controlling the money supply at a global level. Thus, Bitcoin is a fully decentralized system that is not controlled by any central authority or control point that could be corrupted or attacked [3].

In the second section of the paper, we present the Bitcoin digital currency; in the following section, we first analyse the Alt-Coins currencies; afterwards, we present and analyze a series of Alt-Coin projects that brought technical or economic changes, highlighting the differences between these new projects and the original Bitcoin system. We analyze these systems in a chronological order, according to their launch date. In the final part of the third section, we present and compare a series of technical and economic characteristics of the Bitcoin and of some of the most important Alt-Coins currencies, while in the fourth section we highlight some advantages and disadvantages of the Bitcoins and Alt-Coins digital currencies.

2. The Bitcoin digital currency

Bitcoin is the result of several decades of research in the field of distributed systems and cryptography. This concept is based on a series of innovations that have led to a powerful

solution: a peer-to-peer decentralized network (represented by the Bitcoin protocol); a register of the public transactions (represented by the blockchain, a transaction database that is shared by all the nodes participating in a system based on the Bitcoin protocol); a decentralized, deterministic and mathematical system for issuing the currency (through the distributed mining); a decentralized system of transaction verification (the transaction script).

Bitcoin uses a peer-to-peer computer network, each computer being a node that runs a specialized software. Unlike the centralized systems' case, in which the control belongs to a small group of people or to an institution, in the case of a peer-to-peer network, the changes can occur only after most of the involved parties have agreed upon a decision. Sometimes, in certain situations, this condition is not sufficient, as a minority that does not agree to these changes is able to prevent them. If the majority still forces the implementation of the changes, this could lead up to malfunctions of the entire network [3].

Without a doubt, in the decentralized systems, the changes that have not been approved by the majority of the peers, being contrary to their own interests, are rejected. This is one of the most important advantages of these systems when being compared to the centralized ones. Another fundamental advantage of the centralized systems consists in their robustness against the inside and outside attacks. The Bitcoin system does not require the existence of a centralized trusted party in order to operate, being designed as to deter the malicious attacks that could originate from inside the network, if the attacks had not originated from a majority of peers.

Bitcoin is also able to manage the "double-spending issue", that occurs when a peer (or two different people) try to use the same funds twice. In a decentralized system, when multiple copies of the database are shared between the existing peers, maintaining a consistent database is a difficult problem. In the context of Bitcoin, the problem is how the network handles the messages between the nodes, taking into account the fact that the messages might be corrupted and could originate from the attackers who try to destabilize the database. Bitcoin is managing this problem successfully.

As Bitcoin is an open source software, it provides a series of specific advantages. Thus, any user has the right to use the software, to copy, modify and redistribute it. In the case of a proprietary software, the user is not usually allowed to know details regarding the source code. On the other hand, an open source software always gives access to its source code. The major advantage of an open source cryptographic software is that it allows users to verify that the code does not contain vulnerabilities and they can contribute to its future development.

There are two main types of open source licenses. The "Copyleft" type of open license imposes to the users the obligation that, after making software changes, the modified version should be launched under the same license (the share-alike Requirement). The GNU Public License (GPL) is an example of an open source "Copyleft" license. The second type of open source licenses, the "Permissive" ones, impose few restrictions regarding the redistribution of the software. In this case, a derived software preserves the original copyright notice. Some of the most common open source software belong to the "Permissive" family: the MIT license, the Apache license, the BSD license. The Bitcoin core was released under the terms of the MIT license, originating at the Massachusetts Institute of Technology.

In the case of a proprietary software, the owner is the only one that manages the software's maintenance and updating. However, for an open source software, any developer can assume these tasks. In the case of an open source license, the developers are allowed to develop and launch a new software project independently, starting from an original project, through a process named "forking". Any developer can create a fork, thus contributing to the development of the original software. The "forking" enables customers to choose which branch to follow. For most of the open source projects, the "forking" process takes place seldom. Bitcoin is a particular case since it has been modified and forked several times by the developers who wanted to put the new variants to the test. Thus, new alternative cryptocurrencies, referred to as Alternative Coins (Alt-Coins), have emerged. We will analyze these further, in the following section.

In some cases, the developers are much more interested in improving and extending an open source software than a company that owns a proprietary software is, after having reached its desired market share. On the other hand, a problem faced by many open source projects consists in the fact that, although there are many users interested in using that software, there are only a few developers interested in contributing to its development. Many open source projects have difficulties in obtaining financing or in their development. The Bitcoin software is also facing these problems [4].

Bitcoin uses a distributed database that stores and keeps track of the common assets in a copy of the ledger. The database is distributed, so each node of the network (each participant) keeps a copy of this ledger. By design, the copies from different nodes are consistent. Each user has control of its own funds using a private cryptographic key. When he wants to spend some funds, he must use its private key in order to sign a message specifying how those funds will be used and in what amount. This message is sent through the network. After having received a copy of the message, each participant in the network verifies the validity of the message and afterwards updates its database copy accordingly.

The public does not generally know the procedures and protocols designed to protect the traditional financial databases. Instead, Bitcoin reveals to the public the database and creates a protocol based on an open source software in order to secure it. This protocol is designed to be robust against attacks originating from within the network. Even if Bitcoin makes public all the financial information that flows throughout its network, the identities of the users that are behind the transactions remain hidden. The system does not use personal information in order to identify the holders of the funds, but instead uses their addresses in the form of very long strings of letters and numbers. Bitcoin makes the bank statements of all its users public, but keeps their identities hidden.

In principle, it is not possible to correlate the Bitcoin addresses of the users with their identities. However, various techniques can be used to analyze the information within the network and obtain some details about the correlations between the Bitcoin addresses and the users behind them. The Bitcoin is not an anonymous system. Analyzing the traditional payment systems, one can notice that an employer is not able to find out how an employee spends its funds, although the employee's bank holds such information. If an employee is paid in Bitcoins, the employer has access to information on how the employee is spending his funds using the Bitcoin network. However, the employee has different ways to hide a series of information regarding its transactions. In many cases, the fact that the Bitcoin transactions are not anonymous but rather transparent is a positive factor. Thus, the

transparent use of the funds helps improving the quality of services, avoiding corruption, offering the possibility to verify the financial statements using the system of the public ledger.

As other similar protocols, Bitcoin allows the safe transfer of values, whether these are money or digital assets. The digital transfer of value is based on using the "smart contracts" that do not require the human presence, intervention or interpretation in order to be settled. For these contracts, the settlement is achieved entirely by running a software application.

An example of such an application consists in the autonomous agents, software developed for performing specific tasks. In [3] is presented an example of this kind of software that is running in a cloud, providing users file-sharing services in a storage space, rented for this purpose. Using the Bitcoin system, the software is able to handle its own funds and to sign intelligent contracts with the cloud services providers. Similarly, a storage agent can set up smart contracts with its end users, pay the cloud provider using the Bitcoin system and receive payments from his users via the same method. Thus, a decentralized system of payments represents an ideal starting point for new businesses and technologies, because it offers development opportunities without having to obtain any permits or authorizations.

The Bitcoin software is an Application Programming Interface (API) for digital currencies, while the Bitcoin currency (BTC) is an application of this software. Bitcoin is an open platform used for the exchange of values, a protocol based on which one can develop various applications. Regardless of the Bitcoin digital currency's future development, the Bitcoin platform will remain in the future extremely useful for developing new applications and implementations, representing a starting point for innovations in finance.

The Bitcoin platform creates opportunities for reducing the associated costs of settling and maintaining the contracts, by means of intelligent contracts. Being more efficient and reliable, these contracts have the potential to influence the economic situation at local and regional level, the evolution of corporate and governmental decisions.

In the following section, we depict and analyse some of the most important Alternative Coins cryptocurrencies developed through the "forking" process, deriving from the Bitcoin system or its forks.

3. The Alternative Coins

The Bitcoin open source project's code can be considered today as the starting point for a wide range of digital currencies. The most common software source codes resulting from the Bitcoin project are represented by the decentralized alternative currencies, also named Alternative Coins that use the same basic functional blocks as Bitcoin in order to implement digital currencies.

Many Alternative Coins are not significantly different from the Bitcoin digital currency, representing only attempts, some of them being less useful or important. However, there are also notable versions whose contributions to the digital currencies field are significant, because they implement different approaches or bring significant innovations to the original Bitcoin model. These alternative currencies differ from Bitcoin and bring innovations in three main directions, namely: they offer a new monetary policy, an

innovative consensus mechanism or specific improved features (e.g. improved anonymity).

From a historical perspective, the first derivative of the Bitcoin currency through the "forking" process is IXCoin, launched in August 2011. This currency has changed a series of the Bitcoin's parameters, for example, it accelerated the creation of the digital coins. The Tenebrix digital currency was launched in September 2011, shortly after IXCoin. It was the first cryptocurrency that has implemented a proof-of-work (POW) alternative algorithm, called "scrypt". A proof-of-work algorithm is meant to prevent the occurrence of the denial of service attacks and other service abuses. The Tenebrix developers intended to obtain a digital coin impervious to the attacks made using Graphics Processing Units (GPUs) and Application-Specific Integrated Circuits (ASICs), by using an intensive memory algorithm. Although Tenebrix has not been a successful digital currency, it represented the starting point for Litecoin, which has been a great success and has led to the development of hundreds of Alternative Coins, based on its code. The Litecoin system, launched in October 2011, has also used the "scrypt" as a proof-of-work algorithm and implemented additional improved methods for generating blocks, thus achieving a lower generation time of up to 4x from that of the Bitcoin. In some transactions, many users prefer this coin to the Bitcoin due to its advantages [5], [6].

The Alt-Coins development continued during the period 2011-2012, when several other projects based on Bitcoin or Litecoin were launched. At the beginning of the year 2013, there were 20 Alternative Coins currencies, while at the end of the same year more than 200 currencies were launched. In the year 2014, the attempts to develop and implement new digital Alternative Coins currencies have continued, reaching 500 types of Alt-Coins at the end of the year 2014. Currently there are more than 660 software Projects available (among which 7 were launched in March 2015) [5]. Today, more than half of the current Alternative Coins are derived from the Litecoin project through a "forking" process.

The development of Bitcoin and of its alternative currencies has focused on error correction control. In many cases, the Alternative Coins derived from Bitcoin through the "forking" process are not subjected to the Bitcoin's constraints and to the backward compatibility requirements, thus allowing them to implement new features. In the following, we present and analyze a series of Alt-Coin projects that have brought significant technical or economic changes, highlighting the differences between these new projects and the original Bitcoin system. We depict the systems in a chronological order, according to their launch date: Freicoin (FRC), Namecoin (NMC), Litecoin (LTC), Peercoin (PPC), Primecoin (XPM), Dogecoin (DOGE) and Auroracoin (AUR). Other examples of Alt-Coins include: Anoncoin, Aphroditecoin, CryptoNote, CureCoin, DarkCoin, Devcoin, Qixcoin, Safecoin, SolarCoin, SpainCoin, Splash, TAGCoin.

3. 1. The Freicoin digital currency

The Freicoin (FRC) digital currency, launched in February 2011, is characterized by the fact that it uses the demurrage, a tax on the transactions, through which the system retains a certain fraction of Freicoins. This fraction increases with the time elapsed since the moment when the currency has been traded for the last time. Thus, Freicoin apply to its users an annual percentage rate of charge of about 5%, according to certain operations in

its network. Freicoin has a negative interest rate for the stored value. Through the demurrage, the consumption is encouraged while the hoarding of money is discouraged.

Freicoin implements a monetary policy opposed to that of the Bitcoin system. The Bitcoin's policy is a deflationary one, while that of Freicoin can be considered similar to the expansionary monetary policies that increase the money supply and thus lead to inflation. However, in the Freicoin case, the demurrage's effect is constant and thus can be handled without risks. Although the Freicoin currency cannot be considered a success, it is an interesting example of Alt-Coins, being innovative in terms of the implemented monetary policy.

3. 2. The Namecoin digital currency

The Namecoin (NMC) was launched in April 2011, being both a digital currency and a decentralized key/value repository that has the role of implementing an alternative DNS (Domain Name System). The DNS associates various information with domain names assigned to each of the participating entities, in this case the DNS transforms the users' addresses into IP addresses. Namecoin uses the ".bit" domain implemented through an alternative Domain Name System. The Namecoin system also provides support for stock certificates, email addresses, SSL certificates, encryption keys, file signatures and many other applications. It includes also the Namecoin currency that is used for paying the transaction fees.

Although Namecoin enables users to use any namespace, there are certain namespaces that have predefined meanings. When they are read from the blockchain, the software application receives some information that determines its further actions. Any user from a Namecoin node owns a copy of the key/value pairs that can be accessed any time.

A domain registration of the type Namecoin ".bit" is linked to a Namecoin address, instead to a name or to a physical address. The private key of a Namecoin address has control over the domain. Therefore, changes can be made to a domain with a high degree of anonymity. The Namecoin's developers state that the use of alternative DNS is safer, faster and cheaper than that of the traditional DNS [2], [3].

3. 3. The Litecoin digital currency

The Litecoin (LTC) digital currency, one of the first Alt-Coin systems, was launched in October 2011, and is considered the most successful of all the currencies developed through the "forking" process, derived from the Bitcoin system.

As in the Tenebrix system's case, from which it derived, Litecoin uses a proof-of-work (POW) alternately algorithm, called "script", a function that requires an amount of RAM (Random Access Memory) in order to be computed. Another innovation brought by the Litecoin system lies in the fact that it has implemented a faster block-generation method that reduces the computational time and speeds up the transactions' inclusion in a block.

The "script" generates pseudorandom numbers that are stored in the Random Access Memory, in order to be further accessed. The Litecoin's algorithm accesses this memory several times in order to return the result. The Litecoin's "script" implementation requires only 128 kB of memory, an amount that should not raise resource problems for the

computers of the system's nodes. Using a memory-hard function as a proof-of-work has certain advantages. First, the number of miners increases as anyone who owns a computer can perform this task. In the case of Bitcoin, mining requires a specialized equipment and this fact reduces the number of miners. Another advantage of the "scrypt" system is that in some of the cases it can lower the resource waste compared to the traditional proof-of-work systems [3].

The Litecoin enthusiasts consider that one of the most important advantages of this system is the fact that it implements the "scrypt" that can sustain more attacks made through Graphics Processing Units (GPUs) and Application-Specific Integrated Circuits (ASICs) than the SHA-256 algorithm implemented in the Bitcoin system [2].

3. 4. The Peercoin digital currency

Peercoin (PPC) was introduced in August 2012 and represents an innovation in the field of digital currencies because it is the first Alt-Coin that uses a hybrid algorithm, combining the proof-of-work and proof-of-stake methods in order to issue new currency. In a proof-of-stake system, the new blocks are being generated by the digital currency holders in proportion to the number of the coins that they hold. The proof-of-stake blocks' generation requires a reduced consumption of electricity [2].

As we have mentioned before, within the Peercoin system there are two types of blocks: generated by proof-of-work and by proof-of-stake. The Peercoin blocks generated in the proof-of-work system follow similar rules to those generated in the Bitcoin system. For the Peercoin blocks generated in the proof-of-system, the transactions are assigned by taking into account the age of the coin. This is computed as the product between the number of coins involved in the transaction and the time that has elapsed since the moment when the funds were used for the last time. The age of the coin is used by the proof-of-work system to determine the blockchain's security: if a forking process takes place, the correct branch is considered to be the one that is the oldest. When generating coins in the Peercoin system, first, the proof-of-work system is used, and afterwards, the proof-of-stake system becomes the primary source of the digital currency [3].

3. 5. The Primecoin digital currency

The Primecoin (XPM) was launched in 2013. It is based on a proof-of-work algorithm that searches for chains of prime numbers (Cunningham and bi-twin chains). The Primecoin blockchain contains these prime numbers, providing both a public ledger of the transactions and a public ledger of the obtained useful scientific results.

Most proof-of-work functions provide results useful only for securing the blockchain. In contrast with those cases, in the Primecoin's case, the results obtained through the proof-of-work function have also a scientific value. The chains of prime numbers found by the proof-of-work algorithm help researchers in understanding the distribution of prime numbers, which are extremely important in various scientific domains. The proof-of-work functions must mandatory be efficiently verifiable and the verification should be possible through means of fast computations. In addition, these functions' difficulty should be easily adjustable, as miners enter or leave the network.

The Primecoin's proof-of-work function satisfies both of the above mentioned requirements. The verification of the prime numbers or of the chains of prime numbers is sufficiently efficient. By adjusting the length of chains of prime numbers, one can change the difficulty of the mining process. The length of a chain of prime numbers is a discrete value and therefore the difficulty will increase exponentially. This problem has been solved by the Primecoin developers using a fractional chain length [3].

3. 6. The Dogecoin digital currency

The Dogecoin (DOGE) digital currency was released in December 2013 and is based on a fork of Litecoin. Dogecoin is remarkable due to its monetary strategy: the monetary policy of rapid issuance that encourages the rapid spending. Although the Dogecoin system started solely for entertainment purposes, it quickly became quite popular, attracting a large, enthusiast and active community. The Dogecoin currency is inflationary, but its inflation rate decreases over time. Unfortunately, in 2014 Dogecoin experienced a rapid decline [2].

3. 7. The Auroracoin digital currency

Auroracoin (AUR) was launched in February 2014 and is derived from the Litecoin project through the "forking" process. Auroracoin uses, just like Litecoin, the "scrypt", a proof-of-work (POW) alternately algorithm. The innovation introduced by this system consists in the currency's distribution. Thus, 50% of the monetary supply has already been created at Auroracoin's inception, while the remaining 50% comes from the regular miners. The initially created amount of digital currency is distributed to the population of Iceland. This distribution began in March 25, 2013 and each citizen has received the same amount of this digital currency [2]. This process has facilitated the building of a community around this coin that has led to its strengthening.

3. 8. Technical and economic data regarding Bitcoin and some of the most important Alt-Coins currencies

In the following, we present and compare a series of technical and economic characteristics of the Bitcoin and some of the most important Alt-Coins currencies. The data was retrieved from [5], [6], [7] in March 2015. The main results are synthesized in **Table 1**.

Table 1. Technical and economic data regarding Bitcoin and some of the most important Alt-Coins currencies

No.	Digital Currency	Date Founded	Market Capitalization (USD)*	Algorithm	Total Coins	Block Time	Block Reward
1	Bitcoin (BTC)	January 2009	3,526,550,721	SHA-256	21 Million	10 Minutes	25 Coins
2	Freicoin (FRC)	February 2011	70,072	SHA-256	100 Million	10 Minutes	645.43 Coins

* On March 28, 2015

3	Namecoin (NMC)	April 2011	4,727,814	SHA-256	21 Million	10 Minutes	25 Coins
4	Litecoin (LTC)	October 2011	64,206,724	"SCRYPT"	82 Million	2.5 Minutes	50 Coins
5	Peercoin (PPC)	August 2012	7,489,023	SHA-256	No Limit	10 Minutes	82.56 Coins
6	Primecoin (XPM)	July 2013	239,271	"SCRYPT"	**	1 Minute	***
7	Dogecoin (DOGE)	December 2013	111,327	"SCRYPT"	100 Billion	1 Minute	10,000.00 Coins
8	Auroracoin (AUR)	February 2014	54,257	"SCRYPT"	21 Million	5 Minutes	12.50 Coins

The exchange rate for the Bitcoin at 29 March 2015 is 1 BTC = 987.09 Lei = 244.52 USD = 225.24 EUR. During the time, the Bitcoin's exchange rate has varied in a spectacular way, ranging from practically a zero value in 2009 to a price of 200-300 USD in March 2015 (**Table 2**).

Table 2. The Bitcoin's exchange rate evolution during time

Date	Price for 1 BTC (USD)
January 2009 – January 2010	basically none
February 2010 – May 2010	< 0.01
June 2010	0.08
February 2011 – April 2011	1
8 July 2011	31
December 2011	2
December 2012	13
April 11, 2013	266
May 2013	130
June 2013	100
November 2013	350 –1250
December 2013	600 –1000
January 2014	750 –1000
February 2014	550 –750
March - May 2014	340 –700
March 2015	200 –300

** Unlike Bitcoin, one cannot deduce the total number of coins in circulation from the current block's height; the history of the difficulty data is required.

*** Self-adjusting block reward: the number of Primecoins released per block is not fixed but is always equal to 999 divided by the square of the difficulty.

By analyzing the market capitalization of Bitcoin and of the most important Alt-Coins (based on data retrieved on 29 March 2015) one can observe that more than 89% of this capitalization comes from Bitcoin, more than 8% comes from other currencies (some of these cryptocurrencies are not even derived from Bitcoin), more than 1 % comes from Litecoin and all the other Alt-Coins have a total of less than 0.5 % from the total market capitalization [8]. The results are synthetized in **Table 3** and **Figure 1**.

Table 3. The market capitalization of Bitcoin and of the most important Alt-Coins

No.	The Digital Currency	The Market Capitalization
1	Bitcoin (BTC)	89.92575%
2	Others	8.11336%
3	Litecoin (LTC)	1.63725%
4	Peercoin (PPC)	0.19097%
5	Namecoin (NMC)	0.12056%
6	Primecoin (XPM)	0.00610%
7	Dogecoin (DOGE)	0.00284%
8	Freicoins (FRC)	0.00179%
9	Auroracoin (AUR)	0.00138%

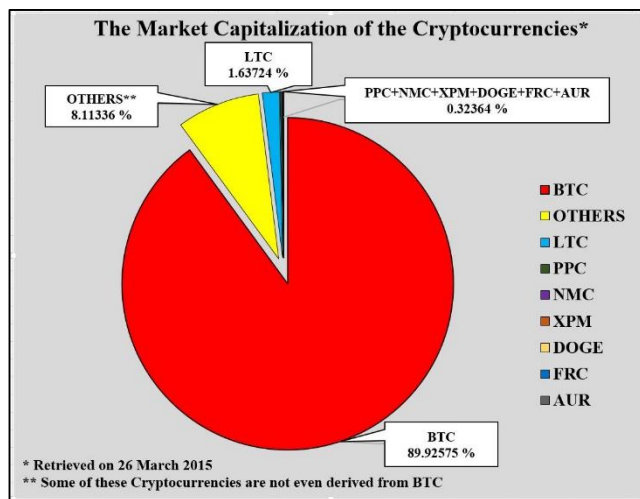


Figure 1. The market capitalization of Bitcoin and of the most important Alt-Coins

4. Advantages and disadvantages of the Alt-Coins

As the costs of launching Alternative Coins are very low, the number of the released Alt-Coins is very high. The Alt-Coins critics say that only those Alternative Coins that bring significant improvements to Bitcoin will survive. On the other hand, the Bitcoin's sustainers say that Bitcoin presents both direct network effects (as the number of people

that use Bitcoin to store values increases, Bitcoin becomes more valuable) and indirect network effects (as the number of people that want to spend Bitcoin increases, the interest of traders to support this system becomes greater).

If a network has $n \in \mathbb{N}$ users, then each user can establish a total of $(n - 1)$ connections with the other users and the total number of connections across the network is $\frac{n(n-1)}{2} \in \mathbb{N}$, which is proportional to n^2 asymptotically (that is, an element of $O(n^2)$). In **Figure 2** are represented some examples of a network effect: two users can establish only one connection; five can establish ten connections, while twelve users can establish 66 connections.

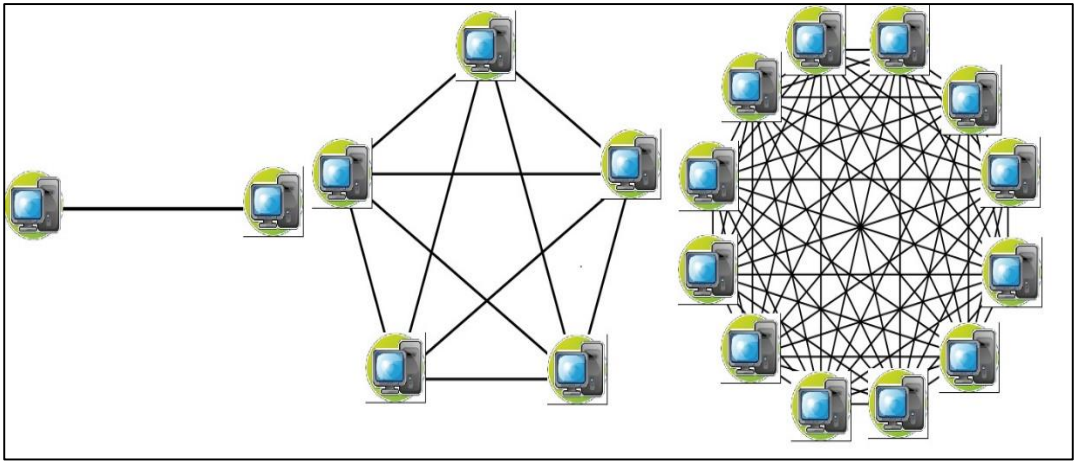


Figure 2. Examples of the network effect

The Metcalfe's law states that "The value of a network is proportional to the square of the number of the system's connected users." Thus, one can obtain a way to quantify the network externalities [2], [3]. One can easily prove that the total number of connections across the network is larger than the number of users, because:

$$\frac{n(n-1)}{2} > n \Leftrightarrow n(n-1) > 2n \Leftrightarrow n^2 - n > 2n \Leftrightarrow n^2 > 3n$$

The last inequality is true for all the values of $n > 3$, which is a reasonable assumption, taking into account the fact that all the involved networks have more than 3 users.

The liquidity of an asset represents the degree to which the asset can be sold quickly without affecting its price, being a way to measure the economic consequences of its network effect. Obviously, in the case of a digital currency, its liquidity depends on the size of its network. The Alt-Coins critics argue that the Alt-Coins users will elect the cryptocurrency with the highest degree of liquidity, making it even more fluid, leading eventually to the collapse of that coin. On the other hand, the Alt-Coin's sustainers claim that the network effect does not happen necessarily on a global scale and even if this effect took place, it would create a market place for Bitcoin's complementary technologies [3].

Many other criticisms have been made against Bitcoin and Alt-Coin [3]. Among them, a few seem to appear most frequently: as the majority of these digital coins use the same standards, the competition between standards is excluded; the costs of transitioning from

the Bitcoin to an Alt-Coin may become significant. The defenders of the Bitcoin and Alt-Coin currencies argue that the transition from one type of currency to another can be made quite easily through a software update. On the other hand, they say that a user can implement and use multiple cryptocurrencies. Another reason for criticism refers to the coordination issues. Critics argue that even if most of the users liked to replace Bitcoin with another currency, the transition would prove to be difficult due to coordination problems [2], [3].

The Bitcoin's and Alt-Coin's sustainers also bring other arguments forward in favor of these currencies. They consider that: the competition between these currencies leads to progress and innovation; the usage of multiple Blockchains reduces the network's load; Bitcoin and Alt-Coins can facilitate the exercise of some public functions, can help achieve scientific purposes (such as Primecoin), can be used to fund public goods (such as Devcoin, CureCoin, Safecoin) or can be used to fund different projects.

5. Conclusions

Coexisting for many years, Bitcoin and Alternative Coins were competing in some aspects, but most of the Alt-Coins currencies do not represent a direct competitor of the Bitcoin. From the contrary, Bitcoin and Alt-Coins cooperate in a mutually beneficial relationship. Bitcoin has benefited from being able to make the first move regarding the network effect and the liquidity. In addition, Bitcoin has managed to cover significantly the users' demand for digital market currencies.

No one can say with certainty what will happen in the future with these advantages, if Bitcoin will be able to maintain its leadership position or if it will be exceeded in terms of popularity, of the technical or economic features by an already existing Alt-Coin or by one that will be developed in the future. One thing is for sure: the worldwide acceptance of the digital currencies could change the global economy as we know it. Analysing the evolution and characteristics of the Bitcoin and Alt Coins, one can conclude that their worldwide acceptance is no longer an impossible outcome, being a plausible scenario in the future.

Just as it happened in the past decades with the personal computers and Internet, the impact of these digital currencies will gradually increase in the future, leading to major changes in our lifestyle, redefining our everyday life, economy and society.

6. Acknowledgement

The article has been supported by scientific research within the project entitled "PRACTICAL SCHOOL: Innovation in Higher Education and Success on the Labour Market", project identified as POSDRU/156/1.2/G/132920. The project is co-financed by the European Social Fund through the Sectorial Operational Programme for Human Resources Development 2007-2013. Investing in people!

REFERENCES

- [1] Tăbușcă A., Established Ways to Attack Even the Best Encryption Algorithm, Journal of Information Systems & Operations Management, Vol.5, No.2.1/2011, Ed. Universitară, 2011, ISSN 1843-4711.
- [2] Antonopoulos A. M., Mastering Bitcoin: Unlocking Digital Crypto-Currencies, O'Reilly Media, Inc., 2014, ISBN 978-1-449-37404-4.
- [3] Franco P., Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley, 2015, ISBN 978-1-119-01916-9.
- [4] Bradbury D., Bitcoin Core Development Falling Behind, Warns Bitcoinj's Mike Hearn, www.coindesk.com/bitcoin-core-development-falling-behind-warns-mike-hearn/, 2014.
- [5] <http://mapofcoins.com/bitcoin> accessed at 28 March 2015.
- [6] <http://altcoindb.com/coins> accessed at 28 March 2015.
- [7] <http://coinmarketcap.com> accessed at 28 March 2015.
- <http://ro.coinmill.com> accessed at 28 March 2015.