Risk assessment of investing in cryptocurrency markets.

The third part

All parts of the article in PDF and TXT formats:
https://github.com/alcib/cryptocurrency/tree/master/articles
The price and quantity indexes from the site Coinmarketcap.com were used to this article by Dec 2017 12:00 PM UTC.

PoW method

So we see: all scam schemes in the cryptocurrencies market are in using the unfair methods of coin's creation. The only fair method of coins creation is PoW (Proof-of-work). This method (PoW) was proposed by Satoshi Nakamoto in his article "Bitcoin: A Peer-to-Peer Electronic Cash System" (Oct 31, 2008). PoW method is used for Bitcoin's creation and for some other cryptocurrencies. The main idea of PoW method is that the quantity of created coins per day was defined in advance. This rule is fixed at the cryptocurrency's algorithm. The coins are evenly distributed among the members of the cryptocurrency network in proportion to their computing powers, which were used for the work of the network. As cryptocurrency networks are working without Data Centers, so newly created cryptocoins are used for payments of the computing powers of the network members. Receiving money in exchange for the computing powers, which were used for the work of the cryptocurrency network, is called mining.

Now we will analyse the cryptocurrencies with capitalization above $0.5 billion, in which PoW coins creation scheme is used.

Bitcoin (BTC) is the oldest cryptocurrency (the Bitcoin network functions since Jan 9, 2009). It has the highest market capitalization.
https://bitcointalk.org/index.php?board=1.0
https://github.com/bitcoin/bitcoin
Capitalization: $334.7 billion
All BTC coins were created by PoW method. Bitcoin mining is done through the using special device ASIC. ASIC is a more effective device for mining than the usual computer. The creation of ASICs has divided members of the cryptocurrency network into two basic groups:
1) Members of the cryptocurrency network, who make financial transactions;
2) Members of the cryptocurrency network, who make mining.
As Bitcoin value is high, so number of participants of mining is much higher than the number of newly created coins per day. To have a higher chance of coins receiving, participants of mining are integrated in **mining pools.** So now the members, who make financial transactions, don't control the Bitcoin network. The mining pools owners control it.
On the one hand, this is contrary to the idea of Satoshi Nakamoto. Cryptocurrency network should work without any centralized nodes and servers, which can impose their conditions on others. But on the other hand, mining pools are interested in successful working of the cryptocurrency network. If mining pool will break the work of its cryptocurrency network, value of the cryptocurrency will fall down and the members of this mining pool will have the loss. As a result, the value of alternative cryptocurrencies will increase.
In view of the above, the largest mining pools decide on further development of the Bitcoin network by a vote. As mining pools owners were interested in successful working of the Bitcoin network, their decisions on the software upgrade were very conservative. Due to this,

more than 7 years the Bitcoin network functions without critical failures. But rapidly increasing quantity of network members led to Bitcoin network software failures, because of the software wasn't for such great quantity of transactions entry. And as a result the increasing of fees and transaction queues in the Bitcoin network. Also reluctance of mining pools owners to change Bitcoin software has led to Bitcoin hardforks in 2017.

Hardfork is a new cryptocurrency, but coins creation is not being from the ground up. All coins of the old cryptocurrency are copied into a new cryptocurrency (hardfork). So not only software but also Blockchain is copied into a hardfork. Coins distribution among network members of the hardfork remains the same as for old cryptocurrency. If an investor had one wallet before the hardfork started, so after its start the investor will have two similar wallets. The quantity of coins, which the investor had before hardfork's start will double. But values of new and old cryptocurrencies may be different. And the investor can exchange coins of one cryptocurrency into another. So the hardforks of Bitcoin network have not affected interests of the investors.

Total capitalization of Bitcoin forks, which were started in 2017, is $371.2 billion. 90% of total amount is Bitcoin (BTC), 8.5% is Bitcoin Cash (BCH) and 1.5% is Bitcoin Gold (BTG).

Nowadays it is impossible to crack the cryptocurrency wallet. So if you forget password for your wallet, you'll lose all coins from the wallet forever. According to the available data, from 15% to 30% of total quantity of BTC coins was lost by now. Total capitalization of Bitcoin and its forks of 2017, less the amount of lost coins, is about $296.9 billion.

Litecoin (LTC) is the cryptocurrency, in which PoW coins creation scheme is used. It has the highest market capitalization after Bitcoin.
https://bitcointalk.org/index.php?topic=47417.0
https://github.com/litecoin-project/litecoin
Capitalization: $17.527 billion
All LTC coins were created by PoW method. Litecoin mining is done through the using special device ASIC. Litecoin started as Bitcoin's fork in Oct 8, 2011. There is not much difference between Litecoin and Bitcoin. Litecoin has other mining algorithm, blocks creation speed and some other differences. Litecoin software and Bitcoin software are still compatible.

Monero (XMR) - is in third place according to market capitalization.
https://bitcointalk.org/index.php?topic=583449.0
https://github.com/monero-project/monero
Capitalization: $5.439 billion
All XMR coins were created by PoW method. Monero mining is done through the using video cards and central processing units of usual computers. Also mining on websites is possible. In this case mining is done through the using computing powers of browsers. Mining algorithm of Monero is resistant to devices ASIC.
Monero started in Apr 18, 2014. Monero transactions protocol is **CryptoNote**. There are a lot of differences between Monero transactions protocol and Bitcoin protocol. The protocol CryptoNote is used for cryptocurrency networks since July 4, 2012.
Nowadays Monero is the most anonymous cryptocurrency. The technology RingCT was installed by the Monero developers in 2016. The technology RingCT lets hide transactions amounts from the persons that are not members of the transaction. The technologies Multisig, Kovri and Bulletproofs are currently being prepared for installing. The technology **Multisig** provides multiple signatures of a transaction. The technology **Kovri** let hide IPs of the

cryptocurrency network. The technology **Bulletproofs** let decrease the size of a transaction. As a result, the Blockchain size will increase not so quickly. Nowadays Monero is the most technologically advanced cryptocurrency. But frequent releases in the Monero software deter investors. Frequent changes of cryptocurrency software can lead to a hardfork creation. Also they often lead to failures that were missed during network testing (testnet).
The project manager Riccardo Spagni voiced Monero as experimental project. It also deters investors.

MonaCoin (MONA)
https://bitcointalk.org/index.php?topic=392436.0
https://github.com/monacoinproject/monacoin
Capitalization: $0.776 billion
All MONA coins were created by PoW method. MonaCoin mining is done through the using special device ASIC. MonaCoin started as Litecoin's fork in Jan 01, 2014. There is not much difference between MonaCoin and Litecoin. MonaCoin has other mining algorithm, blocks creation speed and some other differences. The coin is popular in Japan.

Dogecoin (DOGE)
https://bitcointalk.org/index.php?topic=361813.0
https://github.com/dogecoin/dogecoin
Capitalization: $0.768 billion
All DOGE coins were created by PoW method. Dogecoin mining is done through the using special device ASIC. Dogecoin started as Litecoin's fork in Dec 8, 2013.

In this article we have analysed 470 cryptocurrencies, including ICO tokens with small capitalization. The total capitalization of the remaining 890 cryptocurrencies is $11.3 billion according to Coinmarketcap.com. Perhaps it is possible to find some diamonds among these 890 cryptocurrencies. For this purpose use the methods described in the first part of this article. But financial analysis cannot be used to these cryptocurrencies, as their total capitalization less than daily market volatility.

The opinions

1. Today the only fair method of coins creation is PoW (Proof-of-work).
2. The scam methods of coins creation are ICO, PoS, premining etc. Real (fair) market capitalization of cryptocurrencies, which use scam methods of coins creation can't be calculated. Because in this case the cryptocurrencies value can be easily manipulated. Investments in these cryptocurrencies may be just short time speculations in the cryptocurrencies markets or voluntary donations for scientific research in the field of cryptocurrencies` technologies.
3. Financial analysis cannot be used to cryptocurrencies with capitalization less $0.5 billion. Because the total capitalization of such cryptocurrencies is less than daily market volatility. So you should deal with information from bitcointalk.org and github.com to analyse these cryptocurrencies.
4. The total capitalization of Bitcoin and its` forks, which were started in 2017, less the amount of lost coins, is $296.9 billion.
5. The total capitalization of remaining cryptocurrencies with capitalization above $0.5 billion, in which PoW coins creation scheme is used, is $24.5 billion.
6. So real (provable) cryptocurrencies market capitalization is $321.4 billion by Dec 17, 2017. And 92.4% of total amount is Bitcoin and its` forks, which were started in 2017.

On the one hand, rapidly increasing of cryptocurrencies market needs further intense development of the software. But on the other hand, the financial systems with high capitalization need a conservative approach on the software changes. In my next article I will describe the methods of cryptocurrencies software upgrade that reduce financials risks. Also the weaknesses of the cryptocurrencies technologies will be analysed.

If this article was useful for you, or you are interested in a continuation of my research in that field, please, just do donations:
BTC: 14SZxryp7FVevqVRwHfNFdtt8CbyUwKFAw

XMR:
46v4d1QvQhE9zEt2dMDV5qFqdrZgX5YjqGrPAdta59Z86WnNwKyb4GgL1UfGRuvdTKSyqgJUMdP4mBzgqLjvHjnNScMmT2Q

Alcibiades2018 https://github.com/alcib