World Journal of Engineering Research and Technology

WJERT

www.wjert.org

Impact Factor Value: 5.924

CONCEPTUAL STUDY OF CRYPTOCURRENCIES

***Prof. Prashant Chougule and Dr. Dipti Tulpule**

Asst. Prof. – AMITY Pune.

Asst. Dean – AMITY Pune.

Article Received on 05/03/2021 **Article Revised on 26/03/2021** **Article Accepted on 16/04/2021**

***Corresponding Author**
Prof. Prashant Chougule
Asst. Prof. – AMITY Pune.

ABSTRACT

Cryptocurrencies were designed as an alternative to traditional fiat currencies. They utilise a disruptive new technology called as 'the blockchain' which dissolved the need to depend on a central authority for authentication of transactions. Today, there are more than 1600 different cryptocurrencies, but Bitcoin, the first cryptocurrency is still leading the pack in terms of number of transactions, popularity & market capitalization, followed closely, at least for now, by Ethereum. Investors, speculators, policy makers, businessmen and researchers are showing a rising interest in them due to their potential future applications. This paper attempts to provide an overview on the concept of cryptocurrencies. We will discuss aspects related to the origin, working & various aspects of economics & regulation of cryptocurrencies.

KEYWORDS: Cryptocurrency, Concept overview, Blockchain, Working, Applications, Economics, Regulation.

INTRODUCTION

In a recent interview with Cointelegraph.com, Hester Pierce, the commissioner of the U.S. Securities and Exchange Commission (S.E.C.), has accepted that an increased interest in cryptocurrencies, as noted recently, will motivate the S.E.C. to change its view on cryptocurrencies and change their rules & policies to become more including and accommodating towards the cryptocurrency scenario. (Reynolds, 2020).

On the other side of the world, China, the country which had previously banned cryptocurrencies and all related transactions, is now poised to emerge as a key player in the

cryptocurrency scenario due to its major share in '*hashing power'* (i.e. mining operations, due to cryptocurrency miners having access to very cheap hydroelectric power) and the news that Chinese government is in the process of developing its own sovereign digital currency, with its state backed research unit managing to file 130 cryptocurrency related patent applications as of September 2020. (Huillet, 2020).

With interest in cryptocurrencies heating up in 2 major superpowers in our world, it is only natural that business & academic attention should also follow suit. Since their inception in 2009, in the form of Bitcoin by a person or persons referred to by the pseudonym, Satoshi Nakamoto, Cryptocurrencies have risen in popularity and witnessed growing activity in price, trade volume, value and complexity, numbering over 1800 in 2018 (Frankel, 2018) (now just over 1600). They have been studied (and used) as a currency, a financial instrument, an investment vehicle, and also as a commodity. Investors, speculators, the media, academicians, policy makers & regulators are developing an interest in them (Corbet, Lucey, Urquhart, & Yarovaya, 2018).

Rising interest of academicians in the field of cryptocurrencies is somewhat limited to the bitcoin phenomenon alone. One finds a huge majority of academic literature dedicated to bitcoin while excluding around 1600 of its brethren to various degrees. This treatment is also due to the inherent volatility, speculative nature & highest market capitalization (ORĂȘTEAN, MĂRGINEAN, & SAVA, 2019), causing cryptocurrencies to be a not fully understood field of research (Sharma, Jain, Mahendru, Bansal, & Kumar, 2019). In financial & economic literature, Bitcoin has been explored for its potential as a currency, financial asset, commodity, investment & speculative vehicle (Kayal & Rohilla, 2019). Apart from low transaction costs & anonymity, another reason for immense popularity & interest in bitcoin, and thus cryptocurrencies in general, is because rules pertaining to them were created by engineers, who were free from the influence of lawyers, politicians & policymakers, thus claiming to be a people's currency (Böhme, Christin, Edelman, & Moore, 2015).

So, what are cryptocurrencies, then? One definition is as follows, *"Cryptocurrencies are peer-to-peer electronic cash systems which allow online payments to be sent directly from one party to another without going through a financial institution."* (Corbet, Lucey, Urquhart, & Yarovaya, 2018). It is a digital or electronic asset which may hold value or operate as an exchange medium & which is used in online transactions without needing a central server for transaction verification (Ben & Xiaoqiong, 2019). Due to their

characteristics as an exchange medium, they can be accessed via online currency exchanges facilitating conversion of fiat money into cryptocurrencies & vice versa. They are characterised by absence of a physical presence, lack of association with any central authority, infinite divisibility & high price volatility.

The main purpose of this paper is to collate, assimilate and present the views of researchers on cryptocurrencies with respect to the following aspects;

a. The fundamental concept of cryptocurrencies
b. Their working- mechanism & technology
c. The economic aspects of cryptocurrencies
d. The regulation related aspects of cryptocurrencies

The rest of the paper is structured as follows. The next section will introduce the methodology utilised for selection of the papers reviewed. This will be followed by an introduction to the fundamental concepts inherent in cryptocurrencies. The various economics and regulation related aspects will follow after that.

METHODOLOGY

EBSCO & SCOPUS indexed journals were accessed using various keywords as follows;

1. Cryptocurrency
2. Cryptocurrencies
3. Cryptocurr+Blockchain
4. Cryptocurr+Econom
5. Cryptocurr+Bank
6. Cryptocurr+regulation

The time period chosen for the current purpose was from 2010 to 2020 (December)

All the listed research papers were further filtered for peer reviewed journals related results only & then sorted in ascending order. Mendeley software was utilised here.

The research papers that were obtuse to our purposes were summarily rejected and finally, a list of _____ research papers, was selected for review.

Throughout the whole process, the endeavour was guided by the main purpose of collating the widespread information on cryptocurrencies with a view to make it accessible to the management executive.

Cryptocurrencies- The fundamentals

Need & Origins

Even though Bitcoin, announced by Satoshi Nakamoto in 2008, is touted as the first cryptocurrency, it is actually a much older concept, with work starting on it as early as the 1990s. Rapid development in internet & allied technologies had led to a rising demand for new forms of payment mechanisms which will better suit the online scenario. This was an area where the conventional fiat currencies were found sorely lacking.

In the white paper titled 'Bitcoin- A peer to peer electronic cash system', The author (Nakamoto, 2008) comes up with a variety of reasons why cryptocurrencies are needed. It is pointed out, right at the outset, that commerce on the internet has come to rely a lot on trusted third parties, which provide processing services for electronic payments. It was claimed that, this 'Trust Based Model', as it is called, suffers from inherent weaknesses, namely increase in transaction costs (due to mediation costs), limitation on fungibility, etc. Along with this, also ironically, the current 'trust based model' also necessitates that the merchants must regard their customers suspiciously and demand more information form them than otherwise necessary. It is also argued that, with traditional fiat currencies, the government is always in a position of control, armed with its ability to influence the monetary policy & regulate transaction types. This causes distress amongst stakeholders due to the inherent instability of traditional money, which, along with other inconveniences, can be avoided by using electronic currency.

So, the 'trust' in the system is suggested to be replaced by 'cryptographic proof of work'. This will aid willing transactors to conduct business without the need for any third party to perform the service of verifying the transaction. This would lead to reduction in unnecessary costs and protect sellers & buyers from fraud. The double spending problem- probably the only proverbial wrench in the works- was proposed to be solved via majority of 'honest nodes' pointing out mal-intentioned transactions in a 'peer to peer network' (Nakamoto, 2008).

Thus, due to Bitcoin, it was possible for value to be transferred between minimum two unknown and untrusting transactors without the need of any mediating 3rd party. (Catalini & Gans, 2019).

The Building Blocks- The Blockchain

In order for Bitcoin to become successful in what it endeavoured to do, it needed to be backed up by a system which could not only cheaply verify bitcoin transactions (which have already taken place), but which also incentivises such verification, so that a positive feedback loop is formed. It took an ingenious culmination of *cryptography* ("the art of writing or solving codes"- Online Oxford Dictionary) and *game theory* ("the branch of mathematics concerned with the analysis of strategies for dealing with competitive situations where the outcome of the participant's choice of actions depends critically on the actions of other participants." - Online Oxford Dictionary) to develop a freely distributed, public transaction ledger, called as the 'Blockchain'.

This is how the process works. Suppose a user wishes to make a payment and in the process of doing so, issues instructions to carry on the payment. These instructions are then relayed over the network of other such users. These other users will then use standard cryptographic techniques to verify that the transaction is valid, and that there is no 'double spending' or spending of same bitcoin more than once & the user issuing the payment instructions actually owns the cryptocurrency. Special users in the network, referred to as the miners, will collect the 'blocks' of transactions & then compete to verify them. This is done by solving complex & difficult mathematical problems which are easy to check. These miners will, in turn, receive two things, i.e. some predetermined amount of newly created cryptocurrency will be allocated to them and any other transaction charges voluntarily paid by the parties in question. These 'blocks' of transactions, after verification, will be added to a ledger, referred to as the 'blockchain'.

Using this Blockchain, any participant in the network could cheaply verify (and also settle) transactions in Bitcoin and get paid for doing it (in Bitcoin). This blockchain system is so designed that inbuilt incentives make it more profitable to participate and work honestly in the network rather than allow fraudulent transactions to pass. This ledger (the blockchain) imposes a cost for making amendments to it, with the intention to keep away parties with mal-intentions. This cost is in the form of computing power that miners must supply to solve those complex mathematical problems mentioned before.

Re-usable proof of work

The brain-child of cryptographic activist as well as computer scientist, Harold Thomas Finney II (also called as Hal Finney), Re-usable proof of work (or RPoW) was a system that worked by receiving a non-exchangeable (or a non-fungible) hashcash based proof-of-work token & in return provided an RSA signed token (a token represents an asset or a utility and constitutes a unit of value issued by an organization), which could then be used to transfer value from person to person. Based on Nick Szabo's theory of collectibles, it was intended to be the prototype for digital cash, a sort of precursor to bitcoin type of cryptocurrencies. (Nakamotoinstitute.org, 2004)

Mining

Mining, as a term, is popularly used with reference to Bitcoin, more than any other cryptocurrency. It is the key aspect which allows Bitcoin to function as a decentralised system. It refers to the process of contributing CPU power towards solution of random mathematical puzzles. By doing this, participants, who are now referred to as miners, get to participate in the day- to- day enforcement of the system's rules. Backed by that same CPU power, miners can also vote for or against any proposed changes to the protocols. (Vidan & Lehdonverta, 2018).

Miners with the most computing power will usually (if not every time) be the first ones to solve the previously mentioned complex cryptographic problems, thus, being the first to reap the rewards also. Previous transactions in the blockchain (already verified) will continue to be accepted as valid & true until no one user or pool of users manage to corner majority of the computing power in their hands.

Obviously, this computing power is not cheap, as it includes electricity charges, costly GPU computing boxes and also cost of cooling the computing devices. The system was built in such a way that it will be very costly & discouraging to try to acquire computing power in a bid to establish majority.

In 2013, It was observed that GHash.IO, the largest pool of miners at that time, came very close to acquiring 51% of the computing power required to mine bitcoin. This would have given this collective the unbridled power to determine which transactions will be verified and what the results will be. The GHash.IO collective tried to assure the bitcoin community that it didn't have any intentions of establishing its control over the network. The crisis was averted

when some of the members of this mining pool left to join the smaller pool, possibly to belay the community's suspicions about their motives, thus reducing this collective's share to 38% overnight. Despite these and similar such instances, the bitcoin community still stands by its trust on the robustness of the blockchain system. (Vidan & Lehdonverta, 2018)

How transactions work on Blockchain

Step 1- the Transaction

Minimum 2 parties are required, which will decide to transact with each other. They will decide to exchange some item of established & mutually accepted value for payment in cryptocurrency supported by blockchain. They will agree on the necessary terms & conditions & initiate the transaction.

Step 2- the Block

This above-mentioned transaction, and some more other pending transactions, will be bundled together in what will be referred to as a 'block'. This block will then be sent over to the participating computers in the Blockchain system's network. A block is basically a list of growing records/ transactions, something akin to a page in a ledger. Each block on the blockchain has the capacity to hold 1 megabyte (or approx. 2500 transactions) in itself.

Step 3- Verification

The participating computers (mentioned in step 2), who are also referred to as 'miners', will start evaluating the transactions. They use 'nodes' (which is any kind of device- Laptop, Computers or large servers) to do mining. The miners will use certain agreed-upon rules to determine the validity of these transactions via mathematical transactions. When minimum 51% of the participating computers (or 'nodes') verify the transaction as valid, thereby forming a 'consensus', the transaction stands verified. The miners will be remunerated for their efforts with cryptocurrency.

This is important to understand as you cannot have one (the blockchain) without the other (i.e. the compensation for maintaining the blockchain in the form of cryptocurrencies).

Step 4- Hash

A cryptographic hash is used to time-stamp the blocks verified in step 3. This is done in such a way that a connection (via a 'reference') to a previous block's hash is also included in every new block. This, essentially, leads to the formation of a continuous chain of records that defy

falsification, unless, participating computers can be convinced otherwise. This is believed to be impossible.

Step 5- Execution

The cryptocurrency of appropriate value moves from the account of one party to the other party and transaction is completed.

In short, first, a transaction is requested by the parties involved, then the transaction is shared amongst the participating computers (i.e. miners) in the network, who will the verify the same using mathematical methods. Once verified, the transaction is bundled with others to form a block. This block is then added (via use of a Hash) to a chain of previously verified blocks. Once it is added to the continuous ledger, it is impossible to alter.

Also important to note is that cryptocurrencies are recorded as transactions, meaning that a user does not hold any bitcoins (for eg.) but actually participates in publicly verifiable transactions that show receipt of those bitcoins from another user, who in turn participated in another set of publicly verifiable transactions resulting in the receipt of those bitcoins. In the absence of any transactions leading to spending of those bitcoins, a user (who has previously received those bitcoins) will be deemed to be their possessor. Also, each bitcoin can be easily tracked (by anyone & everyone) through all the transactions in which it was involved right up to the primary transaction. Finally, in order to ensure that fake or unauthorised transactions are not included in the block, provision is made to compare every new block to the most recent published block, allowing to verify that a transaction has, in fact, occurred & there is no double spending of that cryptocurrency (Böhme, Christin, Edelman, & Moore, 2015).

The economic aspects of Cryptocurrencies

The rules for the first cryptocurrency, Bitcoin, were designed & established by engineers, rather than bankers, economists, lawyers or regulators. Even so, cryptocurrencies cannot escape the need to make economic sense. Also, such cryptocurrencies, even in their nascent early stages, are of great interest to economists due to their ability to yield insights about buyer behaviour, seller behaviour, demand- supply interface in the markets, etc (Böhme, Christin, Edelman, & Moore, 2015).

Böhme, Christin, Edelman & Moore (2015), while explaining the basic design principles of Bitcoin (the premier cryptocurrency), point out the importance of scarcity in protecting the

currency in question from counterfeiting & ensuring its price stability, which in a fiat currency system is preserved & ensured by legally accepted book keeping methods & a central authority for issuing such currency. In the cryptocurrency scenario, as there is no central authority to issue the cryptocurrency (as per its requirements or as per government policies) & to track its use & holding, the scarcity of cryptocurrencies (i.e. the supply side of the equation) is provided for in an absolute manner. No new cryptocurrency units can be created until they are mined & verified via a process which is more difficult than traditional book-keeping. Further, there is also a limit on the maximum number of a cryptocurrency that can be produced & sent into circulation (although, some cryptocurrencies, eg. Primecoin or Peercoin, view it as a limitation & have provided for an unlimited money supply possibility).

Finally, the incentives for mining these cryptocurrencies are also designed in a way so as to ensure that cryptocurrencies are mined at a controlled pace.

Also, in the macro- economic sense, Böhme, Christin, Edelman & Moore (2015) observed that the bitcoin economy acts as a variant of Milton Friedman's (1960, p. 90) "k percent rule". This rule proposes fixing of the annual growth rate of the currency supply to a fixed growth rate. At some point, it is inevitable that 'k' will become equal to 'Zero', after the last bitcoin (or any other cryptocurrency subscribing to similar limited supply norms, as bitcoin) has been mined.

This also raises the question about what will happen to the money supply of a cryptocurrency when some of these cryptocurrency units will be lost forever after users forget their private keys or lose access to their wallets due to any reason. Another question raised is about possible ramifications of a situation where the growth of an economy using the cryptocurrencies will outpace the supply of the cryptocurrency. It is expected that such a situation will likely lead to deflation in the economy, bringing into question the logic behind ensuring that the supply of cryptocurrencies is limited.

Böhme, Christin, Edelman & Moore (2015) noted that bitcoin's blockchain uses a crude measure of monetary indicators & leaves a lot of room for improvement in establishing a system of Automatic Monetary Policy system which will be based on more than just nominal data.

For the first time, it became possible to transfer value between two parties who had never seen each other & known each other due to bitcoin. For the first time, 'trust' as we know it, was under threat of ceasing to be neither the precursor, nor the necessary condition for a transaction. Needless to say, the witnesses to the travails of the 2008 U.S. Financial systems collapse hailed this as a welcome event. To make this even more attractive to the now sceptical lot, the cryptocurrencies & its ancillary technologies were expected to do this at a very low cost. As the central 'trusted' authority (eg. Bank) was no longer required, there was no need to pay its various costs & charges, hidden or otherwise. However, researchers have identified 2 costs associated with cryptocurrencies that require our consideration, viz. Cost of verification & cost of networking. (Catalini & Gans, 2019).

The cost of verification is connected with the ability to cheaply verify state, including information about previous transactions and their ancillary attributes, along with the details about the ownership in the tokenised asset or digital asset. (Catalini & Gans, 2019).

The cost of networking is connected with the ability to arrange the way of doing things in such a way that there is no need to involve any centralised intermediary. (Catalini & Gans, 2019).

One can achieve the minimisation of both the above costs by combining the ability to cheaply verify state, on one hand, and designing the economic incentives structure so as to ensure that the resultant digital marketplace allows participants to make joint investments in shared infrastructure & digital public utilities without assigning any prominent role to any actor involved. (Catalini & Gans, 2019).

It was also observed that the above-mentioned digital market places will be characterised by increased competition, lower barriers to entry and lower privacy risk, all the while, exhibiting new inefficiencies & governance challenges.

The Regulation related aspects of Cryptocurrencies

Most of the laws and regulations related to financial aspects, as developed by policymakers worldwide, have been invented & institutionalised before the advent of cryptocurrencies. Even those laws & regulations which were created post 2008 U.S. Financial crises were created with the firm belief that banks & other 'trusted' intermediaries will continue to remain & function as the lynchpins of the financial systems world wide. Needless to say, with

cryptocurrencies occupying more & more space in our economic lives, the shadow of redundancy over these contemporary laws & regulatory devices is only growing darker. In the past, one way to dispel these shadows was to ban cryptocurrencies altogether, however, it is an option which is no longer considered as effective in the coming times. The simple reason for this is that one cannot hope to enjoy the various applications of blockchain technology (in banking, microfinance, HRM, regtech, wealthtech, etc.) without accepting the existence of cryptocurrencies as a means to compensate or 'incentivise' the 'miners' for 'mining' the 'blocks' & maintaining the integrity of the 'blockchain' (Vidan & Lehdonverta, 2018).

So what are these risks that are foreshadowing a legal & regulatory crisis for policy makers in the future? They are mentioned as follows;

a. Money Laundering

Terrorists & criminals are very shy when it comes to using the financial system for holding their ill-gotten fortunes. Until now, they were known to employ elaborate networks of 'hawala' & 'money laundering' networks to systematically legitimise their money in order to render it usable. Any events causing the creation of records or paper trails of transactions that could lead the authorities to the door steps of the terrorists & criminals, is actively avoided & shunned. Until now, 'Cash', with its inherent anonymity and lack of records, was favored by terrorists & criminals to keep the authorities at bay. (Richard Wright et al., 2014).

That Bitcoin was used as the currency of choice to both, receive compensation for illegal activities, and to operate the dark net based illegal drug & other contraband trading marketplace called as the 'Silk Road' from January 2011 to October 2013, did not help to allay the fears & scepticism of policy makers & regulators that cryptocurrencies will become effective tools in the hands of nefarious elements for the purpose of evading law enforcement. (Stroukal & Nedvedova, 2016).

However, we must remember that it is also possible to regulate cryptocurrencies, their exchanges and other parties involved. For eg, due to its nature, every transaction that ever took place using a unit of cryptocurrency can be easily verified & also connected to a specific cryptocurrency exchange user (via the cryptocurrency public key) (Stein, 2017).

The government has set up various initiatives to pull up exchanges and make them provide information about any suspicious activities. An example of the same would be The U.S. Department of Treasury' s Financial Crimes Enforcement Network (or FinCEN) (Moffit, 2018) or the 6 major legislations passed by the U.S. government in its 116th Congress in 2019.

b. Tax Evasion

The pseudonymous & de-centralised nature of cryptocurrencies also make them attractive for use in tax evasion. (Voreacos, 2018) Initially, due to the novel nature of cryptocurrencies, the tax authorities did find it difficult to assess the tax liabilities of these crypto account holders, but they have since then updated their understanding and various tools available to them at their disposal. (Voreacos, 2018) In a connected instance, The U.S. I.R.S. has also accepted that not all cryptocurrency holders have the intent of tax evasion, as many cryptocurrency holders were simply unaware of the tax liability arising out of their crypto-asset returns. (Borek & Sullivan Jr., 2019).

c. Consumer Protection

Currently, there is an absence of any all-encompassing regulatory framework of any kind that is specifically aimed at protecting consumers enjoying the services of cryptocurrency exchanges specifically. The situation is compounded when it is observed that consumers are especially susceptible to being deceived or misinformed when dealing with cryptocurrencies, a relatively new type of asset for new consumers. (Office of the New York Attorney General, 2018) However, the matter is sought to be resolved by classifying these crypto-exchanges as 'Financial Services Providers' or even something akin to 'stock exchanges' and then extend the existing regulatory framework to them. However, both, the effectiveness of the efforts & efficiency of the results, are subject to debate as of now.

These concerns are but the tip of the iceberg when it comes to studying various concerns as raised by wide-spread adoption of cryptocurrencies. This is the scope for future research.

CONCLUSION

Cryptocurrency adoption and use is no longer a question we can deflect towards the future. Due to the rapid advances in technology & the resultant disruptions caused by it, one may argue that the future is now here to stay.

Due to its novel, mysterious & exotic nature, cryptocurrencies are very easy to misunderstand or to dismiss as too technical for us. The truth is actually far less exotic. These cryptocurrencies exist due to the need to incentivise the blockchain. They have value, which may or may not be be very volatile in nature. Due to the attractive uses & cost reduction potential of blockchain technology, presence of cryptocurrencies cannot be denied for ever.

More and more economies are now adopting the blockchain & its resultant cryptocurrencies. Small countries like Mauritius are now refering to themselves as 'Ethereum Island'. Both China & U.S.A. are actively working on initiatives to integrate cryptocurrencies in their economic lives. Under these circumstances, business executives too, must strive to become comfortable with harnessing of cryptocurrencies in their daily lives. The current work is an honest effort in that direction.

REFERENCES

1. al, R. W. (March). Less Cash, Less Crime: Evidence from the electronic benifit transfer program. *National Bureau of Economic Research*(Working Paper 19996), 1-5. Retrieved from http://www.nber.org/papers/w19996.pdf, 2014.
2. Ben, S., & Xiaoqiong, W. Are Cryptocurrencies good investments? *Studies in Business & Economics,* 2019; *14*(2): 181-192.
3. Böhme, R., Christin, N., Edelman, B., & Moore, T. Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives,* 2015; *29*(2): 213-238. doi:10.1257/jep.29.2.213.
4. Borek, C., & Sullivan Jr., A. (August 5). IRS warns over 10000 virtual currency traders to comply with U.S. Tax Obligations. *JD Supra*. Retrieved from https://www.jdsupra.com/legalnews/irs-warns-over-10-000-virtual-currency-74247/, 2019.
5. Catalini, C., & Gans, J. Some Simple Economics of the Blockchain. *SSRN Working Paper no. 2874598*. Retrieved from https://papers.ssrn.com /sol3/papers.cfm?abstract.id =2874598, 2019.
6. Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (March 18). Cryptocurrencies as a Financial Asset: A systematic analysis. doi:http://dx.doi.org/10.2139/ssrn.3143122, 2018.
7. Frankel, M. (March 16). *Investing*. Retrieved from www.fool.com: https://www.fool.com/investing/2018/03/16/how-many-cryptocurrencies-are-there.aspx, 2018.

8. Huillet, M. (September 21). *Beijing sees digital currencies as 'new battlefield' in global finance*. Retrieved from Cointelegraph: https://cointelegraph.com/news/beijing-sees-digital-currencies-as-new-battlefield-in-global-finance, 2020.
9. Kayal, P., & Rohilla, P. (August). *Bitcoin in literature of Economics & Finance: a Survey*. doi:http://dx.doi.org/10.2139/ssrn.3441652, 2019.
10. Moffit, J. (July 27). The Fifty US States and Cryptocurrency Regulations. *Coin ATM Radar*. Retrieved from https://coinatmradar.com/blog/the-fifty-u-s-states-and-cryptocurrency-regulations/, 2018.
11. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *www.bitcoin.org*, 2008.
12. Nakamotoinstitute.org. *RPOW-REUSABLE PROOF OF WORK*. Retrieved from https://nakamotoinstitute.org/, 2004.
13. https://nakamotoinstitute.org/finney/rpow/#:~:text=Reusable%20Proof%2Dof%2DWork%20(,was%20a%20precursor%20to%20Bitcoin.
14. Office of the New York Attorney General. *Virtual Markets Integrity Initiative Report.* New York: Office of the New York Attorney General. Retrieved from https://ag.ny.gov/sites/default/files/vmii_report.pdf, 2018.
15. ORĂȘTEAN, R., MĂRGINEAN, S. C., & SAVA, R. BITCOIN IN THE SCIENTIFIC LITERATURE – A BIBLIOMETRIC STUDY. *Studies in Business and Economics,* 2019; *14*(3): 160-174. doi:10.2478/sbe-2019-0051.
16. Reynolds, K. (October 11). *Latest news*. Retrieved from Coindesk: https://www.coindesk.com/sec-will-be-forced-to-give-more-guidance-about-crypto-peirce
17. Richard Wright et al. (2014). Less Cash, Less Crime: Evidence from the Electronic Benefit Transfer Program. *National Bureau of Economic Research*, 2020; 1-5.
18. Sharma, G., Jain, M., Mahendru, M., Bansal, S., & Kumar, G. (March). Emergence of Bitcoin as an investment alternative: a systematic review & research agenda. *International Journal of Business & Information,* 2019; *14*(1): 47-84. doi:10.6702/ijbi.201903_14(1).0003.
19. Stein, S. (June 22). Law Enforcement Adapts to Using Cryptocurrency to Catch Criminals. *Bloomberg BNA*. Retrieved from https://www.bna.com/law-enforcement-adapts-n73014460761/, 2017.
20. Stroukal, D., & Nedvedova, B. Bitcoin and Other Currency as an Instrument of Crime in Cyberspace. *Fourth Business & Management Conference* (pp. 219-225). Istanbul: International Institute of Social & Economic Sciences, 2016.

21. Vidan, G., & Lehdonverta, V. Mine the gap: Bitcoin and the maintenance of trustlessness. *New Media & Society*, 2018; 42-59.
22. Voreacos, D. (February 08). IRS cops are scouring crypto accounts to build tax evasion cases. *Bloomberg*. Retrieved from https://www.bloomberg.com/news /articles/2018-02-08/irs-cops-scouring-crypto-accounts-to-build-tax-evasion-cases, 2018.