

Technical and Legal Characteristics of Cryptocurrencies and Related Legal Risks

*Dr. Mohammad Alhihi**

Abstract

This paper explores through critical appraisal the technical and legal characteristics of cryptocurrencies as innovative development in financial market. The paper aims highlights the technical way of producing these currencies, clarifies their legal status, explains the differences between normal e-payment tools and cryptocurrencies transactions, and clarifies the main factors which determine the values of these currencies. Furthermore, the paper discusses the main legal risks associated with cryptocurrencies. The main outcome of this paper is the conclusion that cryptocurrencies have become a real legal challenge for states collectively and individually to develop appropriate legal frameworks to deal with different forms of economic and risk associated with virtual currency.

Key words: cryptocurrency, bitcoin, virtual currency, blockchain, digital money.

* Associate Professor of Commercial Law, KIL AW.

Introduction

The internet has become a part of our daily life, especially our financial, commercial, and social activities as reliable tool of communication. The eager of the experts in computer and internet technologies to develop new ways and technical application that can be used and attract more users is beyond our imagination. Due to the massive use of modern information technology in e-commerce, a new form of technical invention emerged in 2009, namely the development of a new type of virtual currency known as cryptocurrency.⁽¹⁾ This currency is a digital form of units and can be transferred between digital addresses.⁽²⁾ The first kind of such currency was called Bitcoin, which was invented by Satoshi Nakamoto.⁽³⁾ By now, there are more than 1000 invented virtual currencies, such as Litecoin (LTC), Ethereum (ETH), Ripple (XRP), and Dash.⁽⁴⁾

The main idea behind the innovation of cryptocurrencies is to create a decentralized payment system that trade parties can use without the need for a third party to facilitate electronic payments.⁽⁵⁾

Cryptocurrency is a special form of electronic program where the currency is generated as ledger of record and its owner has an account with a special secret encryption. This currency is based on encryption techniques to regulate the generation of its units and verify the transfer of funds. Furthermore, to this date this new currency has no central issuing or regulating authority but instead uses a decentralized system to record all related transactions, which relies on cryptography to prevent counterfeiting and fraudulent transactions. Accordingly, virtual currency does not mean the use of modern telecommunication tools of transferring credit and settling payment obligations between different parties, where a third party works as a moderator to facilitate the process.

(1) Sorbetov, Y., «Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero» *Journal of Economics and Financial Analysis* (2018) 2: (2), www.ojs.tripaledu.com/jefa 1-27.4/3/2019, p. 2.

(2) LOW, K. F. K. and TEO, E., «Legal Risks of Owning Cryptocurrencies,» (Institutional Knowledge at Singapore Management University, 2017) p. 2.

(3) Satoshi Nakamoto is inventor of the first Bitcoin in 2008 based on the idea of proof of work.

(4) Corbeta, S., Luceyb, B., Urquhart, A., and Yarovaya, L., «Cryptocurrencies as a Financial Asset: A Systematic Analysis,» (2018) p. 3.

(5) Sovbetov, Y., «Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero» *Journal of Economics and Financial Analysis* (2018) 2: (2), www.ojs.tripaledu.com/jefa 1-27.4/3/2019, p. 2.

The aim of this paper is to discuss the legal risks associated with the cryptocurrency for related transactions parties, regulators, and criminal legal risk. Essentially, different risks stem from the special characteristics of this innovative type of currency and ways of generating its units. This new form of money does not have a physical existence to be held or transferred physically between trading parties. The other risk stems from the decentralized technology that is being used in generating its units, transferring its ownership, and controlling its related deals, without interference or supervision of any neutral or official party to control such sophisticated operations. Another major risk is related to the burden of proof of the ownership in case of cyber-attack or system failure. In addition, there are other issues and questions which need to be explained and answered. One is whether it is possible to develop a banking system and a set of laws to regulate the opening of accounts for cryptocurrency; and the other is establishing how to decide the value of each unit of cryptocurrency in order to be used as alternative for traditional money. The following sections will attempt to answer the above highlighted points and questions.

1. Technical Background of Cryptocurrencies

In order understand the legal aspect of cryptocurrencies, it very important to identify their technical characteristics. Cryptocurrencies are not physical products, but they represent a form of innovative cryptographic computer programming records of proofs for transactions. Cryptocurrencies usually achieve a unique combination of three features: ensuring anonymity, independence from central authority and double spending attack protection.⁽⁶⁾

The most sophisticated programming system used to generate and control the transfer of such currency is called Blockchain technology. Blockchain is a form of distributed ledger to exchange information and transact digital asset in distributed networks.⁽⁷⁾ This technology works on the basis of a decentralized solution of data management, which does not require any third party to interfere. In other words, the system itself controls all operations of producing the currency units and related transactions are conducted on basis of peer-to-

(6) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019, p.19.

(7) Sari, A. and Kilic, S., «Exploiting Cryptocurrency Miners with Osint Techniques,» in *Transactions on Networks and Communications*, (2017). P62.

peer without the existence of a clearinghouse⁽⁸⁾

Blockchain technology allows its users to create types of very sophisticated cryptographic programs that can work as a chain of electronic blocks of data management without the interference or control of a third party. To put it simply, Blockchain users have secret keys that allow them to register their deals and transactions which are related to the created blocks without the need for any authority's permission.

Cryptocurrency as a product of Blockchain technology is a form of advanced new mediums of exchange for financial transactions without the interference of banks or any other financial institution. The core point for the new development of Blockchain is the creation of electronic blocks that are: permanent, cannot be deleted or altered, and its ownership title can be transferred between users using cryptography keys. The stability and high cost associated with the development of blocks have made it something valuable that can be owned in the form of electronic property, which consequently has led to it being finally classified as an electronic currency.⁽⁹⁾ Essentially, the original motivation behind Bitcoin was to develop a cash-like payment system that permitted electronic transactions.⁽¹⁰⁾ Then these blocks which are usually controlled by its developers started being used and accepted among the members of a specific virtual community.⁽¹¹⁾

The other advantage of using Blockchain technology in developing cryptocurrencies is that the technology works as a log file information record about each transaction and its related balance of all blocks. Basically, this works through broadcasting the information and transactions to all participants of the system of each type of Cryptocurrency.⁽¹²⁾ These stable and unchangeable records, which can be seen by all users increased the trust in the stability of cryptocurrencies and contributed to its usage as an alternative to traditional

(8) Vyas, C. A. and Lunagaria, M., «Security Concerns and Issues for Bitcoin» *International Journal of Computer Applications* (2014): <<https://pdfs.semanticscholar.org/4751/e99514948c2cbef0f6e4a12e65c72f75aea8.pdf>> 9/4/2019, p.10.

(9) Srokosz, W. and Kopyciaski, T., «Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability» *Journal of Teaching and Education* (2015) 4: (2), <www.universitypublications.net/jte/0402/pdf/F5N180.pdf> 619–27, p. 619.

(10) Berentsen, A. and Schär, F., «A Short Introduction to the World of Cryptocurrencies,» (2018) p.15.

(11) Brenig, C., Accorsi, R., and Müller, G., «Economic Analysis of Cryptocurrency Backed Money Laundering,» (*Association for Information Systems*: , 2015) p .7.

(12) *Ibid*, p. 7.

currency. Another advantage for the use of Blockchain technology in developing cryptocurrencies is that the technology provides an infrastructure that enables numerous applications -with very secured record through strong cryptography- to conduct smart contracts and make payment using cryptocurrencies.⁽¹³⁾

The success of the use of Cryptocurrency can be seen by looking at Bitcoin. As an example of Cryptocurrency, it is considered as the first leading form of new nonphysical currency and is the first open source software-based online payment system which emerged in 2008.⁽¹⁴⁾

2. The Differences between Cryptocurrencies and Tools of Normal Electronic Payment Systems

It is important to clarify the difference between Cryptocurrency and the tools which are used to facilitate electronic payment. Essentially, communication technology has often been used in different ways in the financial sector to facilitate payment obligations between trade parties. The terms digital currency or digital cash is used to express the meaning of using modern technology as applications and tools of credit transfer and settling financial obligations between parties. One important point to keep in mind is that, these operations usually need to be facilitated and supervised by third parties such as bank or any other financial institution.⁽¹⁵⁾ For example, digital cash is a payment system with predetermined value which can be circulated freely as electronic files.⁽¹⁶⁾ Furthermore, a centralized payment system can at times be developed under the control of a certain agent such as a bank to solve the problem of double spending.⁽¹⁷⁾ The similarity between digital cash or electronic money from one side and cryptocurrencies from the other is that the operation can be conducted without the involvement of banks.⁽¹⁸⁾

In the above mentioned systems and in other applications of modern technology for electronic payment, all operations are based on traditional money, where

(13) Berentsen, A. and Schär, F., «A Short Introduction to the World of Cryptocurrencies,» (2018). p 15.

(14) Hayes, A. S., «Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin» (2016): <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2648366> P.2.

(15) Daradkeh, L., «The Challenges of Law Keep Pace with the Technological Developments in Banking and Finance» *kuwait International Law journal* (2018): (3 par 1), 325-61, p .333.

(16) Berentsen, A. and Schär, F., «A Short Introduction to the World of Cryptocurrencies,» (2018) p. 2.

(17) *Ibid*, p .2.

(18) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019, p.19.

after a certain time the actual credit has to be transferred physically from the debited side after the settlement of the mutual transaction. Consequently, Cryptocurrency is not the alternative term for digital currency. This is because Cryptocurrency is a new evolutionary form of digital currency with its own value that can be used as an alternative for traditional money for settling financial obligations and payments. Due to the some similarities of digital money and cryptocurrencies of using modern information technologies in both currencies, it has been said by some scholars that cryptocurrencies are advanced form of digital money.⁽¹⁹⁾ To stay within the scope and aim of this paper, electronic transactions and different electronic payments methods are not going to be a major part of our discussion.

3. Comparison between Cryptocurrencies and Normal Money

Money went through many stages of development from the era of barter to commodity money, metal and coins, to gold and silver, continuing by modern monetary systems and checks and ending with the innovation of cryptocurrencies. Overall, money has three main functions, which include being a medium of exchange, a store of value, and a unit of accounting. Money is a medium of exchange where people accept it in making transactions and deals. As a unit of accounting, money provides a simple device for identifying and communicating value. Money serves as a store of value in that it allows us to store the rewards of our labour or business.⁽²⁰⁾

In order for money to fulfil its functions a value has to be decided for each unit and gold has been the most universally used commodity to decide the value of money. The aim of the discussion in this part is to understand the actual nature of cryptocurrencies, i.e. whether they are money or assets and understand how their values are decided.

A. Advantages and legal status of cryptocurrencies

an asset or currency

The advantages of cryptocurrencies are highlighted by their defendants. They emphasize the positive aspects of cryptocurrencies and argue that this form of currency helps in making fund transfer faster, transfer fees lower, and that its

(19) Daradkeh, L., «The Challenges of Law Keep Pace with the Technological Developments in Banking and Finance» *kuwait International Law journal* (2018): (3 par 1), 325-61, p.333.

(20) Bunjaku, F., Gjorgjeva-Trajkovska, O., and Miteva-Kacarski, E., «Cryptocurrencies – Advantages and Disadvantages» *Journal of Economics* (2017) 2: (1), <<http://js.ugd.edu.mk/index.php/JE/index>> p.32.

use in financial transactions is either already accepted or not opposed by many countries.⁽²¹⁾ Moreover, some advocate the use of the innovated currency for its advantage in certain circumstances of foreign payment for countries with unstable currencies.⁽²²⁾ Cryptocurrencies are considered by their advocates as an evolution of cashless medium of exchange that can potentially change the world of finance.⁽²³⁾

For the legal status, scholars are yet to agree on a specific definition for cryptocurrencies. This is because virtual currency appears as currency when it is used as money in a digital form, but it also appears as property or an asset which is something with self value like anything we may own.⁽²⁴⁾ It is easy to see the problem when one looks at the definition of an asset. Generally speaking, an asset or a commodity can be defined as something with the following features: firstly, it has a physical or nonphysical form; secondly, it has a value and thirdly, a person or an entity can own it, benefit from it, or it to generate income. Therefore, an asset is basically defined, as something that can be acquired or purchased, and that has monetary value.⁽²⁵⁾ Cryptocurrencies are not considered money because they are not issued by official authorities; their value has less stability than normal money, and there is no obligation for any one to accept them as money.⁽²⁶⁾

Some scholars believe that virtual and standard currencies are alike and alternative to each other. They justify their stand by explaining that cryptocurrencies can be exchanged between peers like any normal money through e-contract.⁽²⁷⁾ Also, they argue that nowadays most of the money is in electronic form and only a small part is still in cash.⁽²⁸⁾ It has been pointed out that de-physicalization of money is real and acceptable by individuals and states. For example, it has been estimated in 2011 that traditional money in

(21) Ibid, : p36.

(22) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>. 4/4/2019, p26.

(23) Corbeta, S., Luceyb, B., Urquhart, A., and Yarovaya, L., «Cryptocurrencies as a Financial Asset: A Systematic Analysis,» (2018). p 4.

(24) Cvetkova, I., «Cryptocurrencies Legal Regulation» *BRICS LAW JOURNAL* (2018) V: (2), 128, p 128.

(25) Read more: <http://www.businessdictionary.com/definition/asset.html>

(26) Cvetkova, I., «Cryptocurrencies Legal Regulation» *BRICS LAW JOURNAL* (2018) V: (2), 128, p133.

(27) Ibid, p .130.

(28) Ibid, p .133.

British economy amounted to only about 3.6%.⁽²⁹⁾

It can be argued however, that there are many major differences between virtual and standard currencies. Firstly, standard currencies in electronic form can be converted into cash without any difficulties. On the other hand virtual currencies are permanent electronic blocks which are not easy to convert into cash, or delete. Secondly, we can sell virtual currencies and they appear in this case as assets, therefore Bitcoin was considered by some institutions as a commodity.⁽³⁰⁾ However, we cannot do the same with standard electronic currencies. Having said that, it must be kept in mind that virtual currencies do at times work as money, because they are capable of fulfilling the main three functions of money which are: a medium of exchange, a store of value, and as a unit of account. Overall, it can be said that virtual currencies work as assets and currencies at the same time. Essentially, it all depends on how we look at or use them.

B. Mining cryptocurrencies

Unlike normal money which must be issued and controlled by state authority, the production of virtual currencies follows a different approach because of its nature as a cryptographic computer ledger. Cryptocurrencies are basically a compound of electronic chains of blocks interrelated to each other, and connected through Blockchain technology through the use of powerful computers with advanced hardware and software. The system capable to develop virtual currencies is called Mining. Computers build a ledger of electronic blocks with high level of cryptography and connect them with similar blocks built by other computers. In other words, any kind of cryptocurrency is not a product of a single computer, but rather a joint production of many computers working as one ledger worldwide.⁽³¹⁾ For miners to proof their work they have to conduct a lot of trial and error with low level of success. When the proof of mining work reaches a certain stage of data pattern, then the Blockchain network verifies if the new work fits with the currency chain from the original block till the last block in the chain. Each developed block of any given cryptocurrency is a proof and record of the Mining work in form of data and connected with other developed blocks by other computers that

(29) LOW, K. F. K. and TEO, E., «Legal Risks of Owning Cryptocurrencies,» (Institutional Knowledge at Singapore Management University, 2017). p.5

(30) Daradkeh, L., «The Challenges of Law Keep Pace with the Technological Developments in Banking and Finance» Kuwait International Law School Journal, (2018): (3 par 1), 325-61, p.337.

(31) Breu, S. U. and Seitz, T. G., «Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society,» (2018) p .5.

share the same chain. The system for each cryptocurrency through Blockchain controls the speed of collecting the data for a new mining process, the overall production of valid block has to be one block every 10 mints from all miners around the world.⁽³²⁾

The permanent characteristic of cryptocurrencies stems from the technical aspect that produces cryptographic blocks as one ledger shared by many computers worldwide. This means any amendment for any block in the ledger will lead to similar amendment to all other blocks and can be seen by all involved parties.⁽³³⁾ For example, in Bitcoin, each subsequent block is linked to the previous one and cannot be separated and in the case of any attempt to generate an invalid block, the other network members will not confirm it, because the hash of the previous block will not be used in it. To change the hash of a previous block to accept a new block with a different hash, there needs to be a change to the hash of all blocks going as far back as the original block which was created by Satoshi Nakamoto himself, which is essentially impossible. Furthermore, there are numerous cryptographic protection mechanisms to maintain the security and the stability of the whole chain of blocks for this virtual currency.⁽³⁴⁾

C. The value of cryptocurrencies

There are major differences between normal money and cryptocurrency in relation to the factors that determine their market values. In relation to normal money, there are a number of facts that need to be mentioned. Firstly, it is issued and controlled by certain authorities in each state. Secondly, most countries today operate in a fiat currency system, where central banks and monetary reserves control the supply of money to control inflation and the value of the currency.

Thirdly, metallic coins have been historically the earliest form of money still in use today before the paper money.⁽³⁵⁾ the standard weight and

(32) Vyas, C. A. and Lunagaria, M., «Security Concerns and Issues for Bitcoin» *International Journal of Computer Applications* (2014): <<https://pdfs.semanticscholar.org/4751/e99514948c2cbef0f6e4a12e65c72f75aea8.pdf>> 9/4/2019, p.10.

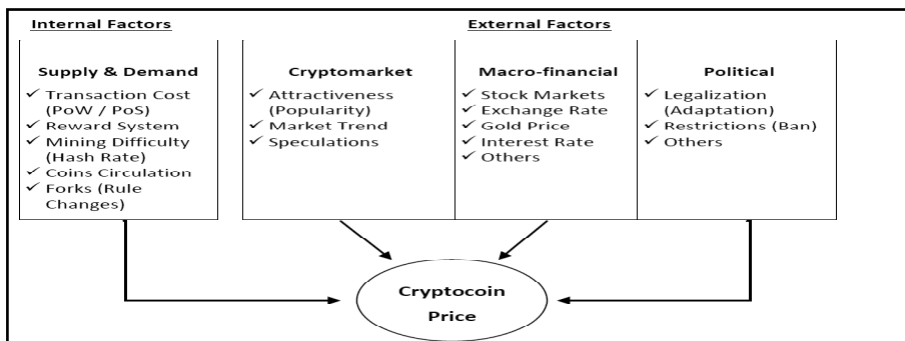
(33) Breu, S. U. and Seitz, T. G., «Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society,» (2018) p.5.

(34) Sovbetov, Y., «Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero» *Journal of Economics and Financial Analysis* (2018) 2: (2), <www.ojs.triapa.edu.com/jefa> 1-27.4/3/2019, p .4.

(35) LOW, K. F. K. and TEO, E., «Legal Risks of Owning Cryptocurrencies,» (Institutional Knowledge at Singapore Management University, 2017. P .4

composition of coinage and the amount of debt for which they pass as legal tender.⁽³⁶⁾ Fourthly, normal money used to be backed by gold, but that has changed and some countries are depending on other economic factors. Fifthly, the current system of legal currency mostly works on mutual trust between the people and the monetary institutions and government. Finally, the value and exchange rate of each currency depends on many factors, especially economic stability, inflation, public debt, interest rate, and political stability.⁽³⁷⁾

In relation to the value of cryptocurrencies, the market has more than one thousand cryptocurrencies with a total market value of almost \$190 billion.⁽³⁸⁾ One of the chief concerns of cryptocurrencies is their high volatility as unknown commodities. There are no financial statements, earnings reports, or financial ratios to study to determine their fair value. Their value is not backed by any economic assets, and is not tied to any national traditional currency of any country. Therefore, their exchange rate is determined according to many factors, which have direct or indirect impacts on their market value. The following figure summarises most of the factors that have direct and indirect impact on the value of cryptocurrencies.⁽³⁹⁾



From the above groups of factors which affect the prices of cryptocurrencies mining cost, supply and demand, and public opinion will be explained in the following section:

Mining cost: Like any other business, cryptocurrency mining needs capital

(36) Ibid, p.4

(37) Cvetkova, I., «Cryptocurrencies Legal Regulation» BRICS LAW JOURNAL (2018) V: (2), 128, p 130.

(38) Corbeta, S., Luceyb, B., Urquhart, A., and Yarovaya, L., «Cryptocurrencies as a Financial Asset: A Systematic Analysis,» (2018) p 3.

(39) The figure is copied from Sovbetov, Y., «Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero» Journal of Economics and Financial Analysis (2018) 2: (2), <www.ojs.tripaledu.com/jefa> 1-27.4/3/2019, p.7.

. The cost to start and run the business includes cost of the building, mining facilities and equipment, electricity consumption, internet bandwidth, and manpower.⁽⁴⁰⁾ The cryptocurrency mining sector is composed of the following principal activities: firstly, advanced mining hardware specially manufactured for cryptocurrencies; secondly, cloud mining services which are services that rent out hashing power of developing blocks to customers; thirdly, remote hosting services which are services that host and maintain customer-owned mining equipment; and finally, a mining pool which is a structure that combines computational resources from multiple miners to increase the frequency and likelihood of finding a valid block.⁽⁴¹⁾

Generally speaking, a high level of energy is needed during the mining process of cryptocurrencies. This is due to the use of powerful computer systems worldwide, and keeping the Blockchain running. The competitive process of adding blocks to the chain is computation-intensive and requires large energy input. It has been estimated that mining Bitcoin, Ethereum, Litecoin and Monero from 1 January 2016 to 30 June 2018 has consumed an average of 17, 7, 7 and 14 MJ to generate one US\$, respectively. In comparison, conventional mining of aluminium, copper, gold, platinum and rare earth oxides consumed 122, 4, 5, 7 and 9 MJ to generate one US\$. In addition it has been estimated that during this period, the estimated mining for all 4 cryptocurrencies was responsible for 3–15 million tonnes of CO₂ emissions.⁽⁴²⁾

Supply and demand: supply and demand are major factors that affect the value of virtual currency, which make their exchange rate volatile.⁽⁴³⁾ It has been stated that there is a limited amount of cryptocurrencies that can be produced. Therefore, a shortage in production could lead to an increase in its value when the demand become high and the supply will be low. For instance, the total number of Bitcoin that can be ever produced which is called total money supply will be 21,000,000 only.⁽⁴⁴⁾

(40) Li, X. and Wang, C. A., «The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin,» (2017) p.51.

(41) Hileman, G. and Rauchs, M., «Global Cryptocurrency Benchmarking Study,» (2017) p5.

(42) Krause, M. J. and Tolaymat, T., «Quantification of Energy and Carbon Costs for Mining Cryptocurrencies» *Nature Sustainability* (2018) 1: <<https://www.nature.com/articles/s41893-018-0152-7>> 711-18, p. 711.

(43) Vovchenko, N. G., Tishchenko, E. N., Epifanova, T. V., and Gontmacher4, M. B., «Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them» *European Research Studies* (2017) XX: (1), <<https://ideas.repec.org/a/ers/journal/vxxy2017i1p36-48.html>>.2/4/2019, p.38.

(44) Hayes, A. S., «Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin» (2016): <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2648366> p. 4.

Public opinion: public opinion is a major factor that can affect the value of cryptocurrencies. When the public perception of the new invention is high and positive its value appreciates and the demand for it increases. For example, it is expected that the value of Bitcoin will depend on transaction capability resulting from public recognition and adoption.⁽⁴⁵⁾ Furthermore, public opinion is often shaped by the media and types of reports published about the advantages, disadvantage, and the economic and legal risks associated with the use of cryptocurrencies in e-trade. Public opinion also reflects in some cases the formal stand of authorities, which will become more positive towards cryptocurrencies and increase their values when the governments accept this form of currency as part of the electronic payment system. However, despite the existence of many types of Cryptocurrency and their use in online trading as part of the stock exchange market, countries still vary in their official stands on this currency. Some countries clearly illegalized the trade in Cryptocurrency, others did not make a clear decision on the matter, and some have indirectly accepted the development of this digital currency and not opposing transactions related to these currencies.⁽⁴⁶⁾

4. Main legal risks associated with cryptocurrencies

The European Banking Authority (2014) defined 70 risks related to cryptocurrencies. The identified risks were categorised into several groups based on who or what is threatened by them. The threatened groups include: A) users of cryptocurrencies for business transactions; B) users of cryptocurrency and cryptocurrency exchange offices; C) financial integrity, including money laundering and other crimes; D) existing payment systems and E) regulatory authorities.⁽⁴⁷⁾ Some opponents to cryptocurrencies identify also the role of cyber criminality and the unknown destabilizing effects on world economies as some of the potential pitfalls of their evolution.⁽⁴⁸⁾

Overall, based on the discussion in the previous parts of this paper about the characteristics of cryptocurrencies, the way they are produced without the control of any official authorities, and the inherent anonymity associated

(45) Li, X. and Wang, C. A., «The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin,» (2017).p 51.

(46) Lansky, J., «Possible State Approaches to Cryptocurrencies» Journal of Systems Integration (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019, pp22-24.

(47) Ibid, : pp22-24.

(48) Corbeta, S., Luceyb, B., Urquhartc, A., and Yarovaya, L., «Cryptocurrencies as a Financial Asset: A Systematic Analysis,» (2018). p 4.

with transactions and wallet owners of those currencies;⁽⁴⁹⁾ it can be said that cryptocurrencies have high legal risks, which could diminish most of their advantages. The following sections will look at the technical and legal sources and the forms of risks associated with cryptocurrencies. Some suggestions to minimize the risks are also explained.

A. Regulatory Issues

There is no consensus to date about the safety of cryptocurrencies. There are those who defend it and focus on its positive aspects and those who are partial as well as those who totally oppose it. This explains the lack of official universal regulations related to its use.

The lack of regulations and the variation in the countries' official stands towards cryptocurrencies actually represent a main source of legal risks. Currently, there are some countries that clearly illegalized the trade in cryptocurrency, while others are yet to make clear decisions about it, and some have accepted it indirectly by not opposing transactions related to these currencies.⁽⁵⁰⁾ In addition, there are some countries such as Saudi Arabia and the United Arab Emirates that have reached an agreement to develop their own form of cryptocurrency to be used between them to settle their mutual trade transactions.⁽⁵¹⁾

Here, it needs to be said that the establishment and implementation of rules and regulations on a national and an international level is a must if the risks are to be reduced. An agreed upon system of regulations with a practical enforcement mechanism is necessary in order to protect investors, asset managers, and financial institutions, and to deal with criminal issues related to cryptocurrencies. Without a unified approach to regulate its use the adoption of cryptocurrencies could create real risks to investors and all parties involved. As a result of different stands towards the legality of cryptocurrencies, it needs to be expected that legal rules related to its taxation status, trading rules, or even its outright legality, could change overnight.

(49) Almukaynizi, M., Paliath, V., Shah, M., Shah, M., and Shakarian, P. «Finding Cryptocurrency Attack Indicators Usingtemporal Logic and Darkweb Data», 2018 Paper presented at the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA IEEE International Conference on Intelligence and Security Informatics (ISI), 9-11 Nov. 2018 p1.

(50) For different official stands towards virtual currencies see Cvetkova, I., «Cryptocurrencies Legal Regulation» *Brics Law Journal* (2018) V: (2), 128, pp137-151.

(51) Zmudzinski, A., «Uae Central Bank, Saudi Arabia to Develop Joint Cryptocurrency for Interbank Transactions,» (cointelegraph, 2018).

The legal variations in countries' stands towards cryptocurrencies have many causes. One cause is its nature as anonymous and decentralized financial transactions. Some literature states that cryptocurrencies as a combination of anonymous and decentralized financial transactions are a source of regulatory challenge for countries.⁽⁵²⁾ In essence, this is because virtual currency is a new form of financial tools and governments as well as banks have yet to form coherent fiscal policies about it. Moreover, due to the anonymity of the operations of cryptocurrencies, it could be very difficult for any country to implement rules and regulations and make it applicable to or enforceable on a system which is outside its jurisdiction and does not have control over it.⁽⁵³⁾ The suggestion to unify the countries' legal stands towards cryptocurrencies is to develop new international agreements and conventions. These need to be established to oblige countries to accept and follow an international framework to deal with virtual concurrencies in order to minimize their risk.

Another cause for the variation or lack of regulations for cryptocurrencies is the nature of these currencies as records in a ledger that uses Blockchain technology. Such characteristic and the anonymity of the owners of records constitute a real challenge for civil law, administrative law, and criminal law. For civil law, cryptocurrencies appear as a measure of value other than money. The challenge for administrative and criminal laws is to find an appropriate approach to limit the use of cryptocurrencies for criminal purposes such as funding terrorist activities and money laundering.⁽⁵⁴⁾

B. System Hacking and Scams

Cyber hacking and scams are the major threats for all activities that have any connection with the internet, and cryptocurrencies as part of cyberspace are no exception and do not have complete protection. Usually the cyber attacks for cryptocurrencies target the mining process and the development of new kinds of cryptocurrencies.⁽⁵⁵⁾

(52) Marian, O., «A Conceptual Framework for the Regulation of Cryptocurrencies» University of Chicago Law Review Dialogue (2015) 53: <<https://ssrn.com/abstract=2509857> > p57.

(53) Breu, S. U. and Seitz, T. G., «Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society,» (2018). p 8.

(54) Srokosz, W. and Kopyciaski, T., «Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability» Journal of Teaching and Education (2015) 4: (2), <www.universitypublications.net/jte/0402/pdf/F5N180.pdf> 619–27, p p620-622.

(55) Sari, A. and Kilic, S., «Exploiting Cryptocurrency Miners with Osint Techniques,» in Transactions on Networks and Communications (2017) p.63.

There are a number of security breaches reported in relation to cryptocurrencies. For example, Bitcoin has been subjected to over 40 thefts, including a few that exceeded 1 million USD in value.⁽⁵⁶⁾ Moreover, it has been reported by South Korea Internet and Security Agency that cyber attacks were able to steal Bitcoin units with a total value of 870,000 USD and Ethereum worth 32.6 million USD, all of them belonging to the biggest cryptocurrencies exchange platform in South Korean called Bithum. The attackers were able to hack into the company computers and collect emails and mobile numbers of some users and used the information to achieve their illegal goal of stealing millions of cryptocurrencies units or tokens.⁽⁵⁷⁾

To sum up, it is clear that despite the high level of technicality of the Blockchain technology, and its arguably high level of security, cyber attackers were still able to infiltrate the system. Fundamentally, they were able to collect massive information from different sources about users and transactions in cryptocurrencies networks, and analyse the data in order to know how to develop a suitable approach to achieve their illegal target.⁽⁵⁸⁾

C. Security and Verification

The verification system constitutes another risk for the use of cryptocurrencies.

It is important to explain the verification system in use to show its weakness. Basically, verification of the ownership of cryptocurrencies and its related deals is based on a pair of cryptographic private and public keys. The private key can be compared to a password needed to ‘unlock’ cryptocurrency funds while the public key -if converted to an address- can be compared to a public email address or bank account number.⁽⁵⁹⁾ To further explain, the private key is similar to the Personal Identification Number (PIN). However, the problem with the private key is that anyone who knows the key can act as the owner for the account and can execute any transaction on the account without the need for any other identification method.⁽⁶⁰⁾ In other words, the private key

(56) Bunjaku, F., Gjorgieva-Trajkovska, O., and Miteva-Kacarski, E., «Cryptocurrencies – Advantages and Disadvantages» *Journal of Economics* (2017) 2: (1), <<http://js.ugd.edu.mk/index.php/JE/index>> p.32.

(57) Sari, A. and Kilic, S., «Exploiting Cryptocurrency Miners with Osint Techniques,» in *Transactions on Networks and Communications* (2017) p.64.

(58) *Ibid*, p.65.

(59) Hileman, G. and Rauchs, M., «Global Cryptocurrency Benchmarking Study,» (2017) p.5.

(60) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019, p.21.

acts as the account number and the pin number at the same time. This means that there is no double checking for misuse. The public key, on the other hand is given during the second part of any deal related to a certain account in order to confirm the transaction and open message initiated by using the private key. Usually public key can be given to and used by many people to be able to read messages initiated by the private key.

The security risks related to malice and technology and the irreversibility of transaction related to human error or illegal action are the most concerning legal issues arising from the technical method of validating the ownership and transactions of cryptocurrencies. The legal risk is related to the real challenge for all parties engaged in cryptocurrencies mining and transactions to secure their transactions. The flaw is that the processes are administered as peer to peer and not supervised by a third party to work as a clearinghouse that could reverse errors and alleviate damage.⁽⁶¹⁾ In addition, Blockchain network does not distinguish between the legitimate owner and those who acquire the private key in an illegal way. The private key of any account in Blockchain network is highly likely to be obtained through hacking or as a result of human error.⁽⁶²⁾ The security concerns in Blockchain technology are related also to the limitation with the ledger storage facility, limited developments in technology, lack of skilled workforce, lack of proper legal codes and standards, variations in processing speeds and time, and computing capabilities.⁽⁶³⁾

Blockchain technology as an open ledger for cryptocurrencies allows participants in the system to know and watch all transactions, without revealing any information about the identity of the parties.⁽⁶⁴⁾ For the system to be efficient as a decentralised ledger, it does not allow reversal of transactions even if a transaction is a result of human mistakes or malice. Even with a court order, it cannot be reversed.⁽⁶⁵⁾ The only way to reverse

(61) Vyas, C. A. and Lunagaria, M., «Security Concerns and Issues for Bitcoin» *International Journal of Computer Applications* (2014): <<https://pdfs.semanticscholar.org/4751/e99514948c2cbef0f6e4a12e65c72f75aea8.pdf>>.9/4/2019, p.10.

(62) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019, p.21.

(63) Kumar, N. M. and Mallick, P. K., «Blockchain Technology for Security Issues and Challenges in Iot,» (2018) p.1821.

(64) Bunjaku, F., Gjorgieva-Trajkovska, O., and Miteva-Kacarski, E., «Cryptocurrencies – Advantages and Disadvantages» *Journal of Economics* (2017) 2: (1), <<http://js.ugd.edu.mk/index.php/JE/index>> p.37.

(65) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to>

a transaction is for it to be conducted as a new transaction by approval of the two parties through their private and public keys. The problem in this case is when some units of cryptocurrency are transferred illegally or by mistakes to an unknown party, and the system does not reveal any information about his identity, it leads to a permanent loss for the units' owner. The latest evidence about the risk of human error as a cause of loss for cryptocurrencies is the death of the founder QuadrigaCX exchange called Gerald Cotton. QuadrigaCX is a leading cryptocurrency in Canada, but the access to its assets is lost due to the death of its founder in India, who was the only one who knew the cryptographic keys for all assets. The value of the holding amount was equivalent to \$190 million. Cotton used extremely meticulous cyber-security and anti-hacking measures to protect the keys to cryptocurrencies accessibility, which made it virtually impossible to crack and to date no one is able crack the keys to access the holding amount.⁽⁶⁶⁾

Record irreversibility is a necessary part of the working mechanism of cryptocurrencies' system, which is also related to the technical characteristic of cryptocurrencies as a chain of records. The whole system units and transactions are interrelated to each other and need to be in chronological order and permanent in order for the system to work as it is meant to.⁽⁶⁷⁾ The irreversibility of transaction record is a major difference between a centralized and a decentralized system.⁽⁶⁸⁾

D. Criminal risk

Cryptocurrencies use Blockchain technology as an open ledger for their mining and transactions, which can be watched by all participants without revealing any information about the identity of the parties.⁽⁶⁹⁾ Consequently, such anonymous system would be very suitable to facilitate criminal actions

Cryptocurrencies>.4/4/2019, p.25.

(66) Cohan. The Key Man Problem p. 235.

(67) Jepkemei, B. and Kipkebut, A., «Blockchain -a Disruptive Technology in Financial Assets» IRE Journals (2019) 2: (9), <<http://irejournals.com/formatedpaper/1701014.pdf>>.10/4/2019, p39.

(68) Sas, C. and Khairuddin, I. E. «Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users», 2017, Paper presented at the 2017 CHI Conference on Human Factors in Computing Systems, Denver, Colorado, USA ACM digital library, <http://eprints.lanccs.ac.uk/83765/1/Design_for_trust.pdf> 11/4/2019, p.6.

(69) Bunjaku, F., Gjorgieva-Trajkovska, O., and Miteva-Kacarski, E., «Cryptocurrencies – Advantages and Disadvantages» Journal of Economics (2017) 2: (1), <<http://js.ugd.edu.mk/index.php/JE/index>> p.37.

such as money laundering and terrorist financial support.⁽⁷⁰⁾ The difficult part of dealing and minimizing the use of cryptocurrencies for criminal purposes is the limited ability of national authorities and agencies to monitor and discover illegitimate transactions on the basis of peer-to-peer without the supervision of any third party.⁽⁷¹⁾ As a result, the European Banking Authority has classified the use of cryptocurrencies for illegal funding as a high priority risk.⁽⁷²⁾

Another reason which make cryptocurrencies suitable for criminal financial operations, is that the system characteristic of allowing individuals to open as many accounts as they like for each type of cryptocurrencies they have without any cost and in a very short period of time,⁽⁷³⁾. This makes it more difficult to trace illegal operations.⁽⁷⁴⁾ In addition, the decentralized characteristic adds another advantage for cryptocurrencies to be used to commit financial crime because no official authority is able to control all operations.⁽⁷⁵⁾

Criminal risk is arguably a substantial barrier to the further technical development and acceptance of virtual currency. However, it has been suggested that self-regulation and adoption of international recommendations could lead to positive outcomes of minimizing criminal risk associated with cryptocurrencies.⁽⁷⁶⁾ On the other hand, it has been pointed out that imposing restrictive regulations on cryptocurrencies should not lead to limit the currencies from reaching their potential or adding extra cost on related transactions.⁽⁷⁷⁾

5. Conclusion

Cryptocurrencies or virtual currencies are advanced technical products of cryptographic unites and accounts as equivalent or as alternative to traditional

(70) Vovchenko, N. G., Tishchenko, E. N., Epifanova, T. V., and Gontmacher, M. B., «Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them» *European Research Studies* (2017) XX: (1), <<https://ideas.repec.org/a/ers/journal/vvxy2017i1p36-48.html>>.2/4/2019, p.39.

(71) Breu, S. U. and Seitz, T. G., «Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society.» (2018) p. 9.

(72) Ibid, p.5.

(73) Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019, p.21.

(74) Marian, O., «A Conceptual Framework for the Regulation of Cryptocurrencies» *University of Chicago Law Review Dialogue* (2015) 53: <<https://ssrn.com/abstract=2509857>> p.56.

(75) Ibid, : p.57.

(76) Breu, S. U. and Seitz, T. G., «Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society.» (2018) p.9.

(77) Marian, O., «A Conceptual Framework for the Regulation of Cryptocurrencies» *University of Chicago Law Review Dialogue* (2015) 53: <<https://ssrn.com/abstract=2509857>> p.59.

money. The main technical characteristics of these innovative currencies are permanent, decentralized, anonymous ownership and operations. Such characteristics have made cryptocurrencies sources of legal and economic risks for individual and states, as well as challenges for the regulators. The main legal risks for individuals who engage in cryptocurrencies business are security issues, system hacking, system failure, ownership verification, and irreversibility of the wrong actions. The risks for states stem from use of these currencies for money laundering and financial terrorist support. The challenges for the regulators is how to develop and impose legal rules, which are able minimize the legal and economic risks associated with cryptocurrencies. The challenges are due to the way of issuing cryptocurrencies through decentralized system on the websites and anonymous ownership and operations through digital keys. The other challenge is for banking and financial regulators of how to deal with the new development and how to deal transactions based on cryptocurrencies. It is a real challenge for the banking system because the system cannot deny the existence of cryptocurrencies forever. If the banking system gradually starts to accept to deal the new currency as equivalence to normal money, the issues would be about the approaches and formula of making conversion between all of them and how to deal with the proof of ownership.

The paper has reached to the following outcomes:

1. Cryptocurrencies are new real developments for the monetary system.
2. Cryptocurrencies are new form of currencies, which can be used for payment obligation transferred between digital address.
3. Cryptocurrencies in exchange market appear as any kind of traditional currencies and any related deal is similar to any deal in any pair of normal currencies.
4. Cryptocurrencies still have high level of economic and legal risks, which are related to lack of national international legal frameworks.

The main recommendations:

1. Implementation international agreements to unify national rules and countries position towards cryptocurrencies.
2. Existed agreements and rules related to electronic banking and commerce can be developed to deal with cryptocurrencies.
3. Information technology experts and legal experts need to work together to develop technical and legal formwork to improve security level and minimize criminal uses of cryptocurrencies.

References

- Almukaynizi, M., Paliath, V., Shah, M., Shah, M., and Shakarian, P. «Finding Cryptocurrency Attack Indicators Usingtemporal Logic and Darkweb Data», 2018 Paper presented at the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA IEEE International Conference on Intelligence and Security Informatics (ISI), 9-11 Nov. 2018 .
- Berentsen, A., and Schär, F., “A Short Introduction to the World of Cryptocurrencies.” 2018.
- Brenig, C., Accorsi, R., and Müller, G., “Economic Analysis of Cryptocurrency Backed Money Laundering.” Association for Information Systems: , 2015.
- Breu, S. U., and Seitz, T. G., “Legislative Regulations to Prevent Terrorism and Organized Crime from Using Cryptocurrencies and Its Effect on the Economy and Society.” 2018.
- Bunjaku, F., Gjorgieva-Trajkovska, O., and Miteva-Kacarski, E., “Cryptocurrencies – Advantages and Disadvantages” Journal of Economics (2017) 2: (1), <<http://js.ugd.edu.mk/index.php/JE/index>>.
- Corbeta, S., Luceyb, B., Urquhartc, A., and Yarovaya, L., «Cryptocurrencies as a Financial Asset: A Systematic Analysis.» 2018.
- Cvetkova, I., «Cryptocurrencies Legal Regulation» Brics Law Journal (2018) V: (2), 128.
- Daradkeh, L., «The Challenges of Law Keep Pace with the Technological Developments in Banking and Finance» kuwait International Law journal (2018): (3 par 1), 325- 61,.
- Hayes, A. S., «Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin» (2016): <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2648366>.
- Hileman, G., and Rauchs, M., «Global Cryptocurrency Benchmarking Study.» 2017.
- Jepkemei, B., and Kipkebut, A., «Blockchain -a Disruptive Technology in Financial Assets» IRE Journals (2019) 2: (9), <<http://irejournals.com/formatedpaper/1701014.pdf>>. (2019) 2: (9).
- Krause, M. J., and Tolaymat, T., «Quantification of Energy and Carbon Costs for Mining Cryptocurrencies» Nature Sustainability (2018) 1: <<https://www.nature.com/articles/s41893-018-0152-7>> 711- 18.
- Kumar, N. M., and Mallick, P. K., «Blockchain Technology for Security

Issues and Challenges in Iot.», 2018.

- Lansky, J., «Possible State Approaches to Cryptocurrencies» *Journal of Systems Integration* (2018) 8: (1), <https://www.researchgate.net/publication/322869220_Possible_State_Approaches_to_Cryptocurrencies>.4/4/2019.
- Li, X., and Wang, C. A., «The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin.», 2017.
- LOW, K. F. K., and TEO, E., «Legal Risks of Owning Cryptocurrencies.» *Institutional Knowledge at Singapore Management University*, 2017.
- Marian, O., «A Conceptual Framework for the Regulation of Cryptocurrencies» *University of Chicago Law Review Dialogue*, (2015), 53: <<https://ssrn.com/abstract=2509857> >.
- Sari, A., and Kilic, S., «Exploiting Cryptocurrency Miners with Osint Techniques.» *In Transactions on Networks and Communications*, 2017.
- Sas, C., and Khairuddin, I. E. «Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users», 2017, Paper presented at the 2017 CHI Conference on Human Factors in Computing Systems, Denver, Colorado, USA ACM digital library.<http://eprints.lancs.ac.uk/83765/1/Design_for_trust.pdf> 11/4/2019.
- Sovbetov y., «Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litecoin, and Monero» *Journal of Economics and Financial Analysis* (2018) 2: (2), <www.ojs.tripa.edu.com/jefa>, 1-27.4/3/2019.
- Srokosz, W., and Kopyciaski, T., «Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability» *Journal of Teaching and Education* (2015) 4: (2), <www.universitypublications.net/jte/0402/pdf/F5N180.pdf>.
- Vovchenko, N. G., Tishchenko, E. N., Epifanova, T. V., and Gontmacher4, M. B., «Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them» *European Research Studies* (2017) XX: (1), <<https://ideas.repec.org/a/ers/journal/vxxy2017i1p36-48.html>>.2/4/2019.
- Vyas, C. A., and Lunagarra, M., «Security Concerns and Issues for Bitcoin» *International Journal of Computer Applications* (2014): <<https://pdfs.semanticscholar.org/4751/e99514948c2cbef0f6e4a12e65c72f75aea8.pdf>>, 9/4/2019.
- Zmudzinski, A., «UAE Central Bank, Saudi Arabia to Develop Joint Cryptocurrency for Interbank Transactions.» *cointelegraph*, 2018.

Table of Contents

Subject	Page
Abstract	63
Introduction	64
1. Technical Background of Cryptocurrencies:	65
2. The Differences between Cryptocurrencies and Tools of Normal Electronic Payment Systems	67
3. Comparison between Cryptocurrencies and Normal Money	68
A. Advantages and legal status of cryptocurrencies an asset or currency	68
B. Mining cryptocurrencies	69
C. The value of cryptocurrencies	71
4. Main legal risks associated with cryptocurrencies	74
A. Regulatory Issues	75
B. System Hacking and Scams	76
C. Security and Verification	77
D. Criminal risk	79
5. Conclusion	80
References	82