IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cryptocurrencies - Advantages And Disadvantages

A. Victor Benevent Raj,

Assistant Professor, Department of Computer Applications, Ananda College, Devakottai,

S. Charline Sugirtha,

Assistant Professor, Department of Computer Applications, Ananda College, Devakottai,

Abstract

Recently, **crypto currencies** and **Bit coin** have become the main topics of the financial industry. A crypto currency is a digital or virtual currency that uses cryptography for security. Crypto currency is difficult to counterfeit because of this security feature. Crypto currency's defining feature, and arguably its most endearing appeal, is its organic nature; it is not issued by any central authority, so it is theoretically immune to government interference or management. Crypto currencies have their advantages and disadvantages. The article covers various aspects of crypto currencies, starting with its early development, challenges and risks, opportunities, advantages and disadvantages, and its future. In addition, the post addressed issues related to the practical and technical function of crypto currencies. It was concluded that it is not easy to predict the **future** of crypto-currencies, as a lot needs to be done especially in the area of formal regulations. However, banks and other financial institutions should see and consider crypto currencies as an alternative for financial transactions in the future.

Crypto currency has been widely adopted as an **investment asset** with the rise of many well-known crypto currency exchanges. Practitioners and enthusiasts have started promoting crypto currency as a means of payment in the sharing economy. This new trend has also gained attention in academia, especially among **information systems (IS)** professionals. Thus, the purpose of this paper is to consolidate the knowledge of crypto currencies in the field of IS through a systematic literature review and provide insights for researchers to seek opportunities for crypto currencies research in the context of the sharing economy.

Crypto currency is a **digital currency** based primarily on block chain technology. Currencies are issued and regulated by the country's central bank and government to combat inflationary and deflationary situations. Today, many countries in the world are focusing on digital currency and transactions. Even someone does not want to regulate their currencies and transactions. This brought further innovation in the new currency

that is crypto currency, one of the most advanced, ambiguous regulations of a simple currency. In this article I have tried to study crypto currency and its development and future prospects in India.

1. Introduction

In historical retrospect, markets in general and financial markets in particular have experienced tremendous development. In this regard, the instruments used as stock exchange instruments also underwent changes, which developed in accordance with the needs of the markets with the aim of facilitating business transactions as much as possible. These instruments used to mediate the exchange of goods are known as money. Most economists define money as something that serves as a medium of exchange, a unit of account, and a store of value. Money is a medium of exchange in the sense that we all agree to accept it when conducting transactions. Merchants agree to accept money in exchange for their goods; employees agree to receive money in exchange for their work. As a unit of account, money provides a simple device store rewards for our work or business in a convenient tool. In other words, money allows us to store a long, hard week of work in a neat little pile of money. Without money, how would we set aside the compensation we receive for later use? Centuries have passed since the era of barter for commodity money, metal and coins, gold and silver, continuing with modern monetary systems and checks, and ending with the latest developments in global currency, such as the introduction of crypto currencies known as bit coin and ethereum. As each type of money played an irreplaceable role in the transactional activity of the given time period. However, as human society in general and markets in particular developed, the need arose for more sophisticated instruments of commodity exchange. In this regard, the introduction of crypto currencies has revolutionized the international payment system on a scale that was unimaginable just a few years ago. A crypto currency is a digital or virtual currency that uses cryptography for security. Crypto currency is difficult to counterfeit because of this security feature. Crypto currency's defining feature, and arguably its most endearing appeal, is its organic nature; it is not issued by any central authority, so it is theoretically immune to government interference or manipulation. Crypto currencies have their advantages and disadvantages. The main advantages of using crypto currencies are that they facilitate the transfer of funds between two parties to a transaction; these transactions are facilitated using public and private keys for security reasons. These fund transfers are done with minimal processing fees, allowing users to avoid the high fees charged by most banks for online transactions. The threat of hacking is the biggest threat to the crypto currency payment system. For example, in the short history of Bit coin, the company has been subject to more than 40 thefts, including several that exceeded $1 million in value. However, despite the potential risks, many observers still look to crypto currencies as a hope that there may be a currency that preserves value, facilitates exchange, is more portable than hard metals, and is outside the influence of central banks and governments. There are approximately 856 crypto currencies (see the following link https://coinmarketcap.com/all/views/all/.) According to Gandal and Halaburda, the competitive crypto currency market is an interesting market to analyze for several reasons. First, it was quite new a market that many players have entered and competed in. It is also an excellent laboratory with well-defined and high-quality price and volume data over time.

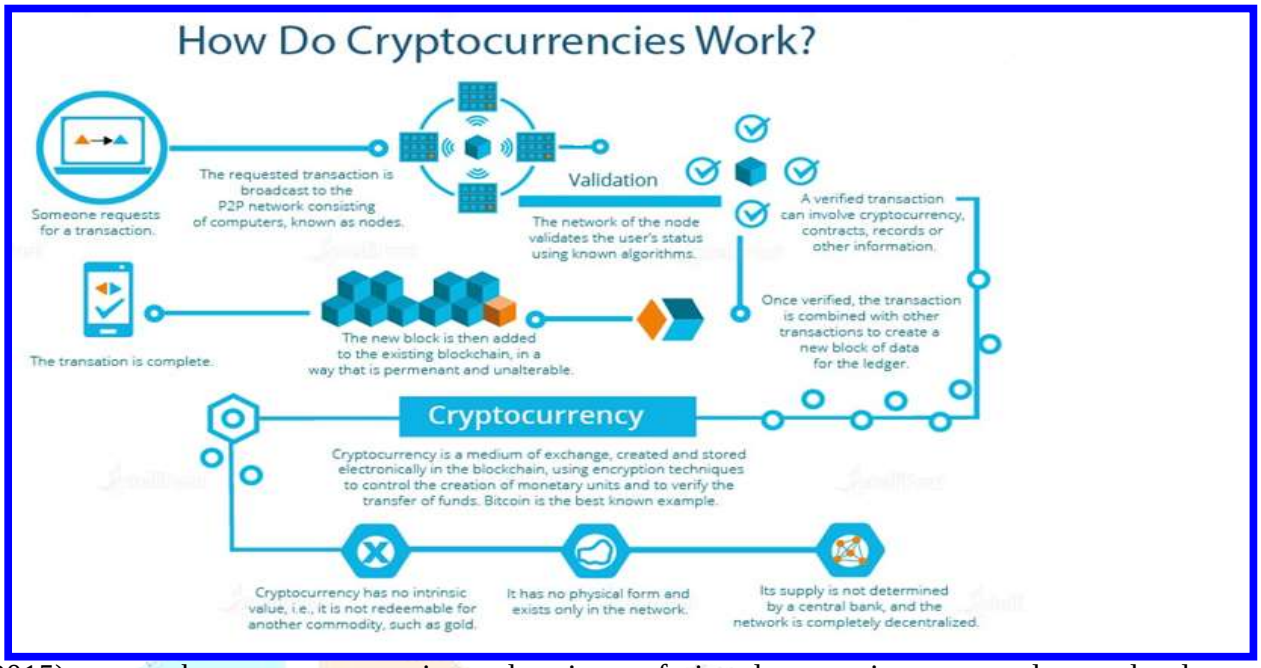
In terms of market capitalization, Bit coin is the leader in a long list of crypto currencies, followed by unearthly and Ripple, which have two million digits. Other crypto currencies have less value, with an increasing trend.

2. Literature review

Crypto currencies in general and Bit coin in particular have fallen outside academia. However, since their introduction, the contribution of academia in this financial and monetary area has been very significant. However, since the crypto currency market is developing at a tremendous speed and there is considerable confusion about what is going on, in our opinion, academic research in this area should be taken with a grain of salt and caution. Despite these facts, academic crypto currency research has contributed by revealing the limitations and pitfalls of the crypto currency payment system, but also suggesting ways to overcome them. The above authors argue that the main three advantages of crypto currencies are anonymity, privacy and confidentiality. However, we believe that the most important feature of a crypto currency payment system is transparency.

One may ask why! The reason why we believe that transparency is the key to the success of a crypto currency payment system is the fact that in this system, unlike a classic bank payment system, where the client only has information about his account. In a crypto currency payment system, everyone in the system can see the financial transactions of all other participants, making the system extremely transparent. Therefore, even if they are not backed by a sovereign authority, it is the high level of transparency that makes crypto currencies acceptable to their users. However, some authors such as Cameron (2016) argue that it is highly unlikely that governments will allow the use of crypto currencies in the way that currently works. Conversely, the author argues that most governments are well positioned to prevent the integration of crypto currencies within current formal financial institutions. Without these institutions, according to the author, the obstacles facing crypto currencies to replace more legally privileged and centrally issued currencies seem insurmountable. When it comes to issues of crypto currency exchange rates against traditional currencies such as the US dollar, despite much public attention, the theoretical understanding of the value of block chain-based crypto currencies is limited. In this regard, Li & Wang conducted a theoretical empirical study on the determination of the exchange rate of Bit coin (vs. USD), taking into account both technological and economic factors. According to the aforementioned authors, the bit coin exchange rate adjusts in the short term to changes in economic fundamentals and market conditions. The long-term price of Bit coin is more sensitive to economic fundamentals and less sensitive to technological factors. The authors further claim to have identified a significant influence of mining technology and the declining importance of mining difficulty in determining the price of Bit coin.

Some authors, such as Smalley, raised the issue of crypto currencies and taxation, saying that more needs to be done in this regard, as taxation of crypto currency transactions are not yet formally regulated. Finally,



Vora (2015) argues that crypto currencies and variants of virtual currencies are a welcome development, they will offer competition to existing modalities of money and government regulation, they will provide alternative means for economic entities for their transactions, and their innovative existence should be encouraged so that their beneficial properties surpass all harmful. Bit coins are here to stay, suggests the aforementioned author, unless governments deem it illegitimate or prohibited by regulatory measures.

3. What is Bit coin and how Crypto Currencies (bit coin) work.

According to Sarah Meiklejon et al (2016), Bit coin is a purely online virtual currency that is not backed by physical commodities or a sovereign obligation; instead, it relies on a combination of encryption protection and a peer-to-peer protocol to witness settlements. As a result, Bit coin has the counterintuitive property that while ownership of money is implicitly anonymous, its flow is globally visible. Bit coin was originally introduced by (pseudonymous) Satoshi Nakamoto in 2008. Since then, it has experienced a huge boom and generated millions in profit for those involved in this business. But how does bit coin work? The above authors Sarah Meiklejon et al (2016, p. 87) explain it as follows: “Bit coin can be briefly understood as a chain of transactions from one owner to another, where the owners are identified by a public key. Hence the address that serves as a pseudonym; that is, users can use any number of addresses and their activity using one set of addresses is not inherently linked to their activity using another set or to their real-world identity.

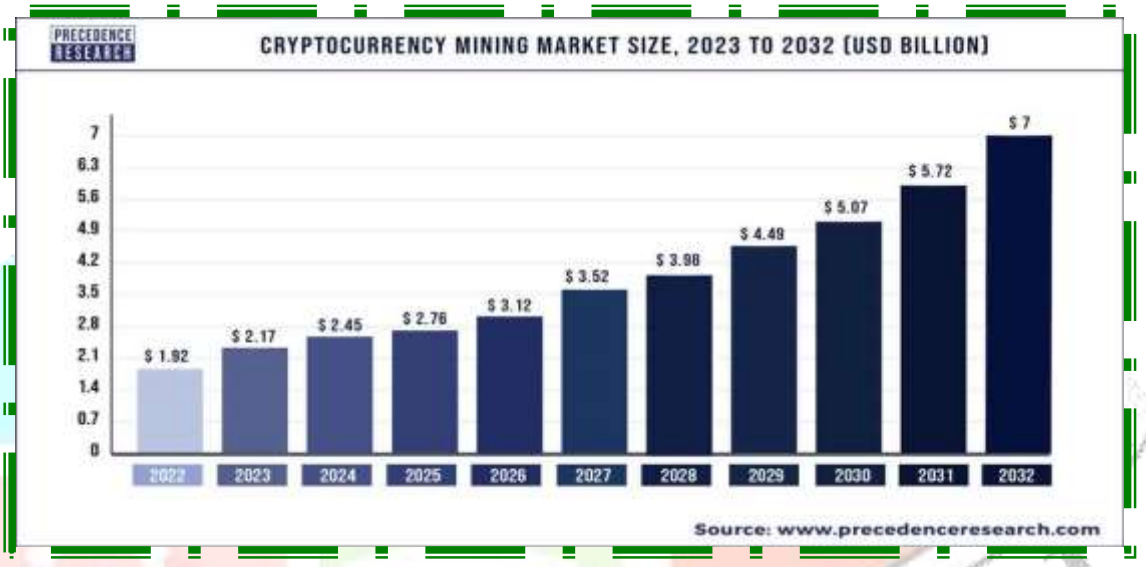
In each transaction, the previous owner signs with a secret signing key corresponding to his hash address of the transaction in which he received the bit coins and the address of the next owner. (Actually, transactions can have many input and output addresses, a fact that we exploit in our clustering heuristic in Section 4, but for simplicity we limit ourselves here to the case of a single input and output.)This signature (i.e., transaction) can then be added to the set of transactions that make up Bit coin; since each of these transactions refers to the previous transaction (ie, when sending bit coins, the current owner must indicate where they came from), the transactions form a chain. To verify the validity of a Bit coin, a user can check the validity of each of the signatures in this chain. To avoid double spending, it is necessary that every user

in the system knows about all such transactions. Double spending can then be identified when a user tries to transfer bit coin after having already done so. In order to determine which transaction came first, transactions are grouped into blocks that serve to time stamp the transactions they contain and guarantee their validity. Blocks build themselves into a chain, with each block referencing the previous one (thereby further reinforcing the validity of all previous transactions). This process provides a block chain which is then publicly available to every user on the system. This process describes how to transfer bit coins and broadcast transactions to all users of the system. Since Bit coin is decentralized and thus there is no central authority that mints Bit coins, we also need to consider how Bit coins are generated. In fact, this happens in the process of creating a block: each block received (ie, each block included in the chain of blocks) must be such that when all the data inside the block is hashed, the hash starts with a certain number of zeros. So that users can find it specific collection of data, blocks contain a nonce in addition to a list of transactions. (We simplify the description slightly for ease of presentation.) Once someone finds a nonce that allows a block to have a correctly formatted hash, the block is then broadcast in the same peer-to-peer fashion as a transaction. The system is designed to generate only 21 million bit coins in total. Finding a block is currently associated with an attached reward of 25 BTC; this rate was 50 BTC until November 28, 2012 (block height 210,000) and was expected to halve again in 2016 and finally drop to 0 in 2140".

4. Development of crypto currencies

Historically, cryptography has been used primarily by the military, secret services, and intelligence services to protect against the leakage of classified information. Most academics in the field believe that an autonomous digital currency that is not connected to any government or other intermediary such as a bank is attractive because of the anonymity and freedom it provides. Transferring money across domestic and international geographies can be done quickly and easily without worrying about government regulations. Horst Fietsel is considered the pioneer of cryptography in the US with his publication of the Digital Encryption Standard (DES) on March 17, 1975 in the Federal Register. Fitsel, then an IBM researcher working on a project codenamed Project Lucifer, filed a patent application for a 48-bit block cipher cryptographic system (also known as the Lucifer cipher). The project was commissioned by Lloyds Bank to encrypt ATM transactions. In 1972, the National Bureau of Standards (NBS) identified the need for an encryption standard to encrypt unclassified but sensitive government documents, and in May 1973 requested a proposal for such a system. The NBS then selected a modified version of the IBM algorithm with the approval of the National Security Agency (NSA). The project was commissioned by Lloyds Bank to encrypt ATM transactions. The original algorithm was strengthened to a 56-bit block cipher by a team led by Walter Tuchman and supported by Carl Meyer. The release of the DES has led to much discussion and debate in academia and civil society. Some academics, such as Martin Hellman and Whitfield Diffie of Stanford University, believed that the original 56-bit block cipher was changed by IBM at the behest of the NSA to provide the NSA with a backdoor into the cryptographic system (Subramanian and Chino).

At the time, questions were also raised about the security of the 56-bit cipher. However, DES became very popular and was soon adopted internationally as an encryption standard. Another development that contributed to the creation of crypto currencies is the so-called **Cypher punk** movement, which "formally" appeared in the early 1990s. The cipher punk movement is an activist movement whose participants seek to propose social and political change and disrupt the status quo by increasing security and privacy through the use of cryptographic techniques. The founders of the cipher punk group were Eric Hughes, a mathematician at UC Berkeley, Timothy C. May, a former chief scientist at Intel, and John Gilmore, one of the first employees (the fifth employee) at Sun Micro systems and the founder of Cygnus Support. such as the Electronic Frontier Foundation. All three were wealthy and shared a strong libertarian bent. The group began by meeting in 1992 in the Bay Area of San Francisco. They started a cipher punk mail



List in 1992 and within two years the mailing list had amassed over 600 subscribers. Another major contributor to the creation of crypto currency is David Chaum, a cryptologist who received his doctorate from the University of California Berkeley. As a PhD student in the 1980s, Chaum explored several concepts and developed several methods aimed at anonymous communication and anonymous financial transactions. In 1981, Chaum published the paper "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", which described a method using public key cryptography to hide the identity of the participant in an email communication as well as the content itself. He explained one of its uses in elections, where an examiner could verify that all votes had been counted correctly without revealing the identity of the voters. Chaum's huge contribution in this field is the creation of a digital currency based on cryptography, which he called E-Cash, and in 1990 he founded a company called DigiCash, an electronic money corporation. The world's first electronic cash payment took place on May 1, 1994. However, most attempts to create a functional crypto currency were not accepted by consumers until Bit coin was introduced in January 2009, when Satoshi Nakamoto, who is believed to be using the name as a pseudonym. He mined the first block of bit coins, known as the genesis block, and received a reward of 50 bit coins.

5. The Future of Crypto currencies - Advantages and Disadvantages

There are different and conflicting views on the future of crypto currencies in general and Bit coin in particular. While those with libertarian views on life are optimistic and accepting of the crypto currency system, other authors, economists and scholars in the field are not enthusiastic about the use of crypto currency in the payment and financial transaction system. An optimistic view of the use of crypto currencies is supported by the fact that they facilitate the transfer of funds between two parties in a transaction; these transactions are facilitated using public and private keys for security reasons.

These fund transfers are done with minimal processing fees, allowing users to avoid the high fees charged by most banks. Additionally, many countries have begun to accept Bit coin as a valid currency. Especially countries that are trying to get rid of cash have a very friendly attitude towards crypto currencies. Arguing that the proponents of the use of bit coin is Market cap of bit coin, ethereum and other crypto currencies, they argue that the crypto currency market has become very large and powerful, so banning it would be costly for any country.

Opponents of crypto currencies, on the other hand, argue that crypto currencies are highly volatile and can be used to launder money or finance illegal activities. In this respect, for example, Tymoigne (2015) is not enthusiastic about the use of crypto currencies and gives reasons why he believes that Bit coin is not a viable electronic currency. He notes that bit coins are illiquid and exhibit high price volatility, and that the discounted cash value of bit coin is zero. He further notes that the currency lacks a central issue and that there is no financial or economic basis for its creation. Ivaschenko provides the pros and cons of Bit coin as below.

Advantages

1. Open Source Crypto currency Mining – BTC uses the same algorithms used in online banking. The only difference in internet banking is the disclosure of user information. All information about the transaction in the BTC network is shared (how, when), but there is no data about the recipient or sender of the coins (there is no access to the personal information of the owner's wallet).

2. No Inflation - The maximum number of coins is strictly limited to 21 million bit coins. Since there are neither political forces nor corporations capable of changing this arrangement, there is no possibility of inflation developing in the system.

3. Peer-to-peer crypto currency network – in such networks there is no master server responsible for all operations. The exchange of information (in this case money) takes place between 2-3 or more software clients. All wallets installed by users are part of the Bit coin network. Each client stores a record of all transactions made and the number of bit coins in each wallet. Transactions are performed by hundreds of distributed servers. Neither banks, nor taxes, nor governments can control the exchange of money between themselves.

4. Unlimited transaction options – each of the wallet owners can pay anyone, anywhere and any amount. The transaction cannot be audited or prevented, so you can make transfers anywhere in the world, wherever another user with a Bit coin wallet is located.

5. No boundaries - Payments made in this system cannot be cancelled. Coins cannot be counterfeited, copied or spent twice. These capabilities guarantee the integrity of the entire system. Every month, the number of online stores, resources and companies that accept BTC is expanding.

6. Low operating cost of BTC - The BTC crypto currency works like physical cash and combines the functions of e-commerce. There is no need to pay commissions and fees to banks and other organizations. The main part of such a process is mathematics, which does not need money. The commission fee in this system is lower than in any other. It is 0.1% of the transaction amount. Operating interest goes to BTC miner's wallets.

7. Decentralization - There is no central control authority in the network, the network is distributed to all participants, and every computer mining bit coins is a member of this system. This means that the central authority has no power to dictate the rules for bit coin owners. And even if some part of the network goes offline, the payment system will continue to work stably.

8. Ease of use - Since the procedure for opening an account for a company in Ukrainian banks is too complicated and can be refused without explanation; using BTC is convenient for companies. The company needs approximately 5 minutes to create a BTC wallet and start using it immediately without any questions or commissions.

9**. Anonymity** - It is completely anonymous and at the same time fully transparent. Any company can create an infinite number of Bit coin addresses without reference to a name, address or any other information.

10. Transparency BTC - keeps a history of transactions that have ever taken place. This is called a sequential chain of blocks or block chain. The block chain stores information about everything. So if a company has publicly used a BTC address, then everyone can see how much BTC they own. If the company address is not publicly confirmed, then no one will ever know that they belong to that company. For complete anonymity, companies typically use a unique BTC address for each individual transaction.

11. Speed of Transaction - The ability to send money anywhere and to anyone within minutes of the BTC network processing the payment.

12. Belongs only to the owner of the wallet - There is a unique electronic payment system where the account belongs only to the owner. For example, on **PayPal,** if for any reason the company decides that the

owner is somehow using the account in an improper way, the system has the right to freeze all funds in the account without notifying the owner. Verification of correct account usage is the sole responsibility of the owner. With BTC, the owner has a private key and a corresponding public key, which is the address to the **BTC wallet.** No one but the owner can withdraw bit coins.

13. No chance of misuse of some personal data for fraud - This is an important point. Today, most purchases are made with credit cards. They are unreliable. When filling out forms on the website, customers are required to enter the following information: card number, expiration date and code. It's hard to think of a less secure payment method. Therefore, credit cards are very often stolen. BTC transactions do not require disclosure of any personal information. Instead, it uses two keys: public and private. The public one is available to everyone (i.e. BTC wallet address), but the private key is known only to the owner. A transaction must be signed by interacting with private keys and using a mathematical function. This creates proof that the transaction is done by the owner.

14. The possibility of investing funds in a transparent and profitable source

Disadvantages

According to the aforementioned author Ivaschenko (2016), the disadvantages are as follows:

1. Strong Volatility – Almost all the ups and downs in the value of BTC depend directly on the declared statements of the governments of various countries. This volatility creates a problem in the short term.

2. The big risks of investing in crypto currency, which should be considered in the medium and long term.

We believe that the list of disadvantages of crypto currency (bit coins) is much longer and related to the risk of money laundering, financing of terrorism and other illegal activities, lack of a central issue, which means that there is no legal formal person to guarantee in case of bankruptcy, etc. Although it is very difficult to predict, many academics and professionals on the subject say that the future of crypto currencies is bright, as they will remove trade barriers and middlemen, reduce transaction costs, and thus boost trade and the economy. . Still, we should consider and pessimistic voices in the academic world as which suggests that the high risk of volatility, hacking risks and lack of institutional backup make the future of crypto currencies not very optimistic.

6. Conclusions

The aim of the work was to provide an analysis of the use of crypto currencies in general and bit coin in particular. Our empirical research found that the future of crypto currencies could be bright if some institutional – formal conditions are met. Most academics recognize the benefits of using crypto currencies to facilitate trade, reduce costs, and the like. Bit coin and other crypto currencies have the potential to replace both traditional and new payment methods. However, to achieve this and become a dominant force in the global payment system, they need to provide significant added value, address and overcome a number of critical issues such as formal regulatory issues. This is unlikely to happen in the short term. However, banks should take a close look at the technology underlying these crypto currencies as a potential generic new way to transfer ownership of value in the long term.

7. References:

1. Bailis, P. & Song, H. (2017). Research for Practice: Crypto currencies, Block chains, and Smart Contracts; Hardware for Deep Learning. *Communications of the ACM*, 60(5), p. 48-51.
2. Bamford, J. (1982). The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization. Penguin.
3. Gandal, N. & Halaburda, H. (2016). Can we predict the winner in a market with network effects? Competition in crypto currency market. *Games*, 7(3), p. 1-21.
4. Ivaschenko, A.I. (2016). Using Crypto currency in the Activities of Ukrainian Small and Medium Enterprises in order to improve their Investment Attractiveness. *Problems of economy*, (3), p. 267-273.
5. Li, X. & Wang, C.A (2017). The technology and economic determinant of crypto currency exchange rates: The case of Bit coin. *Decision support system*, 95, p. 49-60.
6. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, Geoffrey, M. & Savage, S. (2016). A fistful of bit coins: Characterizing payments among men with no names. *Communications of the ACM*, 59(4), p. 86-93.
7. Subramanian, R. and Chino, T. (2016). The state of crypto currencies: Their issues and policy interactions. *Journal of International Technology & Information Management*, 24(3), p. 25-40.
8. Smalley, C. V. (2017). Crypto currency and taxes. *Tax adviser*, p. 1-3.
9. Tymoigne (2015). Do Crypto currencies Such as Bit coin have a Future? No: As a Currency, Bit coin violates All the Rules of Finance. *Wall street journal – Eastern edition*, 265(49), p. 1-2.

   Vora, G. (2015). Crypto currencies: Are Disruptive Financial Innovations Here? *Modern Economy*, 6(7), p. 816-832.