

Bitcoin: main trends and perspectives^{*}

Abstract. *In the article describes the history of the emergence of private money; the principal laws governing the functioning Bitcoin and relationships characterize them. Formulated prospects of Bitcoin as alternative of private money and identify the reasons for opposing the production of their legal status in Russia and other countries.*

Keywords: *alternative private money, e-currency, cryptocurrency, shadow economy, emissions, revenues from “mining”, costs to users, the rate of Bitcoin.*

Introduction. Bitcoin (BTC) – modern electronic currency, exchanged on financial markets since 2009. Due to its economic origins it is considered a variation of alternate private currency and one of the crypto currencies presented.

Cryptocurrency – type of digital currency, which emission and accounting is based on cryptographic methods (for example, proof of work method for information protection and asymmetric cryptography), and system works decentralized in a computer branched (so called peering) network [1]. Principle of anonymous is used in crypto currencies - all transactions are public, but there is no link to particular user within the system (but his/her identity can be found out in case of additional information presented).

Modern times, crypto currencies are considered alternate fiduciary (based on trust) money, emitted and used by private institutional investors. In many countries emission of private (alternate) money is prohibited, in others it's legal, but strictly regulated. Thus, in US during so-called "Free Banking Era" (1837–1866) was issued around 8000 of different kinds of private currency; issuers were particular states, cities, banks, shops, individuals, etc. And up to this day, private money in US are officially legal, but subjected to tax each time transaction is occurred and its nominal value has to be more then 1 USD. In 2009 market of alternative private money blossomed due to world financial crisis.

In a last year due to markets' uncertainty and high volatility of some currencies, alternative private money looked more and more attractive.

Idea of alternative private currency was proposed almost simultaneously and independently from each other in 1974 by B. Klein, and in 1975 - by Friedrich von Hayek [3].

F. von Hayek, well known Austrian economist, in his book 'Private money' criticized current money system itself, and proposed fundamentally new plan for achieving it's stability, based on free competition of alternative private currencies. Likewise, a competition between common goods increases it's qualities for consumers and sort a low quality product out, free competition between private currencies should have the same impact, leaving only those of the most friendly to consumers. Decentralization of currency supply would increase it's efficiency, since federal monopoly on currency emission inevitably destroy it's value and extremely dangerous to society [3].

Fon Hayek's ideas were supported by economy Nobel Prize winner Milton Friedman, in 1986 article "Has Government Any Role in Money" [4]. It was found out, that money systems, which existed before central banks era and were based on a principle of free competition, appeared to be effective enough.

Thus, the idea of alternative private currency has a solid methodological base behind

^{*} This article was supported by the Russian Humanitarian Foundation. Project № 15-32-01213.

and has a history of its implementation in real life. Current variations of electronic private money are crypto currencies presented by different electronic money exchange and transaction systems: Bitcoin, PPCoin, Novacoin, Namecoin, Sifcoin, Litecoin, Quark and others.

Bitcoin is considered to be a most common, capitalized and effective crypto currency, with main exchange and transfer protocol well built in. All other crypto currencies are in one way or other, some variations of Bitcoin, and use similar algorithms.

Methods. Comparative analysis for some examples of crypto currencies is presented in table 1, which reflects a currently dominating position of Bitcoin.

Table 1

Comparative analysis of different crypto currencies [5, 6]

Currency name	Ticker	Year of emerge	Inventor	Site	Market cap.	Hash ^{*)}	Note
Bitcoin	BTC	2009	Satoshi Nakamoto	bitcoin.org	7 bln. USD ^{**)}	SHA-256	First and most popular cryptocurrency; proof of work
Litecoin	LTC	2011	Coblee	litecoin.org	350 mln. USD	Script	Proof of work
Namecoin	NMC	2011	Vinced	dot-bit.org	27 mln. USD	SHA-256	Created resistant for internet censorship;
PPCoin	PPC	2012	Sunny King	ppcoin.org	72 mln. USD	SHA-256	Has no limit for overall emission, hybrid mechanism proof of work / proof of stake
Quark	QRK	2013	Max Guevara	qrk.cc	12 mln. USD	Blake, Bmw, JH, Keccak, Skein	Takes 30 seconds to confirm a transaction; hybrid mechanism proof of work / proof of stake

^{*)} hash (hash – code, message digest) – result of hashing operation – compressing a databases via predetermined algorithm; used for control of transfer, storage, and search of data; widely used for information encryption;

^{**)} market capitalization of Bitcoin is comparative to a volume of relatively small country (for example, Belorussia).

From this point of view, Bitcoin can be examined for basic principles and patterns of crypto currency as a broad sense idea.

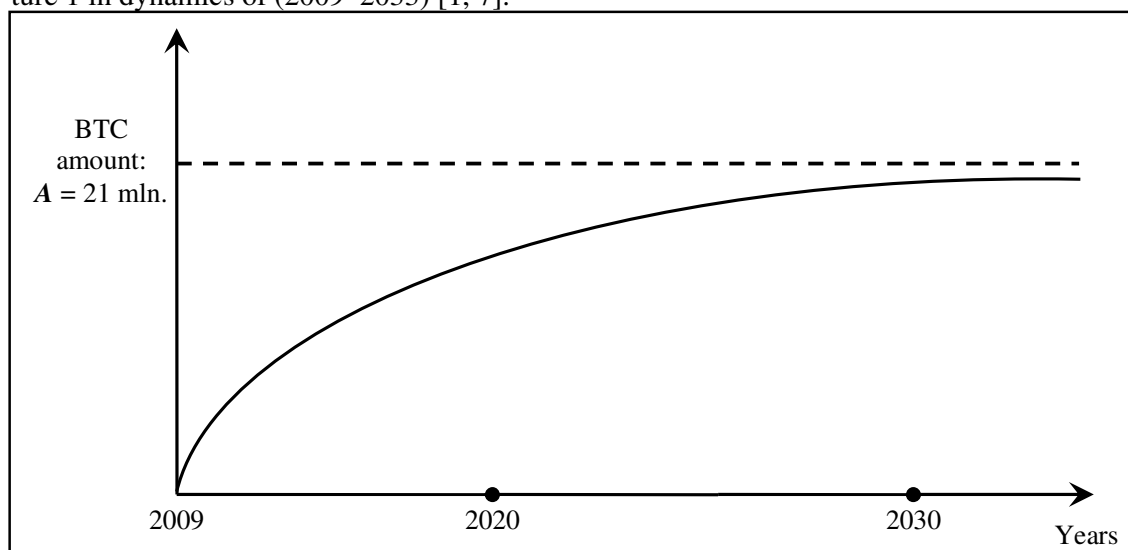
Bitcoin was created in 2009 by japans programmer (Satoshi Nakamoto), or by a group of people under this nickname. Now, Gavin Andersen is responsible for development and coordination of BTC system.

Many analysts claim BTC to be an ideal currency for electronic transactions due to following factors:

- 1) Transaction speed (operation is confirmed almost instantly);
- 2) It's cost (currently, transaction fee is 0.0005 BTC for small volume);
- 3) Exact cryptographically identification of each transaction for particular address, (available to everyone and undeniable);
- 4) Liquidity and convertionability.

Exchange and reconvention of BTC into rubles, dollars, euro and other currencies (also – electronic) takes place in different electronic exchange sites (for example, BTC-e.com, metabank.ru, Bitfinex, BitStamp, BTC China) and takes minutes to execute [6].

Emission of BTC is totally decentralized (performed by users of the system themselves) and limited by time and volume. Expected amount of issued BTC is presented on picture 1 in dynamics of (2009–2033) [1, 7].



Picture 1. Expected amount of issued BTC.

Chart 1 reflects dependency of exponential type, with asymptote in point A , equals 21 billion BTC, which marks systems emission limit. Graphically, function looks like:

$$Q(BTC) = A[1 - \exp^{-at}] \quad (1)$$

Where:

$A = 21$ billion BTC, t – timeframe, a – function parameter which defines its growth acceleration.

Result .Accordingly to displayed chart, it is suggested that curve would reach it asymptote point in years of 2030–2033, which would be an end of BTC emission.

User's production is stimulated by an opportunity of reward in a form of newly issued BTC (for a data processing operation), later this was called a 'data mining' (like mining of raw minerals). Emission is conducted in a random way and is dependent on creation of the information blocks created by overall user's transactions.

Speed of block creation is regulated. It is planned that all network would spend approximately 10 minutes on each block to create, and on 2016 blocks – about two weeks. Each 2016 blocks a correction is performed – if blocks were created faster then in two weeks, speed is reduced and vice a versa. It is done in order to maintain a constant speed of block generation, independently of overall network capacity.

Random emission event is occurred each time transaction legitimacy is confirmed. Any transaction is not considered legitimate (confirmed), until corresponding data would be structured, accordingly, into a blocks. Those form specific links then, which can form different branches. It has been established that each branch is equally legitimate until one becomes longer; when branches are equaling length, the one which had its last block created earlier is confirmed legitimate. Transactions went into less longer link loose its value along with an opportunity of reward.

Probability of this event is likely to decline as link grows its length. Thus, mining income of i -indexed user is based on (pic. 2):

- 1) math expectation of reward for creation of blocks;
- 2) commission value, which is reflected by following:

$$D_i^M = S_i^C(t) \cdot P_i + K_i, \quad (2)$$

where:

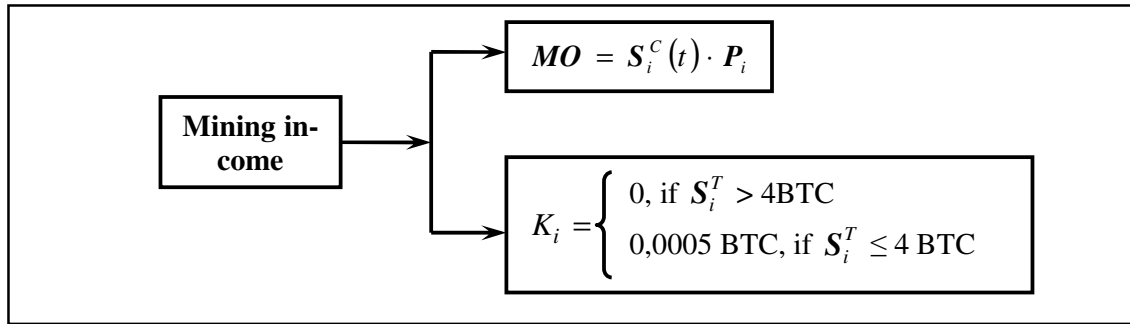
D_i^M – Income from mining;

$S_i^C(t)$ – Discrete (stepwise) reward functions by a factor 0,5, which determines the amount of compensation by i -indexed user, as decreasing geometric progression dependent on time;

K_i – Discrete function reflecting commission value accordingly to step of probability of mining reward for i -indexed user; $0 \leq P \leq 1$;

P_i – Discrete (stepwise) function, reflecting reward value of i -indexed user, as a declining geometric progression, dependent on time;

S_i^T – Transaction value for i -indexed user.



Picture 2. Income for i -indexed user in BTC network.

Probability of reward P_i during 10 minute timeframe (approximate time for a block creation during an established network performance) is defined by equation:

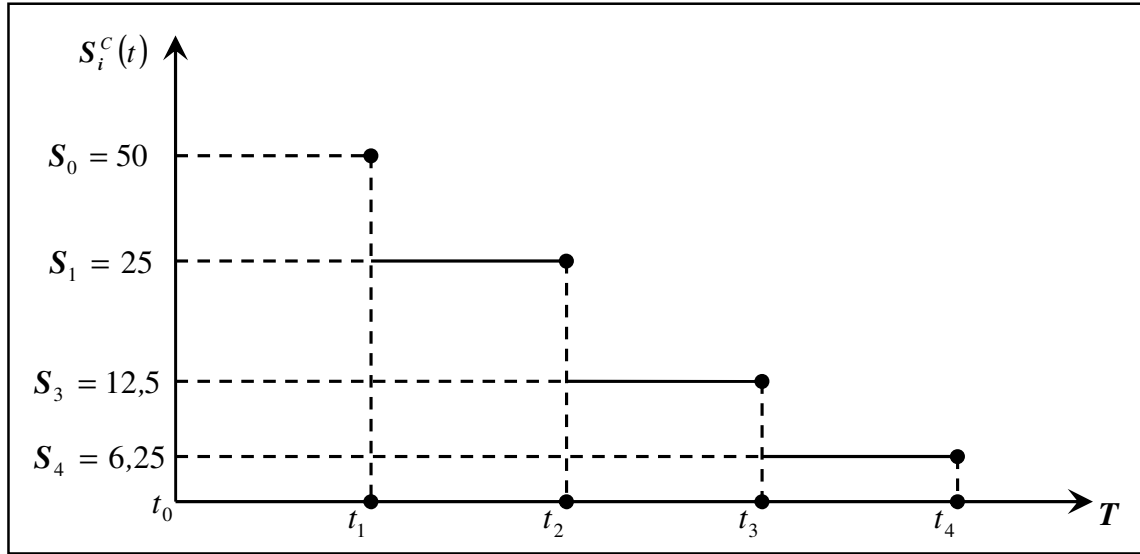
$$P_i = \frac{M_i}{M_{overall}}, \quad (3)$$

where:

M_i – Calculating capacity of i -indexed user;

$M_{overall}$ – Capacity of whole system.

During the time $M_{overall}$ usually grows significantly faster then M_i , therefore probability P_i becomes less. Reward value declines also (pic. 3).



Picture 3. Reward value.

Function $S_i^c(t)$ is defined on a timeframes set by points $t_0, t_1, t_2, \dots$, during which a set of 270000 information blocks created each (which takes approximately four year in average). First cut on a value of emission (point t_1) occurred at 28 November, 2012, less then in 4 years.

Therefore:

$$S_i^c(j) = \begin{cases} S_0, t_0 \leq j < t_0 + 1 \\ S_i^c(j-1) \cdot q, t_0 + j - 1 \leq j \leq t_0 + 1 \end{cases}, \quad (4)$$

Where:

$t_0 = 0$ – First time period;

j – Correction number for emission reward;

q – Correction coefficient; $q = 0,5 < 1$;

S_0 – First time reward ($S_0 = 50$ BTC);

$t \in [0, T]$ – Time gradient of the system.

Accordingly to formula (4) emission reward value declines geometrically: $S_i^c(t) \rightarrow 0$ while $t \rightarrow \infty$, and after emission ends, mining income D_i^M would consist only of commission.

Already this time it takes significant calculating capacities and expenses for electricity. Thus, net income from mining should be corrected by taking into account occurred expenses Z_i :

$$\tilde{D}_i^M = D_i^M - Z_i, \quad (5)$$

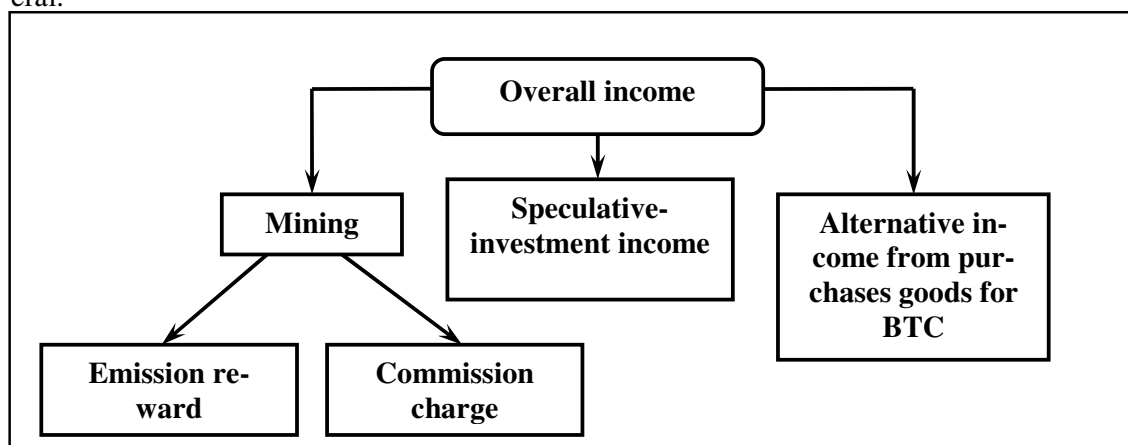
Where: Z_i – expenses, growing along with network expansion, at a first time frame were not significant to take into account.

Since it became much harder for users to generate blocks (amount of calculating power required to create one block in 2013 became half a million times higher, then when system had only started to work), users start to join so-called mining pools to combine their effort

and increase a probability of emission reward comparatively to solo mining.

Rules of emission provided privilege for mining pioneers: in relatively simple and effective conditions (each 10 minutes – 1 block and 50 BTC out of thin air), they managed to mine significant amounts.

Thus, experts estimated more then 1 million BTC in Satoshi Nakamoto virtual wallet, an equivalent of several hundred millions of dollars in 04.2014 [8]. Later period presumes a change in user's activities, from mining to investment, (pic. 4) and online shopping. Speculative income is dependent on BTC rate forecast and development of crypto currencies in general.



Picture 4. Income of BTC network user.

Forecasts are mainly contradictory. Some experts expect further growth of BTC rate and decline of its volatility, presenting such arguments as limited emission and demand growth. Optimists evaluate future BTC rate as 40 000 use and higher; comparing BTC network to Internet, they speculate that in year of 1993 it was absurd to imagine some domain names to cost 10 millions of dollars, nevertheless it's a price after 20 years [9, 10].

Others expect BTC rate to decline 100 times over, after which it is supposed to blow like another financial bubble [11].

Such a variety of opinions is due to volatility of current BTC market, which reflects instability of any emerging and rapidly expanding system. So, during a relatively short period of time, BTC rate grew with incredibly high speed: from 0,3 cents (25.04.2010) till 1000 USD (28.11.2013), so average growth estimated as 725% per month, in 2014 it remained in range of 400-500 USD (table 2).

Table 2

Main tipping points in BTC dynamics [1]

Date	BTC exchange rate	Event
25.04.2010	0,3 cent	System start
10.02.2011	1 USD	BTC equal to USD
30.05.2011	8,89 USD	Growth after Forbes «Crypto Currency» article
09.06.2011	29,57 USD	Growth after article about underground resource «Silk Road»
19.06.2011	5 USD	Decline after a news about MT Gox exchange
28.11.2012	20 USD	First cut down of emission (2 times)
22.02.2013	30 USD	New historic high
01.04.2013	100 USD	Period of fast growth (end of February-March)

10.04.2013	266 USD	Period of extra fast growth
16.11.2013	900 USD	Different rate at different exchanges
28.11.2013	1100 USD	maximum for period
05.12.2013	500 USD	Panic sales after China's central bank's ban on BTC operations current
2014–2015	400-500 USD	Period of relative stabilization
	200-300 USD	

Crypto currency (BTC in particular), has its supporters and oppositions relatively its role and place in financial system in general.

German Gref views crypto currency as a very interesting experiment, shifting a paradigm of currency emission. It should definitely remain legal, has to be studied and, probably, regulated in a right way [13]. In case of favorable scenario for development and practical implications, it can seriously affect both financial markets and social life in general. Taking into account rapid capitalization growth in crypto currencies markets and relatively low growth of world's financial markets, after some time crypto currencies sector can claim a significant part.

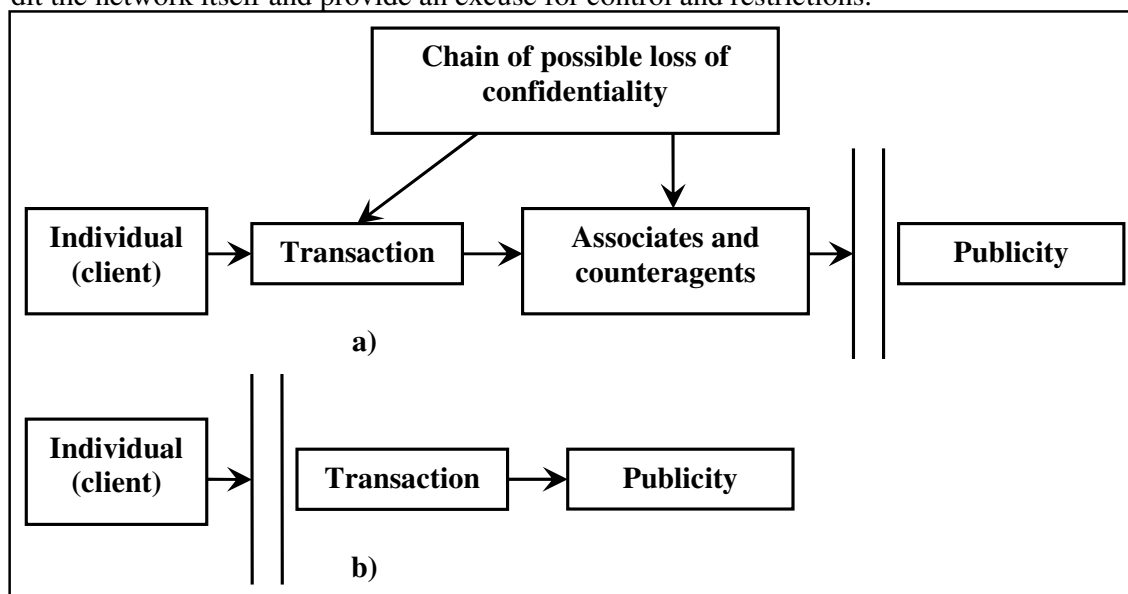
Conclusion. As for BTC system in particular, its supporters consider it a major breakthrough in computer science, same way as world wide web in 1993 and personal computers in 1975 [14, 15]. They point also high level protocol and flawless logic utilized in the system. Dan Kaminsky, known cyber security specialist, confessed that he tried to hack into network in 2011, but failed to find any weak point [16].

Crypto currencies skeptics doubt its benefits as a financial instrument and perspectives for long term existence [17]. Three major arguments re pointed out:

1. Network has a conflict of interests with a state as an institution management: state loses its control over financial streams, which means it loses power over economical situation in general. Therefore, state would naturally reject out-of-control alternative currency exchange network between individuals. Of course, direct restriction is not possible, as it is not possible to restrict individuals to communicate with each other over internet. Alex Fork, an author of popular book "BTC – more then just money", claims that government not able to fully control BTC. By law, electronic currencies can be banned, but there is no means to practically control it [18]. Nevertheless, government has massive leverage in crypto currencies' functioning process. Like restriction to exchange into national currency (China did it in 2013), or into major currencies, discrediting the idea of international alternative currency itself. If such a sanctions would be implied by biggest economies cooperatively, BTC would turn into a kind of penny stock. And this scenario is quite possible as more and more countries gradually introduce such a restrictions.

2. Network is also in a relative conflict with society in general. It is hard to say what was on Satoshi Nakamoto mind when he presented his network with a principle of anonymity. Maybe, it was “golden rule” of business: big money does not like any public exposure. Maybe, he wanted to make BTC attractive for most users, including businessmen, entrepreneurs, which are into legitimate business, but would prefer privacy as a protection from possible competitors. But his privacy model (pic. 5) has opened a wide area of opportunity for so-called “shady business”. One of famous examples - internet-shop “Silk Road”, which traded various types of drugs, pornography, etc. for BTC. It was shut down in October of 2013 by FBI with a turnover of 30000 BTC or approximately 25 million USD. Other Example – in same autumn of 2013, assassination market was found in Tor network, which was dedicated to raising BTC for funding political and social assassinations [19], etc. All those facts discre-

dit the network itself and provide an excuse for control and restrictions.



Picture 5. Comparison of confidentiality models: a) traditional; b) in BTC system.

3. Cryptocurrency and BTC delivers significant economic damage first of all – to financial sector and national currencies, as a serious competitor; reduces income from emission and transactions. Many experts point at undisputed link between BTC and flow of capital abroad, because due to its cryptographic qualities, BTC is a useful system for covert capital displacement. And this leads to decrease of investment activities, reduced tax income, utilization of illegitimate financial schemes, etc.

4. In methodological view, BTC as an instrument of exchange is criticized by many experts. Former head of Federal Reserve System, Alan Greenspan, during his interview to Bloomberg news agency said: “Currency should have its own value. And it takes a lot of imagination to realize that BTC has any on its own. I really could not” [20]. And BTC supporters answer was: “Maybe he can tell then, what is the real value of US dollar on its own?” – pointing that trust was always a real value of all currencies, which is a principle of all fiduciary money.

Regardless on which scenario would take place in future, whether BTC network continues or cease to exist, its role and impact on society and financial sector can not be underestimated. The very fact of its existence modern times is not by a random chance.

Financial sector and stock markets has reflecting qualities and one way or other display most important events for society [11]. One of the most significant world’s trends is a change into information society and economics of knowledge [12]. If IT-technologies and calculating computer power can be considered one of the most important way of applying current knowledge and intellect, then, methodological base for BTC is totally aligned to this trend. And appearance of this cryptocurrency is a reaction of financial markets on innovations that take place in a society, according to which; holders of knowledge have an advantage over others. Very same thing happens within BTC, when income from mining is likely to be shared between users with most calculating powers. And it’s not by a chance, that in US (one of the most advanced countries on it’s way to information society), there is no direct restrictions for BTC; instead, there is a motion towards its legislation.

That shows that in future, systems of that kind, based on a conception of knowledge (if not BTC, then some of its analogues), and would take its rightful place in a society.

- 264 Bibliography list:
 265
 266 1. <https://ru.wikipedia.org/wiki/Биткойн>
 267 2. Klein B. The competitive supply of money // Journal of Money, Credit and Banking, 1974,
 268 № 6, p. 423-453.
 269 3. Hayek F. Private money / http://www.libertarium.ru/1_lib_prmoney
 270 4. Friedman M. Has government any role in money? 1986.
 271 5. Brief crypto currency review / <http://btcsec.com/bitcoin-forks/>
 272 6. Crypto currencies as peering systems / <http://paysyst.ru/crypto-payment-system.html>
 273 7. Bitcoin: analytics, reviews, complexity, forecasts / <http://onecoin.ru/info>
 274 8. Earned wealth of Satoshi Nakamoto / <http://habrahabr.ru/post/177149/>
 275 9. K. Winklewoss forecast BTC rate to grow up to 40.000 us /
 276 <http://www.banki.ru/news/lenta/?id=5992054>
 277 10. Venture Capitalist Chris Dixon Believes Bitcoin Will Hit \$100k /
 278 <http://www.coindesk.com/venture-capitalist-chris-dixon-bitcoin-will-hit-10000/>
 279 11. Egorova N.E., Bakhtizin A.R., Torzehevskiy K.A. Stock markets forecast with econom-
 280 ic-mathematical modelling. – M.: URSS, 2013.
 281 12. Economics of knowledge // Ecology and life, 2003, № 1.
 282 13. German Gref on cryptocurrency in Davos / [http://newmoneyfeed.com/news/german-](http://newmoneyfeed.com/news/german-gref-o-kriptoalutah-v-davose)
 283 [gref-o-kriptoalutah-v-davose](http://newmoneyfeed.com/news/german-gref-o-kriptoalutah-v-davose)
 284 14. What is so important about BTC? / [http://habrahabr.ru/company/host-](http://habrahabr.ru/company/host-tracker/blog/210126/)
 285 [tracker/blog/210126/](http://habrahabr.ru/company/host-tracker/blog/210126/)
 286 15. Marc Andreessen. Why Bitcoin Matters / [http://dealbook.nytimes.com/2014/01/21/why-](http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/)
 287 [bitcoin-matters/](http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/)
 288 16. Dan Kaminsky tried to hack BTC, but failed / <http://www.xakep.ru/post/60452/>
 289 17. Experts expect a 100 times over decline in BTC / [http://teh-](http://teh-nomad.livejournal.com/1987856.html)
 290 [nomad.livejournal.com/1987856.html](http://teh-nomad.livejournal.com/1987856.html)
 291 18. Alex Fork interview, writer of “BTC - more then just money /
 292 <http://www.coinside.ru/2014/07/03/intervyu-s-avtorom-knigi-bitcoin-bolshe-chem-dengi/>
 293 19. 12 amazing facts about Bitcoin / <http://hitech.vesti.ru/news/view/id13771>
 294 20. Everyone Is Baffled By Alan Greenspan's Comment About Bitcoin /
 295 <http://www.businessinsider.com/alan-greenspan-bitcoin-comment-reaction-2013-12>