D.Beirak, student
A.Morozov, Ph.D, Ass.Prof., research advisor
S.Kobzar, language advisor
Zhytomyr State Technological University

CRYPTOCURRENCIES. THE FUTURE

The popularity of the first most successful cryptocurrency — Bitcoin, has caught a lot of attention and made people consider this concept something bigger than just a bunch of calculated hash-codes. In this issue, let us focus on the main parameters that are most likely to effect cryptocurrencies' future. Also, it's assumed that basic information on this topic is already known.

First thing we have to cognize here is that cryptocurrencies are open-sourced. That means, not only could they be influenced by the tacit or explicit power of authorities, but of course by society's and community's culture. That gives us pretty unpredictable system which is very sensitive to all the trifles around. In this article we're not going to cover that side of the subject and will focus only on the technical queries and issues of their nature.

The very cryptocurrencies' fundamental is the hash-algorithm type and today we have foremost in usage *SHA-256* and *scrypt*. As we all know, Bitcoin uses the first one and many of its forks, like Litecoin for instance, use the second. Bitcoin was the first successful attempt of implementation, and not to mention, it is not outshined till this day. But we have to admit that it also has one grave issue associated with hash standard which is supposed to be a risk of anti-decentralization what is a total opposite to initial concept. Having *SHA-256* gives benefit to rich users who utilize ASICs to mine coins. Sure, at the very beginning, Bitcoin was opened equally to everybody, although to be carried out outside of the "early community" boundaries it should have had some means for that. It is common knowledge, that Bitcoin solved this quandary owing to exchanges and real life usage, but what should we expect here with the younger Coins which are the major issue for cryptocurrency world themselves?

Alternate ways are a good thing, although the alternative has to be reasonable. We have one as Litecoin which introduces the usage of *scrypt*, but what about those forks of forks which are regularly used only for trading speculations and making easy fiat money without any support of crypto-idea? Today there are more than 200 Coin specimen only listed on *coinmarketcap.com*. But not every single of this list is so important and unique to even dare to distract your attention. No, the situation we have on the market is totally out of control. Basically, all those mint forks are the perfect things to mine as much as possible, wait until the price enlarges and then sell as quickly as you can. So what's the result of all that trouble? Fiat money. Thus what we learn from here is that supporting only reasonable forks makes sense. And here we are ready to discuss what a reasonable fork is.

We call a fork reasonable if it not only gives something new to what has been done previously, but also follows and develops the main ideas of cryptocurrencies which are decentralization, security and transparency. Actually, that is not all — there are more concerns to deal with, but those three are seen to be essential. That's why I gave the Litecoin good words. Due to *scrypt* algorithm it was able to become more user-friendly than Bitcoin, making producing of ASICs hardly possible. Sure, Litecoin has its own problems including security, but here we are talking about it as an example of something new and sound. That way, let us plow through the rest of parameters and see which are good to go along with future Coins.

First thing is, as discussed, a hash function. *Scrypt*-based seem to be preferred because of social components: they are more suitable for common hardware and less tend to centralize the computing power, which is fairer to users. And speaking about what is fair, there should also be no premine whatsoever, unless it is a currency, designed for special purposes.

Next, it has to be invulnerable for attacks. It is a good idea to start with block-chain backups and mining algorithms improvements to make it harder to manipulate or dominate the network. Another necessity is a reasonable finite volume of coins. It appears that infinite amount doesn't work, as well as having them too few or too many. The total volume has to be calculated in terms of time, enough for people to catch up in perspective, or basically, the ability to widen the audience in future. But that should be done in the way to not distract people because of the lack of advance.

Also, talking about convenience, there has to be expedient time for block creation to make transactions faster, but also rational in terms of security.

Proof-of-stake technology is quite controversial. It is seemed to be handy when coins are scarcely minable so even if implemented, it has to be abolished until the latest phases.

It is taken for granted that the new Coin has to develop a solid community and support and also we are not talking here about marketing and promotion. But one vital thing to mention is how cryptocurrencies can be actually used in foreseeable future.

For now, cryptomoney is naturally suitable for donations. It is easier to send and, speaking of new currencies, way easier to get. Another field for usage is online shops which accept them. For the first time, it would be enough to offer some cheap and truck goods and services. A lot of work on these two segments can be done by independent creators: musicians, filmmakers and bloggers. And that is a real path for cryptocurrencies putting into, because only real people can give the future to something if they really want it to exist.