Journal of Computer Sciences

Case Reports

The Conceptual Principals of Bitcoin Crypto Currency

Seitim Aiganym

Department of World and National Economy, Turan University, Republic of Kazakhstan

Article history
Received: 24-05-2014
Revised: 16-11-2015
Accepted: 26-12-2015

Email: Seitima@mail.ru

Abstract: In recent years, ideas about crypto currencies with interesting and new for today monetary principles becoming more and more popular. The crypto currencies' met different attitude to it new for the world finances principals. There are different talks. Ones think that it may improve monetary system, others think that it is a toy money that may cause instability and crash the world finance. However, the fact is that innovative concept of e-currency still developing and becoming more popular and in this way crypto currencies, particularly the most popular one-bitcoin is more useful and more preferable way of transaction in Internet. For today its audience accumulated a 9 billion USD on exchange stocks specially designed for crypto currency. The paper is about the new currency and about its innovative principles that can be used in current financial situation.

Keywords: Crypto Currency, Bitcoin, Decentralized System, Deflation Theory of Money, Theory of Demand and Supply, Peer to Peer Principle

Introduction

There is no doubt that 21st century is information technology's century. As an electricity Internet is one of the most needed resource in simple modern life. Information, trading, consultation, some kinds of services are became more available by Internet. Sales, in some cases services turn the focus to online trading. All what we can do by Internet saves time and money not only for consumers, but also for companies that offers different service. Comparing with traditional markets, goods in Internet have more facilities to be known, so it raises sales. Progress of technologies stormed big audience and we can meet a big variety of devices that make modern life closer to the Internet space. Trend of growth of sales in Internet is obvious. For more comfort and security online users register e-wallets for payments in Internet. Informational technologies have sunk deeper than before in using fields.

About 2008/2009 economic crisis have influenced on world money circulation system. Particularly world trust and hope on American dollar going to fall and there are some ideas in the economic world about creating new notes. One of them is The East Africa countries Union. They are planning to issue own currency in 2014 was cited in (Koroleva, 2013) article. The same ideas interested Customs Union of Kazakhstan, Russia and Belarus. In December 2008, ALBA group countries-The Bolivarian Alliance member countries met to approve the technical details of the introduction of the SUCRE - new regional currency and in 2010 it was implemented for inside use in noncash form.

Tomberg (2010) judgment, head of the Energy and transport research Center of the Institute East of RAS, MGIIR Professor, we can't to deny dollar's status as world money at all. It can cause global economics collapse. However, we can watch increasing intention of some countries to reform the system that based on dollar and the idea is not only "anti-American" countries' like Iran and Venezuela, but also ones whose economic prosperity depend on dollar. The latters are the record dollar reserve holders (China) and hydrocarbon exporters (Arabic countries, Russia). For today we can say that pegging the national policy to the dollar not always makes positive influence. So several countries and groups working at own regional currencies. Thus, we can see how the world economy is becoming more diverse and complex.

This seen not only in creation new currencies, but also in creation of new forms of notes. From plans to actions have gone one unexpected for the world economy monetary system – Bitcoin. Facts about the popularity and convenience of the new payment system speak for themselves. New system based on cryptography may become an alternative global currency system in the principles and forms of circulation of money. Bitcoin system was implemented as transaction system for Internet-commerce. The speed, ease, no third

parts, very little fees for transfer, the irreversibility of the transaction all of this are made Bitcoin popular in Internet in short time. But today, the field of Bitcoin use have rose. The coins were the subject of bargaining and the speculative interest. Shortly it marked as BTC.

We can conjecture, if the popularity of this new wave came after crisis of 2008 and make positive influence for developing trend in Internet, or it is just an evolutionary level. But it is obvious that rise of the crypto currency's era comes to this time. The conception of currency with decentralized issue in Internet became known in short time.

Lately in the world felt very sharp public interest in crypto currency bitcoin. News feeds are full of a wide variety of facts. People can pay in bitcoins for a pizza, even for a tickets to space travelling. Famous investors brothers Winklevoss invested in bitcoins 11 million USD. Now they are ones of the 150 ticket owners to the space travel from Virgin Galactic. University of Nicosia (UNic) the biggest university in Cyprus accepts bitcoins for education fees said Ioannis-Alexandros (2013). UNic is the first educational institution worldwide that works with bitcoins as with real money.

Unfortunately, not all related to bitcoin news are with positive wave as it was mentioned before. Where is a benefit - there is a risk and not everyone can successfully operate with it. So there is a version that bitcoin rate shocks caused suicide Otemn Rathke, head of bitcoin market First Meta. At the end of February 2014 her body was found in her apartment in Singapore. That period was one of the crisis for the crypto currency. Hacker attacks, negative reactions of China central bank and other news entailed bitcoin rate to fall. In short-term period it is difficult to assess the rate. Negative news pull its rate down, lower price stirs interest and curve again climbs up. Things act in accordance with market mechanisms. So thing make a lot of interesting discussions around the new digital currency.

Problem

Today, when the whole world is dissatisfied with USA's monopoly power to issue dollars, the topics about new money, new monetary system became extremely urgent. On Euro's example there is more than one issuing countries. In spite of this in Euro monetary system there is also unexpected moments. In this system not everything was taken into account. Greek debts indicate that. And in crypto currency's system we see fresh vision. On the face of its decentralization, money issue, can be mentioned like unpositive, but with bitcoins all of them work for the benefit of society. Decentralized, so there is no single regulator. But the system has been based on open source where all the necessary data like unit issue, coin generation, total number of coins, exchange rate, transaction data known to all. It turns out that well-known financial institutions with central banks led the world economy to the state where many terms depend on the world currency's rate, where countries are start exchange devaluation chain, where the incomes of the society face the risk of smooth or instant (in case of default of the national economy) depreciation. When bitcoin's value determined by common law of supply and demand, where only coin owners regulate the price. If no one buy or sell them, just if there is no economic operations with bitcoins, the system will lose its importance and so its value too and here works a mutual point: Each user depends on the system and the system's functioning depends on the users. So we can sum that default risk depends on the consumers activity and not from the policy of any country.

Bitcoin Generation and transaction program, the functionality of the currency includes all necessary qualities that have to have a world currency. The system have quantitative limit. They can be exchanged to traditional monetary units. Value of the currency is determined by the market. So here supply and demand are the only factors that make its value. The main uniqueness of this unit is in its decentralized emission and here can be seen a paradoxical for a modern financial system moment, where the system with some bank functions works without a banks, without a center. All users act as a kind of joint bank. The program was based on peer to peer principle (for more details see part "Transaction and issue mechanisms"). Thus the issue of the coins insured from individual intervention and side regulation. Number of coins found initially, the issue and transaction rate directly dependent on bitcoin consumers. Increased number of users influences on the speed of new coins' generation. More users, more difficult to generate the coins. This insures the currency from inflation risks. Total emission of currency known initially, it is equal to 21 million coins. The generation of each coin carried by users, particularly by their computer capacities'. Passing known mathematical algorithm, which is carried out by solving specific cryptographic tasks, computer user or group of them generate new coin units and mined new ones are divided among the participants of the process.

Transaction and Issue Mechanisms

We have mentioned before that bitcoin is a decentralized crypto currency with peer-to-peer network. What does it mean in monetary field? On programming language by Kelaskar *et al.* (2002) Peer-to-Peer (P2P) applications allow peers to connect or disconnect from a network at any time and are based on a loosely coupled resource distribution model. P2P is based on an equality of participation. Interpreting this concept in the language of economics, we can say that Bitcoin is not controlled

by a single central bank and operates with collective participation of users of the system.

In order to make full vision let us start with simple transaction algorithm. In his application Satoshi (2008) explains transaction as an initial level which makes the system to work. All transactions are arranged in chain which forms block diagram. Block chain is a public transaction log, which is based on Bitcoin network. In block chain included all agreed transactions, without exception. New transactions are confirmed if their initiator has necessary found for transaction. This insures double use of the same funds. Integrity and history of transactions in the block chain are based on cryptography. The steps to run the network are as follows:

- New transactions are broadcast to all nodes
- Each node collects new transactions into a block
- Each node works on finding a difficult proof-of-work for its block
- When a node finds a proof-of-work, it broadcasts the block to all nodes
- Nodes accept the block only if all transactions in it are valid and not already spent
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof of work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

After understanding the mechanism of the transaction let us go to the concept of bitcoin issue, unit generation. New units of bitcoin generate by mining, today it is also one of the ways to earn BTC. Mining is a distributed system used to confirm transactions. In order to confirm a transaction, units should be packed in block chain. The Chain passes strong cryptographic requirements. After all steps are done, whole network conformed the chain, problem is solved, the system creates waited coin units. These rules do not allow fraud intention to change the previous block, so in this case all of the following units would have been invalidated. In addition, mining eliminates the any possibility of sequential adding of units in the chain by any user. So, no one can control block chain or replace other parts to return implemented transaction. As we mentioned before, after solving the problem, miners rewarded with coins, which are distributed between the participants. The more number of participants, the harder the process goes. To compensate for increasing hardware speed and varying interest in running nodes over time, Satoshi (2008) created the proof-of-work. Difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases. The generation of coins made by this algorithm. In contrast to traditional currency, Bitcoin have initial limited monetary base. Underlying rules in program base and can't be adjusted. The generation of coins will be stopped after last 21st million coin created and there is one good point, to avoid deflation moments, each coin can be divided up to 10 in 8th power. As division insures from deflation, limited issue help with inflation risks. This two points are the ones that don't have any other currencies today. We may think, that this principles can be brought to create new reformed monetary system. Let's return to issue principles. Mathematically conditionally bounded resource defines (determines) by the speed function in creating total units of crypto currency from times speed function in creating total units of crypto currency from times. This function is inversely proportional to time. So with the lapse of time the rate falls down and tends to zero. If we take the integral of this function over time, we can get an exhibitor that is shown on the Fig. 1.

Figure 1 shows the final number of coins and the estimated time when the last unit will be produced. The system always updates the monetary base. The system is programmed to mine coins in packs approximately every 10 min, the number of coins in one pack is equal to 50 coins. The number of coins in a pack reduces by the time. The weight of pack becomes lighter twice every 4 years.

Operation principle of the crypto currency is decentralized and transaction accounts reflected on a common open platform so any user in system can monitor it. Open access to all information about transactions protects from forgery. But crypto notes are made anonymously. As we mentioned before, transaction information can be monitored by any other users, exceptions is only for the self information. As the registration system does not request any identification data. No one can know who is the real owner of the bitcoin wallet if the owner didn't want that. This property has become useful for criminals. When there is an anonymity, area with such property become like a heaven for people with unscrupulous motives. Even though there is no central Bitcoin server to compromise.

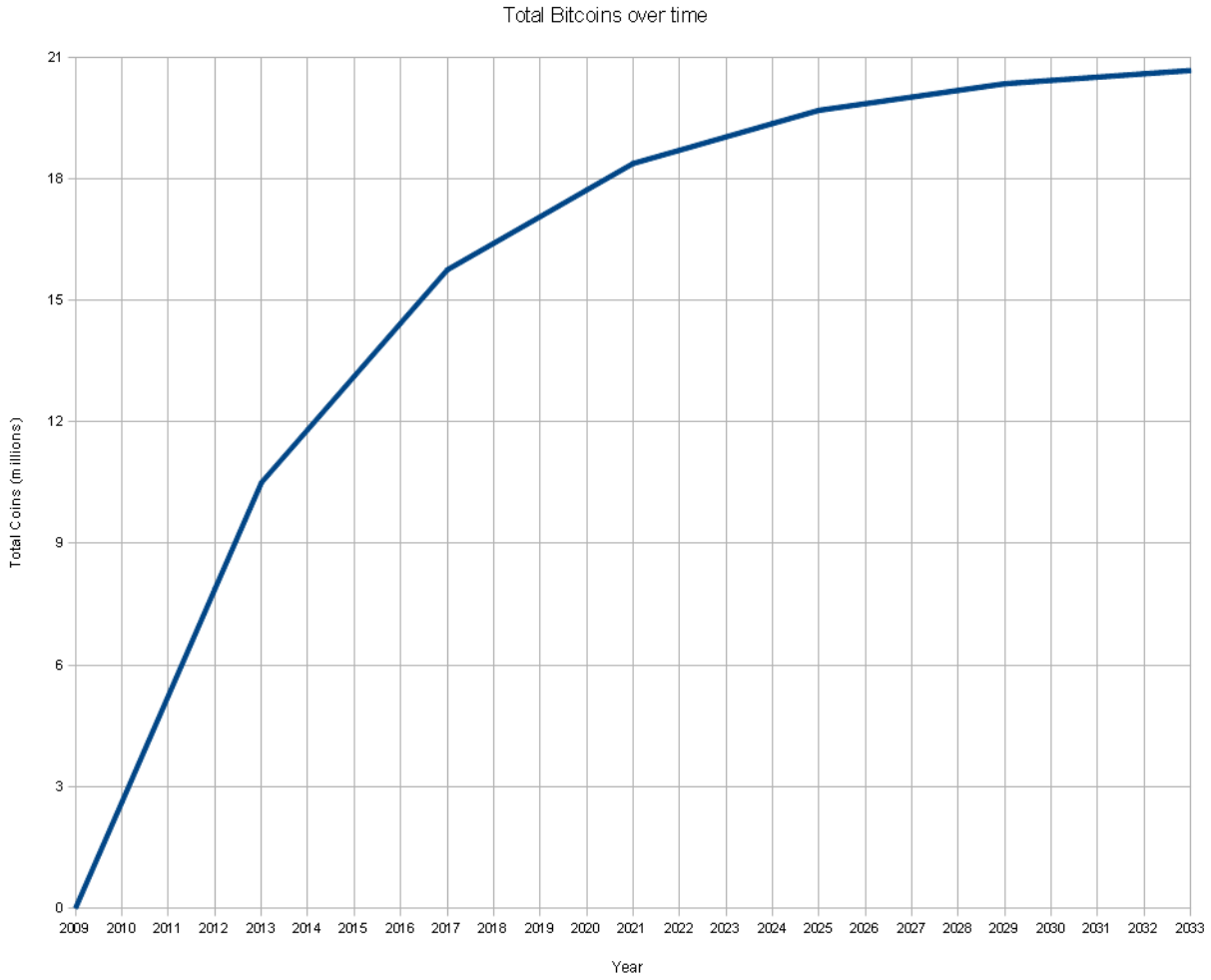

Fig. 1. The trend and the forecast of bitcoin emission for 2009-2033 years.
Source: http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

The FBI (2015) assesses with high confidence, based on reliable industry and FBI reporting, that criminals intending to steal bitcoins can target and exploit third-party bitcoin services and an individual's Bitcoin wallet. Malicious actors can compromise personal computers and accounts using malware and hacking techniques to steal users' bitcoins and use botnets to generate bitcoins.

First the concept of crypto currency was described by Wei (1998). Then in 2009 the first practical version was launched in mail list about cryptography by nickname Satoshi Nakamoto. Developer or group of them did not publish their names and left the program. They made the process to be acted and functioned by the users only.

Relying on the fact that money is a specific commodity with maximum liquidity, which is a universal equivalent value of other goods and services in the world or in the social economic context, Bitcoin system was designed in accordance to the idea of the new form of money that uses cryptography to control unit's issue and turnover, without relying on government. That is the bitcoin trading platform organizers' view. From the classical economic theory's view, money is the universal equivalent of goods and services, simply, it may be all things that people agreed to accept as exchange tool for goods and services. This definition have no doubt to assume that Bitcoin is a currency unit. However, like most exchange means, except for "real money" (as gold and other precious metals) – it is "unreal" money, but with determined value by the specific agreements between people, governments and states.

Instability of the global monetary system, financial cataclysms in 2008/2009 increased the interest in crypto currency. Beginning from 2010, by the help of a big number of developers working on the unit's project, Bitcoin community has increased significantly. In June-July 2011 mass media's attention to the Bitcoin system has led to the fact that buying coins began to spread massively. So it caused a financial bubble which decreased in size to the second half of 2011. But the

trend saved and continued to grow up. On September 27 in 2012 for the purpose of standardization, protection and promotion was founded Bitcoin Foundation. Today BTC economy is rapidly developing.

The idea of creating such kind of money substitutes is very actual today. In crisis and post-crisis periods work on improving always actualizes and activates. Besides, as Keynes (1993) cited in his work to Pigou's definition of money in his theory of production and employment – "there is no independent role of money in the economy. They worth just as much as benefits they can give". Here bitcoins meet the requirements of a simple system of currency values.

Implication

The idea of the Bitcoin system presents us how modern monetary system can be transparent, responsive for economic needs, automatically controlled withal all users involvement. Of cause today bitcoins are in circulation without a legal status, but also not forbidden in a lot of farsighted countries. As Sberbank CEO Herman Gref said in an interview at the World Economic Forum in Davos (Switzerland) "It's a very interesting global experiment that breaks the paradigm of currency issuance" and banning it would be a "colossal step backward" (Pronina and Kravchenko, 2014). He also wrote to the Kreml to stop curbing the use of crypto currencies.

So nowadays legal institutions don't know how to organize or use it in traditional system. That is the problem: when traditional system functions by central operation, Bitcoin system works by democratic de-central operation. All users by their action form its operation. For today's reality where traditional monetary system faces crises with their central management, this kind of system can be a good example to rebuild it for future stability.

Conclusion

There are some fears of this system and that have reasons. Bitcoin community is growing. It is a fact. If this system shows instability, there will be a risk of mass unrest and in this situation it will not be limited by one country, region or continent. Because all around the world where is an Internet access where people can and use the bitcoins. If the new currency system show stability and meet all the demands of the consumers, we can talk about the decline of the dollar monopoly era. Or, what is more likely to be, the emergence of the "second" parallel financial system, which can make the world finances more secure and flexible.

While analysts observe and give their skeptic views, Bitcoin market is growing up. But it is not easy to say how securely is it and in what situation the crypto-wallet holders will be in the coming decades. All the same, money should include the value of things and the labor by which it was mined and the generation of it is very complicated process, which is not only dangerous in short-sighted hands, but also fraught with global implications. Analysts and financial institutions of the world are thinking about this doubtful future of bitcoins'. Some wait unprecedented success in such projects, some see here special handmade interest. There are many sides that approve and disapprove the system, but there is no one on the neutral side. Without a dependence on the talks the crypto currency system still rising and developing.

Acknowledgement

Article was written by the Author. No Technical and Financial assistance were supported. All payment will be done by the author.

Ethics

This article is original and contains unpublished materials. The corresponding author confirms that there is no side with ethical issues involved.

References

FBI, 2015. Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. 1st Edn., Maroon Ebooks, pp: 20.

Ioannis-Alexandros, I., 2013. Euronews. http://www.euronews.com/2013/11/21/cyprus-nicosia-university-first-to-accept-tuition-fees-in-bitcoins/

Kelaskar, M., V. Matossian, P. Mehra, D. Paul and M. Parashar, 2002. Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid, IEEE Computer Society Washington, DC, USA.

Keynes, J.M., 1993. Anthology of economics classic.

Koroleva, A., 2013. Vostochnaya afrika vstala na evropejskij put. Expert Online.

Pronina, L. and S. Kravchenko, 2014. Bitcoin backed by sberbank's gref as Russia plans curbs. Bloomberg.

Tomberg, I., 2010. Sucre dlya poloviny ALBA. Open Economy.

Satoshi, N., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.

Wei, D., 1998. B-money. http://www.weidai.com/bmoney.txt