International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 8
August, 2023
Pages: 30-47

Examining and Analyzing the Challenges of Using Digital Currency and Policies

Mona Rajab Zade Baghi[1]; Mostafa karamipour[2]

[1] Master of Criminal Law and Criminology, Iran

[2] PhD in Criminal Law and criminology, Iran

http://dx.doi.org/10.18415/ijmmu.v10i8.5070

Abstract

The challenges related to cryptocurrencies can be mentioned among the security problems of facilitating internet crimes, tax evasion and money laundering, whose institutionalization in the society causes disruption in the economic and even political and social system. An important challenge that has always existed in legalization and exists in this field as well is that the laws should not be so restrictive that they become cumbersome and prevent the growth and birth of start-up companies; Because among the crimes that can be committed in connection with virtual currencies such as Bitcoin are: money laundering, theft, fraud and gambling and buying and selling of prohibited items, which will increase if these crimes are not legalized and criminalized. In addition, organized crimes that have much wider and more destructive effects should also be taken into consideration; The effect of crimes related to cryptocurrencies is so much that they are mentioned as a threat to the development of countries. Accordingly, considering the importance of this type of crime, in this part, it is mentioned to examine the challenges that currently exist in Iran.

Keywords: *Digital Currency; Politics; Facilitation of Internet Crimes; Tax Evasion and Money Laundering*

Introduction

Introduction (Virtual currencies have all the economic characteristics of money because they are used as a means of buying goods, online services, a unit of measure and a means of storing value. Therefore, some believe that it should be considered as money. On the other hand, some others emphasize that it is a commodity. The United States Commodity Futures Trading Commission (CFTC) has also accepted the recent opinion due to its expanded interpretation of the commodity; But the drawback of identifying virtual currencies as goods is that anti-money laundering regulations can no longer be applied against them[1]. To date, no country has created digital currency as legal tender. In other words, there are no special regulations and standards in the world related to virtual money as one of the types of digital money; This means that digital money is not an official national currency in any jurisdiction. Although

[1] Jeffrey H. Matsuura, "Effect of digital currency on traditional currency regulations", translation and research: Saeed Siah Bedi Kermanshahi and Reza Mohebi, Fars Legal Research Quarterly, No. 2, Spring 2018, pp. 125-126.

Bitcoin and other forms of digital currency are widely used around the world, they are not legal tender. The value of digital currency is based on the willingness of parties to offer and accept digital currency as a valid transfer of economic value in a transaction. Digital currencies are not supported or guaranteed by any government. Of course, it's not surprising that the cryptocurrency industry is very willing to declare bitcoins as money, as this allows everyday users to not worry about the possibility of some of their bitcoins being stolen. And this fear of users is completely reasonable; Because the majority of thefts from reported Bitcoin users constitute only 6 to 9% of the total Bitcoin in circulation, which if we add the income from the crime of theft in general, we get a much larger figure.[2]

Now the question that arises is: if the buyers of bitcoins only buy these stolen bitcoins, can they assure ordinary investors that they will not lose their money due to the purchase of stolen bitcoins? Investors and Bitcoin buyers can demand that exchanges selling bitcoins register, validate, and identify the customers to whom they sell bitcoins that later turn out to be stolen. Therefore, as mentioned, the relatively new emergence of virtual currency has led to the need to establish comprehensive regulations for virtual currencies. It is true that there is no law in this regard, however, it is not true to say that the issue of virtual money is in a complete legal vacuum and the general framework of electronic commerce regulations can be applied in this regard. So far, many countries have benefited from this law regarding the regulation of relations between individuals in the e-commerce space; Regarding the crimes related to cryptocurrencies, using many documents and standards that have been approved so far regarding the crime of money laundering, including the United Nations Convention on International Organized Crime in 2003 and the Convention against Corruption of this organization in 2005, can be cited[3]. In February 2015, in the United States, according to the court's verdict, a person who tried to create a market for selling drugs under the name of "Silk Road" and used the virtual currency Bitcoin for his payments, was sentenced to prison; Two months before that, a person who had established a bitcoin exchange was arrested on the charge of not reporting suspicious banking activities of money laundering by using the exchange accounts of Silk Road customers and running an illegal money transfer business.

In this regard, we can refer to a fraud case that was raised and processed in the state of Texas in 2013. In this case, the defendant argues in his defense that bitcoins are not money, and therefore, any investment requests related to them and the acceptance of these requests by the defendant cannot include related laws. But in the end, the court accepted Bitcoin as money or a form of money and convicted the accused.[4]

The identity of the exchange parties of crypto currencies remains unknown The origin of the unknown identity of the parties to the exchange of encrypted currencies lies in the possibility that the user profiles of the owners of these currencies do not match with their real identities. In fact, the owners of these funds are not nameless, but anonymous, and therefore it is easier for them to commit such violations and crimes; Although it is possible to track transactions and identify the traces of a user in these networks, the policy on transparency and tracking has not been such a thing. In fact, in this regard, it should be acknowledged that the exchange parties through Bitcoin can exchange this crypto currency without their identity being revealed, and in this way, buy and sell goods and any kind of services, and even simply exchange Bitcoin. do Encrypting digital currencies is for the purpose of making the content unintelligible and returning it to the previous state requires decryption, and in this way, the exchange and the identity of the parties to the exchange of such currencies are protected[5]. Of course, despite the criticism of digital

[2]Mishkin, Fredrick S., The Economics of Money Banking and Financial Markets, Pearson Education,4 th Edition, 2004, p:44.

[3]Pacy, Eric P., "Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes", NEW ENG. L. REV. vol. 121, 2014, p. 49.

[4]see: SEC v. Shavers, No. 4: 13 -cv-00416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 2013 (and Complaint at 1–2, SEC v. Shavers, No. 4: 13 -cv-00416 (E.D. Tex. July 23, 2013)

5

currencies and the announcement of the existence of risks in various dimensions, such as the fact that this money is economically unsupported, there are also advantages that encourage people to use them in transactions. Ease of access and exchange online, hiding the identity of the parties and their increasing value are among these things. This is the desire to use crypto-currencies while the exchange through them is not free of risk, for example, the private key is a key in the form of a code that contains random and irregular letters and numbers, and its owner does not have access to this key. It will not be possible to exchange. If this private key is lost or forgotten, bitcoins will be lost.[6]

The exchange of cryptocurrencies can be in the form of buying bitcoins from other users who own bitcoins, and it can also be used to buy any product or service. Currently, online stores are emerging that allow customers to exchange goods without intermediaries and pay through cryptocurrencies. This expansion is to the extent that it is likely that their goal is to replace huge websites such as Amazon and eBay; for example, an individual buys a product online from online stores instead of paying from his bank account, the service fee or Pay for the goods you need with Bitcoin. In this way, even international exchanges can be done without the need to use the banking network, which is the beginning of the criminal use of cryptocurrencies such as money laundering, because the identity of the parties to the exchange is unknown, and the origin and destination of these transactions are not known. If the origin of the money is illegitimate, it can be converted into legitimate money in this way.

However, if the identity of the natural or legal person who owns the public address of the virtual currency is known, a large amount of information can be obtained regarding his actions on the network. Today, some private companies specialize in revealing the transactions of these currencies and developing tools to analyze their illegal activities. However, the same level of fakeness and unknown identity is also effective for criminals and especially terrorists who use virtual currencies. In any case, sending an address, for example, Bitcoin, to a media or a public network in the form of voice and video messages is far better and more beneficial than advertising on the bank account number. However, the possibility of tracing virtual currencies limits the activities of criminals to a great extent. Despite what was said about the possibility of tracing virtual currencies, there are also several methods to prevent them from being recognized or so-called "layering". One of these methods is to use the services of "mixers" or "backers" who collect and redistribute the virtual currencies of multiple users and thus hide the path of transactions. In this regard, sites such as CoinJoin and DarkWallet use multiple combined methods. Although many currency mixing practices are not illegal, new research shows that many of these services are actually aimed at laundering illegal money. In the middle of 6104 people affiliated with ISIS used Bitcoin hashing technology to hide exchanges and transactions.[7]

In recent years, innovations have emerged in the use of alternative currencies with an emphasis on maintaining more personal privacy, which benefit from the anonymity feature far more than Bitcoin, which are generally referred to as "Privacy Coins". Although these currencies, like Bitcoin, are open source and are based on the public blockchain, their identification details are no longer public. Among them, we can mention Monro, Dash, and Zedkash. Several studies in recent years indicate the widespread use of privacy coins in criminal acts. In any case, in order to manage the risk of virtual currencies, a situation-oriented solution, by identifying the participants and maintaining their identity and transaction records, can be a great way forward. Although the identification of the participants has many benefits after committing the crime, such as proving the crime and identifying the criminal, which is considered in this preventive application approach. Nevertheless, when the user is aware of his identity and knows that his actions are being recorded, the risk of committing a criminal act increases and as a result, committing

[5]Bohme, R. Christin, N. Edelman, B. & Moore, T. Bitcoin: Economics, Technology, and Governance. The Journal of Economic Perspectives, 29(2), 2015, p: 213.

[6] Bohme, R. Christin, N. Edelman, B. & Moore, T. Bitcoin: Economics, Technology, and Governance. The Journal of Economic Perspectives, 29(2), 2015, p: 213.

[7]see: SEC v. Shavers, No. 4: 13 -cv-00416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 2013 (and Complaint at 1–2, SEC v. Shavers, No. 4: 13 -cv-00416 (E.D. Tex. July 23, 2013)

criminal acts decreases. However, this method will be responsive when participants of virtual currencies operate within the scope of the regulatory environment. In order to solve the unknown characteristic of virtual currency users, the regulations related to authentication can be operationalized in this area. The obligation to authenticate the user through a mandatory authentication identifier when opening a virtual currency account, as well as the obligation to declare such accounts by exchangers/exchangers, solves many problems caused by lack of transparency and anonymity. It is also important to have tools to identify and monitor virtual currency accounts, at least when their transactions exceed a certain amount. The approach mentioned in the document "Requirements and regulations of the field of cryptocurrencies" has been brought to the attention of the Central Bank of Iran. The central bank has tried to reduce the risk of this area to some extent by adopting a risk-oriented approach. First: The list of cryptocurrencies that can be exchanged in cryptocurrency exchanges is determined by the central bank and notified in three-month intervals. [8]Secondly: Cryptocurrency exchanges will be required to comply with anti-money laundering and customer identification laws. Individual buying and selling of cryptocurrencies is allowed only in case of complete identity verification and exchange of identity information and documents and information related to the origin of financial resources or cryptocurrencies. This is the implementation of the legal duty of the exchanges as one of the covered persons, according to Article (5) of the amended Anti-Money Laundering Law of 2017, which must, in accordance with Article (7) of the aforementioned law, authenticate and identify the clients, real owners and In case of action by representatives or lawyers, verify the position and identity of the representative, lawyer and the original. Thirdly: Cryptocurrency exchanges are obliged to record all information related to buying and selling, customers, as well as the reasons and origin of transactions and provide them to the central bank upon request. Anyway, in the end, it should be acknowledged that the anonymity of the parties to the exchange of crypto-currencies is the biggest challenge of political systems, which will prevent the identification and monitoring of the financing of opposing groups. In the end, this could be the beginning of many political and security crises.[9]

Broadness and decentralization Security in the structure of Bitcoin is a multi-dimensional issue and different from other currencies. Since Bitcoin is a decentralized virtual currency, it is designed to eliminate the possibility of fraud or its conversion in the transaction process at a specific time. Therefore, the structure of this currency and its use of blockchain technology make any change of record and the possibility of manipulation in the transaction process impossible. In addition, as mentioned, Bitcoin transactions take place without the need of an intermediary or any third party, so the person has full authority to manage and control his assets. This, in turn, leads to a reduction in the power of governments, and by eliminating the need for government support, it creates grounds for the withdrawal of political structures from the management of the monetary system.

Currently, the development of knowledge and technology has caused the scope of crimes to expand significantly, and this expansion reduces the possibility of arresting and prosecuting the perpetrators due to the fact that they are committed in an organized manner and with new tools. If in the past crimes such as theft, fraud and forgery were possible in the real, material and objective space, today these crimes and such crimes are possible not only in the real space, but also in the virtual space. By entering the websites of banks and various economic institutions, one can steal other people's property and as a result commit fraud, and by making unreal writings and attributing them to people, significant material and moral losses can be imposed on them. One of the most important scams is through virtual using virtual currencies and cryptocurrencies. It is natural that criminals and terrorists are more inclined to use decentralized currencies. These types of currencies that have open source and decentralized interfaces are called "unlicensed" currencies because their access is not limited. There is no single competent center

[8]Bohme, R. Christin, N. Edelman, B. & Moore, T. Bitcoin: Economics, Technology, and Governance. The Journal of Economic Perspectives, 29(2), 2015, p: 213.

[9]Berg, Svenja and McCarthy, Killian J., "The Economics of ISIS — A Case of Theft or Money Laundering?", Freedom from Fear, vol. 11, 2016, p. 84.

to prevent access to the network of these types of currencies. These networks cannot be suspended, punished or completely blocked like centralized systems. It is on this basis that the expansion of the use of cryptocurrencies has also been extended to illegal online stores. Stores that sell various illegal goods such as drugs through the Internet by giving ownership to Bitcoin. In 2011, the first illegal online store was launched in the United States called Silk Road, which allowed users to buy and sell illegal goods through Bitcoin; In addition, this website was also using "TOR" software to hide and make the exchanges anonymous.

Anyway, although virtual currency networks have a decentralized system, their intermediaries mainly use a centralized network. These intermediaries provide the exchange of virtual currencies and wallets. While two users can transfer this type of currency easily and through the peer-to-peer network within the Bitcoin network, it has been proven that the transfer between the Bitcoin network and other virtual or real currencies is often accompanied by problems. which cannot be solved without the help of a third party. Exchange intermediaries such as Binance and Coinbase fill this gap. Based on this, intermediaries can limit the user's access to services like banks. During the unrest in Charlotteville, America, currency transfers to the Daily Stormer network were closed by Coinbase. In explaining the reason for his action, this intermediary announced it because of "preventing user account abuse, currency creation fraud, threatening or promoting violence against others" and stated that "he will continue this restriction policy until the situation calms down". However, it should be recognized that this centralized aspect of a decentralized ecosystem provides a natural "bottleneck" for regulation and oversight. In fact, the problem of converting virtual currency into real currency has caused widespread problems for criminals[10]. Intermediaries such as Coinbase usually impose restrictions on user activity, such as limits on the amount of transactions per week or month. Therefore, although the lack of concentration and open source of virtual currencies facilitates illegal actions, in practice, the restrictions of conversion of these currencies modify their ability to a large extent. Cryptocurrencies, especially global currencies such as Bitcoin, are not subject to monetary, financial and banking sanctions; This has caused that there is no obstacle for its exchange for countries under sanctions such as Iran; In fact, this is due to the special nature of cryptocurrencies. Unlike some international payment systems such as PayPal, although they have facilitated financial communication in the transnational dimension, they are under the influence of international sanctions against countries and do not provide services to such countries, including Iran. Bitcoin and other similar cryptocurrencies are known as an alternative solution to circumvent sanctions due to their unique features that were actually formed in the framework of a certain ideology such as "replacing Bitcoin with the existing global monetary system". Therefore, in turn, by removing intermediaries in financial communication and making it "person-to-person", in addition to formal financial institutions (such as banks and exchanges), in practice, informal financial businesses such as brokers or Rial liaisons, which are the origin of some The effects are bad, it has been removed. Therefore, as mentioned, the areas related to Bitcoin and cryptocurrencies are extremely wide and this technology affected the entire industry, so it is very difficult to determine the affected areas for legalization. On the other hand, blockchain technology is designed based on decentralized architecture. It is cross-border and not limited to a specific geography, and this issue will also make legalization in this area difficult, but with a correct and evolutionary understanding of it, laws can be enacted in a way that covers the majority[11]. - Expansion of technological dimensions in different areas - The cross-border nature of Bitcoin and Blockchain technology The first method to determine the areas prone to legalization is to separate the areas according to their type of service and determine the priority of action by considering behavioral patterns, by experts (to determine the priority, you can use the available statistics and patterns for supply and demand in Harkam used the areas) Currently, the areas that need to be legislated can be listed as follows: - Fields related to Pardakht services - Fields related to facility services - Areas related to

[10]Shamlou, Baqir; Khalili Paji, Aref, "Risk-based criminal policy against virtual currency technology", Majlis and Strategy Quarterly, year 27, number 139, fall 2019, p. 268.

[11]Khaleghi, Abolfath; Akhtari, Sajjad, "Globalization of criminal law in the light of the fight against organized crime", detective magazine, second volume, year 8, number 29, winter 2013, p. 25.

investment services. Each of these areas has a degree of importance that should be prioritized according to culture and behavioral patterns, and then the governing bodies in each of these areas, together with experts from digital currencies, law and economics Working group to explain the necessary requirements in that field.[12] The second method is the separation of areas susceptible to legalization according to the structural components. In this method, unlike focusing on the services provided by digital currencies and blockchain technology, we will focus on the structure and components of this ecosystem. That is, unlike the previous method, which starts with the end users and the application of the law, the implementation of the law will start with the main actors and performers. With this logic, the current space of this system will be divided as follows: - Digital coins - Initial supply of coins - Smart contracts - exchange offices - Extractors In this case, according to the importance of each of these areas and the opinions of experts, these areas should be prioritized, relevant institutions should be determined and legislation should be applied.[13]

The quality of applying the laws and regulations of virtual currencies Since virtual currencies are not created through permission or government actions, they are not considered legal money and therefore are not subject to the supervision of relevant regulations as official currency. And this issue as an important challenge in the field of legalization is that the laws should not be so restrictive that they become cumbersome and prevent the growth and birth of start-up companies. What comes to mind from the word "legalization" at first glance is its contrast with prohibition. However, there is no consensus among experts about the exact meaning of this approach. One of the most important reasons for these differences should be considered that many have used the term "decriminalization" or "decriminalization" instead of legalization and somehow They believe in their synonyms. Nedelman is one of the most famous proponents of legalization, who used legalization and decriminalization in the same sense. Theft, fraud, gambling, buying and selling of prohibited items, etc. are some of the crimes that can be committed in connection with Bitcoin, in the absence of legalization and criminalization. In addition, organized crimes that have far more extensive and destructive effects should also be taken into consideration. The impact of these crimes is such that they are considered as a threat to the development of countries. One of these organized crimes is money laundering.[14]

Money laundering in its traditional form also presents the police and security forces with many difficulties in the field of crime detection, because the crime of money laundering is a delayed crime and there are always preliminary crimes, the proceeds of which are converted into laundered money. . Now, if money laundering is done through crypto-currencies, it becomes much more difficult to detect the crime and requires special measures. Accordingly, despite this situation, some jurisdictions have allowed regulatory authorities that oversee traditional currency to play a role in overseeing digital currencies. In the monetary and banking system, there are many laws and requirements resulting from various international, regional and national obligations, directives and guidelines so that the country's economic system can provide a safe and healthy environment for domestic and foreign investors and capital owners from Ensure the safety of their property. Banks, financial and credit institutions and natural and legal persons providing monetary, banking or any mediation of funds must act according to special laws[15]. Establishing a financial institution is accompanied by obtaining a license and checking various qualifications, and undertaking banking operations without a license sometimes guarantees criminal

[12]Kodkhodaei, Abbas Ali; Nowruzpour, Hessam, "The challenge of virtual currencies in the fight against money laundering and terrorist financing with an emphasis on the actions and recommendations of the Financial Action Task Force (FATF)", International Legal Journal, No. 62, Spring-Summer 2019, p. 20.

[13]Umlauft, Thomas S., "Is Bitcoin Money? An Economic-Historical Analysis of Money, Its Functions and Its Prerequisites", 85th International Atlantic Economic Conference, At London, United Kingdom, June 2018, p: 1.

[14]Jeffrey H. Matsuura, "The effect of digital currency on traditional currency (money) regulations", translation and research: Saeed Siah Bedi Kermanshahi and Reza Mohebi, Fars Law Research Quarterly, No. 2, Spring 2018, p. 126

[15]Jeffrey H. Matsuura, "The effect of digital currency on traditional currency (money) regulations", translation and research: Saeed Siah Bedi Kermanshahi and Reza Mohebi, Fars Law Research Quarterly, No. 2, Spring 2018, p. 126

execution. In the case of opening accounts and providing services to natural and legal persons, monetary and banking institutions must comply with special regulations, which failure to comply with these regulations will result in financial and disciplinary fines, depending on the case, and in some cases, cancellation of the license of the offending institution. Customer identification guidelines (KYC) and adequate customer identification (CDD), keeping records and transaction information and reporting suspicious transactions (STR) are among the things that should be done in order to prevent as well as ease and accelerate the detection and prosecution of crimes. According to Article 5 of the Anti-Money Laundering Law, all owners of non-financial businesses and non-profit institutions, as well as natural and legal persons, are required to authenticate and identify clients, submit reports of suspicious banking, registration, investment, exchange, brokerage and similar transactions or operations. Maintain records related to client identification, owner, account records, operations and internal and external transactions. Despite the aforementioned laws and regulations and many other similar laws, it is not possible to implement any of the mentioned cases in virtual currencies due to the lack of a central custodian and supervisor and peer-to-peer architecture. People can create a user account from anywhere in the world without the need to visit a bank or financial institution in person and register their information and identity details. No person is obliged to authenticate and check the competence and correctness of users' information. Basically, in virtual currencies, because the verification of transactions is based on mathematical formulas and cryptographic algorithms, and its purpose is to preserve the privacy and anonymity of individuals, authentication of individuals is irrelevant.[16]

On the other hand, it is not possible to apply supervision and restrictions such as checking the citizenship of individuals, the amount of funds allowed to transfer or deposit and withdraw, the country of origin or destination, reporting suspicious transactions and blocking the accounts of individuals; Because all financial operations are out of the official monetary and banking system as a vital point, and no information system related to transaction records, interception code or identification and characteristics representing the identity of persons is available to supervisory institutions for their review and control. In other words, virtual currencies have abandoned the laws related to the banking system and the fight against money laundering. Currently, Japan has developed regulations for virtual currency exchange service providers. According to these rules, buying and selling virtual currencies or converting them into other virtual currencies; Intermediation, brokerage or brokerage of virtual currencies to buy, sell or convert them; Management of users' money or virtual currencies in relation to their purchase, sale or conversion, as well as mediation, brokering or brokerage for users' virtual currencies, is known as virtual currency exchange services, and a license must be obtained to perform them. Imprisonment and monetary fine, as well as cancellation or suspension of all or part of the activity of the exchange, are the guarantees of executions that will be applied to related parties in case of violation of the relevant regulations.[17]

Executive challenges in proceedings in general, crime detection that includes interception, discovery, and the study of evidence in the field of cybercrimes It faces very different challenges compared to normal crimes. Although these challenges are obvious in the detection of cyber crimes, they are associated with more challenges in the money laundering crime, whose traditional model is also associated with many difficulties compared to other crimes. In the following, the implementation challenges are addressed, which are the same challenges related to the implementation of the judicial process and criminalization of crimes related to cryptocurrencies through encrypted currencies.

Pre-trial challenges One of the main challenges facing the criminalization and prosecution of cybercrimes is the lack of ease in determining the jurisdiction in which the crime occurred. Although this problem mainly exists in cyber crimes, in such a way that a person can commit a crime in a region on the

[16]See: International Standards for Combating Money Laundering and Financing of Terrorism (The Forty Recommendations of the Financial Action Task Force (FATF)) Translated and Compiled by: Zare Qajari, Ferdous; Qaim Maggi, Ali. First Edition. Tehran, Tash Publishing House, 2013.

[17]Mai Ishikawa, Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case; Journal of Financial Regulation, 2017, p: 129.

other side of the globe by using a computer and the Internet. In other words, the criminal act occurred in one jurisdiction and the result of the crime is realized in another jurisdiction. This causes serious problems in the investigation, finding evidence and finally determining the competent court to deal with the crime. The challenges that are related to the criminalization of crimes related to crypto-currencies and are related to pre-trial are the detection and prosecution of crimes related to crypto-currencies, the confiscation and seizure of virtual currency and the protection of seized virtual currency, which are listed below. They are reviewed.[18]

A- Discovery and prosecution of crimes related to cryptocurrencies The discovery and prosecution of crimes, which are carried out by judicial officers and under the supervision and training of judicial authorities, are considered to be one of the most important stages of criminal proceedings. The accuracy, speed and correctness of officers' performance can speed up or slow down the progress of the next stages of law enforcement and judicial proceedings. The security forces in general and the police in particular are at the forefront of fighting and detecting cybercrimes. Criminalization of cybercrimes is much more complex than normal crimes, and the police, as the responsible institution in detecting crimes in this area, needs to synchronize its technical knowledge with technological advances. Although each country should take into account its own conditions to plan to strengthen the ability to fight against cybercrimes, including crimes caused by crypto-currencies, and of course, different countries do not have the same capabilities, and policies should be tailored to Apply the specific capacities of their country. In addition to the efforts to strengthen the police capabilities, there are specialists outside the security institutions who have rich experiences in the field of cryptocurrencies, but there is a lack of communication between them and the relevant officers in this field who may not have sufficient skills or at least the necessary mastery of the mechanism. They do not have cryptocurrencies in order to prevent crimes by means of cryptocurrencies.[19]

B- Virtual currencies have a completely digital nature and do not have any real and physical effects and signs outside the virtual space. In addition, due to the newness of this phenomenon, the judicial officers do not have the necessary knowledge about the working method and technical subtleties of virtual currency. This issue causes new challenges to appear in the stages of discovering and prosecuting crimes. Due to the transparency of distributed ledger technology (public block chain), it is possible to view all virtual currency transactions, and regulatory and law enforcement agencies can monitor them. In other words, in order to solve this problem, considering that the financial transactions suspected of money laundering or the existing reasons and evidence may be from outside the territory of the country that is being prosecuted, international cooperation is inevitable. The global approach to cryptocurrencies is not necessarily negative, but it is considered to have many economic benefits, but the limitations that exist at the national level for a single country require international cooperation to reduce the use of cryptocurrencies as It makes a tool for money laundering necessary, these collaborations should not create a restriction on the legitimate use of these currencies. International cooperation can be done through various channels, including bilateral or multilateral international treaties, as well as following the frameworks proposed by the International Police in order to create coordination and unanimity in the fight against money laundering through cryptocurrencies.[20]

But the main challenge is how to determine and detect suspicious transactions in virtual currencies and identify its parties. As mentioned earlier, each transaction is linked to a cryptographic code, called the public key. The only possible way to discover the identity of users is the use of complex technical methods of network analysis and the use of information sources, and it is not

[18]Senthilkumar Arun and Graham Naomi, Cryptocurrency Law Enforcement Challenges and Opportunities. A Risk Perspective, Australia &. New Zealand Society of Evidence Based Policing3, 2018, p: 11.

[19]Kethineni, Sesha,; Cao; Ying, Cassandra, Dodge, Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes; Southern Criminal Justice Association, 2017, p: 153.

[20]Nigh, B & Pelker, C (2015, September 8), Virtual Currency: Investigative Challenges and Opportunities, Viewed 19 March 2018, p: 8.

possible to discover crimes related to them without using advanced technical methods. In addition, it should be kept in mind that people can use multiple addresses (public key), which makes the process of discovery and tracking very complicated and practically impossible. Considering that the degree of anonymity of individuals depends on their skill level in using double anonymizing methods and tools, therefore, the detection and identification of professional criminals is much more difficult and costly than ordinary individuals. Another related challenge in this field is the lack of face-to-face relationship in the use of virtual currencies. Considering that in some new payment methods, the user acts anonymously, the combination of using virtual currencies and new payment methods makes it difficult to identify, track and prosecute the accused. The mentioned cases are among the challenges that judicial authorities and law enforcement officers face in the phase of identifying and discovering crimes related to virtual currencies.[21]

In the field of block chain analysis, as well as helping to expand the use of investigative tools in criminal cases, which is proposed by the International Police Innovation Global Forum (IGCI), is an analysis framework and software system that is based on three The basic axis is based on: cataloging, analysis unit (scale) and web relations (global information network) and their task is to review, record and record transactions and also find behavioral patterns among them, the results of this analysis Finally, it is categorized into four groups: 1-Statistics related to the activity of a certain address 2- A diagram between various transactions and the addresses of bitcoins 3 - The transaction path related to the address of each bitcoin 4- A category that contains the addresses of all bitcoins that belong to a similar wallet. In this regard, in December 2017 in the city of Vienna, Austria, a training program was held in the field of investigations related to crimes caused by crypto-currencies, especially money laundering and terrorist financing, under the supervision of the United Nations Office for Combating Crime and Narcotics. According to the report of this organization, official representatives from financial and security intelligence units related to financial crimes from different countries, including the Islamic Republic of Iran, also participated in it; The focus of the program was on raising awareness of the dangers of Bitcoin misuse, as well as investigative and criminal investigation techniques related to money laundering through cryptocurrencies. The result is that, despite the specific limitations and capabilities of each country, it is necessary, considering other characteristics of crimes related to crypto-currencies, which indicate the need for international cooperation in the fight against such crimes, international training and exchange of experiences between The police and the institutions involved in this matter should be expanded in different countries, because it can facilitate the future path in dealing with the increasing volume of money laundering through cryptocurrencies.[22]

C- Confiscation and confiscation of virtual currency In cases where foreign currency is a means or subject of a crime, it should be seized or confiscated according to the laws. According to Note 2, Article 3 of the Anti-Money Laundering Law: "All instruments and devices that are used in the process of money laundering crime, or acquired as a result of the crime, or during the commission of the crime, are used or allocated for use at any stage of prosecution and investigation. If it is found that the owner knows about the criminal intent of the perpetrator, it will be confiscated..." According to Article 9 of the same law: "The original property, income, and proceeds from the commission of the crime of origin and money laundering crime (if there is no such thing or price) of the perpetrators of the crime Money laundering will be confiscated" and in the continuation of the note of the same article: "If the proceeds of the crime are converted or changed into other property, and if it is transferred to a third party in good faith, its equivalent will be confiscated

[21]Kethineni, Sesha,; Cao; Ying, Cassandra, Dodge, Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes; Southern Criminal Justice Association, 2017, p: 153.

[22]UNODC, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, 2014, p: 45.

from the perpetrator's property." According to Article 5 of the Law on Combating the Financing of Terrorism, the judicial authorities and judicial officers under the supervision and training or the order of the judicial authority are obliged to perform the following actions as the case may be: A- Identification, discovery and blocking of the funds used or allocated To finance terrorism and the proceeds obtained from them. B- Identification and confiscation of property subject to the crimes mentioned in this law and their proceeds, which have been completely or partially converted into other property and have changed status. C- Confiscation of the property and proceeds of the crime that are mixed with legal property in such a way that the said property can be confiscated in the estimated amount. - Note: The persons subject to this article are obliged to freeze the funds and confiscate the properties of individuals, groups and terrorist organizations, as well as persons subject to the Anti-Money Laundering Law, according to the order of the judicial authority. B- Confiscation and confiscation of virtual currency In cases where foreign currency is a means or subject of a crime, it should be seized or confiscated according to the laws. According to Note 2, Article 3 of the Anti-Money Laundering Law: "All instruments and devices that are used in the process of money laundering crime, or acquired as a result of the crime, or during the commission of the crime, are used or allocated for use at any stage of prosecution and investigation. If it is found that the owner knows about the criminal intent of the perpetrator, it will be confiscated..." According to Article 9 of the same law: "The original property, income, and proceeds from the commission of the crime of origin and money laundering crime (if there is no such thing or price) of the perpetrators of the crime Money laundering will be confiscated" and in the continuation of the note of the same article: "If the proceeds of the crime are converted or changed into other property, and if it is transferred to a third party in good faith, its equivalent will be confiscated from the perpetrator's property." According to Article 5 of the Law on Combating the Financing of Terrorism, the judicial authorities and judicial officers under the supervision and training or the order of the judicial authority are obliged to perform the following actions as the case may be: A- Identification, discovery and blocking of the funds used or allocated To finance terrorism and the proceeds obtained from them. B- Identification and confiscation of property subject to the crimes mentioned in this law and their proceeds, which have been completely or partially converted into other property and have changed status. C- Confiscation of the property and proceeds of the crime that are mixed with legal property in such a way that the said property can be confiscated in the estimated amount. - Note: The persons subject to this article are obliged to freeze the funds and confiscate the properties of individuals, groups and terrorist organizations, as well as persons subject to the Anti-Money Laundering Law, according to the order of the judicial authority.

D- Due to the anonymity they provide, virtual currencies can be used to hide the origin of money by converting to or buying other virtual and real currencies. Likewise, investing in virtual currencies can generate more income due to the increase in the price of virtual currency or the extraction of new currency. In discovering and prosecuting crimes related to virtual currencies, especially money laundering and terrorist financing, it seems difficult to distinguish whether virtual currency should be confiscated as a means of committing a crime or the proceeds of crime. Although in practice, this issue does not have much effect on the manner and methods of their seizure and confiscation. On the other hand, the nature of virtual currencies is such that they present a different image of themselves. For example, Bitcoin itself does not exist in any form, not even as a digital file; In fact, they are just records of different transactions between different addresses that regulate the increase and decrease of account balances. Therefore, if virtual currency is considered as a means of committing a crime or the proceeds of a crime, it cannot exist physically on a specific device or place. Considering that Aruzmazi has a direct relationship with a specific address that has effective control over them, Aruzmazi can only be seized by accessing the wallet or its encryption code.[23]

[23]UNODC, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, 2014,p: 55.

Virtual currencies do not have a fixed location. Unlike centralized computer networks that have a central server, virtual currencies operate based on a distributed network, which uses the computing and software power of groups. Unlike centralized networks, which can be stopped through the coercion of the central managing body or physical access to the location of the central hardware, this is not possible in virtual currencies due to the distributed structure. In addition, what is noteworthy is that it is not possible to block or prevent the transfer of virtual currencies due to the decentralized nature and lack of a responsible institution. However, as a solution in this regard, both executive bodies and exchanges can use effective tools to track dirty money. If a user's bitcoin wallet is stolen, he can go to the police and report it. Stolen assets are fully traceable through blockchain and whenever someone tries to deposit them in the stock exchange, they can be seized, which depends on the establishment of a specific law in this field in the country.[24]

E- Protection of confiscated virtual currency In some countries where the national currency is subject to instability, individuals and businesses may decide to use other virtual currencies, especially Bitcoin, as a tool to store economic value. People want to protect their economic assets in such a way that the value of those assets is also maintained. If the national currency is subject to rapid depreciation, it will quickly cause citizens and businesses to lose significant value. In such a situation, if digital currency provides a more stable value, they may prefer to have digital currency. Accordingly, in order to be considered as an alternative to established (currently existing) currency, virtual currencies should be widely accepted and easily convertible. Digital currencies are only accepted by individuals and businesses when they are used for a wide range of transactions. In addition, a virtual currency should be easily converted to traditional currencies. Therefore, without providing such conditions, individuals and businesses will not want to keep digital currencies. One of the fundamental elements of the value of a virtual currency is its ready conversion to the national currency of the country and to the currencies of other countries. Some economists believe that a significant part of the value and potential appeal of virtual currency is its conversion into foreign currency. One of the main challenges of the bailiffs and judges is the maintenance of confiscated property. Virtual currencies do not exist in physical form, and holding them presents unique challenges. If the virtual currency is confiscated, its storage has its own requirements[25]. The judicial officers must transfer the virtual currency to a digital wallet belonging to the judiciary or the police to be stored in it. The wallet belonging to legal entities and its private key must be protected using technical methods so that it is not stolen and protected from any manipulation. Obviously, considering the wide variety of virtual currencies and virtual wallets, how to choose the best and safest wallet should be determined by experts in this field. Also, measures should be taken to eliminate the possible abuse of responsible persons. In addition, the change in the price of virtual currencies during the storage period and how to sell confiscated virtual currencies are also issues that need to be investigated.[26]

Challenges during the proceedings Among the challenges that exist regarding cryptocurrencies and are related to good justice, one can consider the use of electronic evidence and the citation of these evidences in relation to crimes related to cryptocurrencies and competent authorities dealing with these types of crimes due to their transnational nature. They and their extent are mentioned below. A- Use of electronic evidence In forensic science, the crime scene plays a very vital role.

[24] Tara Mandjee, Bitcoin, its Legal Classification and its Regulatory Framework, Journal of Business & Securities Law,p1, 2019, p: 16.

[25]Jeffrey H. Matsuura, "Effect of digital currency on traditional currency (money) regulations", translation and research: Saeed Siah Bedi Kermanshahi and Reza Mohebi, Persian Law Research Quarterly, No. 2, Spring 2018, p. 142.

[26]Article 36 of the regulations on the collection and citation of electronic evidence: "Officers and persons who, according to the law, are authorized to collect, inspect, store, preserve and transfer data and computer or telecommunication systems, in addition to changing the price of virtual currencies during the storage period and The method of selling confiscated virtual currencies is also one of the issues that need to be investigated.

In crimes outside the cyberspace, due to the presence of material and physical reasons, the investigation of the crime scene helps to continue the investigation and detection of the crime. However, in cybercrimes, due to the lack of or difficulty in preserving the crime scene, the process of investigation and investigation may face problems. In other words, in cyber crimes, preserving and investigating the crime scene is completely different and requires special expertise and training for this type of crime. In other words, unlike the traditional and physical evidence that is provided in a criminal activity and can include physical documents and evidence, witness testimony, video, photos, etc., electronic evidence is formed in the virtual space and must be found in this environment. and with electronic tools such as computers and related devices. Electronic hardware and software systems and devices can include a wide range of computer networks, mobile phones, data storage devices, cloud storage spaces, the Internet, etc. in terms of the technology used. All of the above may be used in the process of creating and storing information that can be cited as evidence. Basically, virtual currencies work online and all transactions are based on the network of computers and data. Therefore, in crimes related to virtual currencies, most of the related reasons are electronic and no physical documents are available; Except in limited cases where virtual currencies have been converted into real money through a legal entity that is required to record and maintain records, or vice versa. Therefore, it is very difficult to record and record the activities that take place through cryptocurrencies and to document them, therefore, in order to present reasons in court and prove the accusation, measures should be taken to increase the capabilities of obtaining evidence and documentation. to be In explaining this issue, it should be acknowledged that the difficulty of tracking and discovering evidence in virtual currencies is such that only experts can handle it. If the accused has used anonymizing tools or virtual machines, the discovery and identification of virtual currency or its use cannot be easily documented. However, the transactions recorded in the block chain are immu Electronic evidence, especially in the case of virtual currencies, is subject to change and highly volatile. Because the codes related to virtual currencies are a number of numbers that occupy very little space in the virtual space, so they can easily be hidden in the smallest storage space. If the personal computer of the suspect or the accused is confiscated, the necessary measures must be taken to obtain the reasons immediately[27]. Stored information may be lost due to updating software or deleting previous data and registering new data in computer systems. If the criminal has a high level of expertise, he can use special software to delete the data in the computer at specific intervals so that access to them is not possible. Due to the need to preserve the integrity and integrity of electronic evidence and to assign an anonymous electronic signature to the accused person, the collected information must be in accordance with the general principles related to the reason and method of its study in criminal matters, as well as in accordance with the citation of electronic evidence. This issue is important for judicial officers and other law enforcement agencies, because technical measures and specialized methods must be used to obtain evidence, maintain and present it in necessary cases.table and therefore referable. But the main issue is how to prove and assign them to a certain person, considering the anonymity of users and transactions.[28]

F- Competent authority to deal with cryptocurrency crimes Among the important issues that can be discussed in the face of virtual currency is the jurisdiction of the courts dealing with crimes related to cryptocurrencies; Virtual currencies operate in an online environment that has eliminated national boundaries and turned e-commerce into a global phenomenon. One of the main challenges in this regard is determining the jurisdiction to recover the proceeds from crimes related to virtual currencies. In other words, one of the main challenges regarding the damages caused by virtual currency crimes is the possibility of prosecuting the perpetrators of these crimes

[27]Najabati, Mehdi, Scientific police (scientific crime detection), Tehran, Samt, 16th edition, 2014, p. 145.
[28]UNODC, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, 2014, p: 60.

and dealing with their charges as well as compensating for the damages caused by the crime. To deal with these crimes and take appropriate decision; Obviously, this issue can directly overshadow international security in the economic field and even diplomatic relations; However, due to the lack of criminalization in the field of domestic and international law, at least until the time of international law, it is cause for consideration in a competent court; Because it is possible that any operation of opening this conversion account or currency transfer can be done anywhere on the planet, and because sometimes the origin of this operation cannot be traced, or because some countries do not interact with each other and provide judicial assistance on the assumption of traceability, and even some others from the countries that are in hostilities and in the case of committing some of the elements of this crime in the territorial jurisdiction of these countries and their non-cooperation will cause the arrest of the accused, prosecution, investigation and also the handling of their accusations will not be realized; On this basis, it is necessary to organize international regulations or multilateral treaties between countries to grant global jurisdiction to deal with such crimes and to compensate damages caused by committing crimes related to cryptocurrencies. Based on this, in the domestic law, Article 118 of the Criminal Procedure Law stipulates: "When the traces and evidence of a crime are discovered in the jurisdiction of the investigator's mission, but the place of occurrence is not known, the investigator, while conducting the investigation, will try to discover the place of occurrence. commits a crime and if the location of the crime is not determined until the end of the investigation, the investigator will express his opinion on the matter." One of the cases where the location of the crime can be unknown is the crimes related to virtual currencies that are committed in the cyber environment without a known physical and central location. In these cases, if it is possible to identify and determine the geographic location of the hardware carrying the virtual wallet, the location of the wallet can be considered as the crime scene. Because the control of virtual currencies is done through the wallet. In addition, regarding the arrangements that should be made for international cooperation, it is necessary to determine the competent jurisdiction.[29]

conclusion Virtual currencies as a new phenomenon in the virtual space are accompanied by profits and losses. Increasing speed, reducing cost, increasing privacy and ease of use of these currencies have made them popular and prosperous. These currencies generally include two categories of centralized and decentralized virtual currencies (virtual currency for buying virtual goods and services, virtual currency for buying goods and services in the real and virtual world, virtual currency for buying goods and services in the virtual world and providing money in the world real and virtual currency with two-way conversion and the possibility of use in the real world). Virtual currencies include cryptocurrencies, which at the internal level of these cryptocurrencies include global currency, central (national) bank currency, regional currency, and cryptocurrency from initial coin/token supply. In this regard, the most important cryptocurrency is Bitcoin, which is in the world's cryptocurrency category; One of the unique aspects of Bitcoin and other virtual currency systems is the fact that individuals and organizations can directly participate in the creation and use of those systems without relying on intermediaries. However, due to anonymity and the lack of a central institution to monitor and enforce laws, it has become possible to use Bitcoin in criminal activities.

The expansion of cryptocurrencies in Iran revealed the need for legal activism around various aspects of this technology; Although it started with adopting passive approaches, it is moving behind many countries towards relative changes. The most important aspect of legislative interventions in Iran can also be seen as the criminal intervention in this area, which was trying to consider cryptocurrencies as currency, unlike many countries, instead of prioritizing criminal legislation in this area within the framework of the regulations to deal with crimes related to cryptocurrencies, including money laundering.

[29]Naderi, Shima; Melabi, Majid, "Investigation of legal solutions for mining and trading of digital currencies and basic (virtual) code: legal gaps and suggested solutions" Journal of Legal Civilization, Volume 4, Number 9, Autumn and Winter 1400, pp. 12-13

take into consideration, choose a different procedure by smuggling it; Which could achieve the goal of managing the criminal risk of cryptocurrencies without creating such a complex structure and simply in the light of anti-money laundering regulations. In fact, it seems that there is no need to identify cryptocurrencies as a foreign currency, which has not been done in practice by any country. The majority of countries that have dealt with cryptocurrencies and legislation have identified this technology as a financial value or asset and not money or foreign currency; In this framework, by legally identifying the service providers related to this technology and trying to include some requirements regarding them, they have prepared the ground for regularization of this field; This makes sense in the framework of the theory of replacing virtual currencies with the existing monetary system. It should be noted that global cryptocurrencies such as Bitcoin, although they have many advantages, they still have a great challenge; In other words, the advancement of information and communication technology and the creation and development of technological tools in cyberspace have created many challenges for policy makers and legislators. In addition to the political and economic dimension, these challenges also have extensive legal-criminal dimensions that have had significant effects on delinquency, which can generally be mentioned as legal challenges and executive challenges in the proceedings. . Legal challenges include things such as: the ambiguity of the legal nature of virtual currency, the unknown identity of the parties to the exchange of crypto currencies, the extent and decentralization and the quality of the application of laws and regulations of virtual currencies, and enforcement challenges in the legal process (before and during the legal process)) includes cases such as discovering and prosecuting crimes related to cryptocurrencies, confiscation and confiscation of virtual currency, protection of seized virtual currency (challenges related to pre-trial) and the use of electronic evidence and the ambiguity of the competent authority to deal with cryptocurrency crimes (challenge) related during the proceedings). Therefore, the dominant effort of countries is to marginalize this technology and reduce its position as a value or asset; For this reason, this technology has not been given a value such as money or foreign currency in any country; Nevertheless, the policy adopted by Iran in identifying cryptocurrencies as foreign currency, although theoretically it will lead to the adoption of a strict criminal policy regarding them, but in practice it is not considered a suitable policy; Because on the one hand, the identification of this technology as a value was enough to be covered by anti-money laundering laws and to enable the requirements related to money laundering for users and related service providers; On the other hand, the identification of world-class cryptocurrencies without support and with very high price fluctuations, where there are new uncertainties regarding its creator, can be very effective in creating the desire of the general public to enter it; With the complexity of its buying and selling, due to the inclusion of foreign exchange laws and regulations, it can be the basis for the potential criminality of many people, which include crimes such as money laundering, financing of terrorism, smuggling of goods and currency, theft of virtual currency, fraud; In addition to these crimes, cryptocurrencies may make it easier to commit some crimes such as evading government taxes, blackmail, gambling and betting, and crimes related to bankruptcy. Nevertheless, therefore, due to the spread of such crimes, the need to criminalize cryptocurrencies is of particular importance, and these needs can include protective needs (supporting criminal justice in the form of effective prudence and supporting economic security) and He paid attention to preventive necessities (prevention for the purpose of globalization and prevention for the purpose of danger); Because crimes related to cryptocurrencies, due to their transnational nature and extent, cause crimes at the domestic and international level, and due to the dangerous nature of these crimes and the negative impact on the country's economy, they have adverse effects; However, Boddy admitted without hesitation that regulating these technological tools, such as Bitcoin, would present lawmakers with a tough test. A test that reveals serious limitations and even incapacity in the field of regulation, which can involve wide risks. Undoubtedly, the legislative approach in this field is not outside of two general policies. First, the strict policy and prohibition of any use of cryptocurrencies and the second policy, the drawing of a suitable and dynamic legal framework, which is called a risk-based policy. Strict policy and prohibition should be considered a failed policy; Because, on the one hand, virtual currency technology has positive functions, banning its use means denying the use of its advantages, and on the other hand, this approach will not have an effect on reducing criminal risks; Because the charms and unique features of virtual

currencies will be effective in attracting virtual criminals regardless of the prohibitions created. But the risk-oriented policy will also have many challenges; Because the main issue is that, in general, is it possible to deal with crimes related to cryptocurrencies as a policy or not? Undoubtedly, legislators can enact laws in this field, but the ability to implement them is a matter of reflection. The complexity of this becomes more visible especially when the use of virtual currencies is done in the dark platform of the Internet, i.e. the dark net. Therefore, it seems that the effort for legislation should give way to leadership and management in this field. Because the discourse of leadership and management, in addition to being compatible with the nature of the Internet space, gives order to the communication of actors in this space. This has been manifested in the field of financial-economic delinquency in the approach of risk management. Based on this, efforts are being made to prevent the occurrence of crime as much as possible by managing and directing the existing risks, and if it occurs, to detect it quickly. Prevention of financial-economic crimes in cyber space is also included in this strategy. Adopting a risk management policy against virtual currencies and including risk-based laws and trying to reduce the occurrence of crime should become the priority of criminal policy against this special form of virtual crime. Because the examination of the policy approaches of some leading countries indicates the selection of a risk-oriented approach in the framework of developing anti-money laundering programs to deal with risks. FATF's criminal approach to virtual currencies in the light of the transnational requirements of the special group of financial risk-oriented criminal policy in this field, including monitoring and control, obtaining licenses and registering activities, recording records and submitting suspicious reports, applying restrictions and other countermeasures and cooperation International is aimed at reducing the criminal risks of virtual currencies. Nevertheless, it is necessary for Iran's criminal policy makers to develop a coherent framework for preventing and dealing with criminal risks by choosing such an approach and creating the necessary legal structures and using the capacities of the anti-money laundering amendment law approved in 2017 and avoiding any passive approach. Pay virtual currencies. Based on this, in this regard, crimes related to cryptocurrencies can be prevented with social and situational prevention as a criminal solution; Regarding social prevention (development-oriented social prevention and community-oriented social prevention), it can be done by raising children properly in the family and correcting religious attitudes and beliefs both in this environment and in society, and raising the level of public awareness and improving economic conditions. Crimes can be prevented and in addition, at the level of situational prevention, it is possible to establish relevant laws for the purpose of adequate control and supervision of the government, recognition of legal exchanges, legalization of virtual currency by the legislature, creation of cryptocurrency (Bitcoin unit). Privatization and registration of Bitcoin ownership with insurance, which are all realized by government and private institutions, took action to deal with crimes related to cryptocurrencies.

References

1. Theft or Money Laundering?", Freedom from Fear, vol. 11, 2016.

2. Boehm F. , Pesch P. , Bitcoin: A First Legal Analysis. In: Böhme R. , Brenner M. , Moore T. , Smith M. (Eds) Financial Cryptography and Data Security. FC. Lecture Notes in Computer Science, Vol 8438. Springer, Berlin, Heidelberg," n. d, 2014.

3. Bohme, R. Christin, N. Edelman, B. & Moore, T. Bitcoin: Economics, Technology, and Governance. The Journal of Economic Perspectives, 29(2), 2015.

4. Brito Jerry and Castillo Andrea …. And Spencer E. Ante, Bitcoin Startups Begin to Attract. Real Cash, Wall Street Journal, May8, 2013.

5. Brown, SD,'Cryptocurrency and Criminality: The Bitcoin Opportunity', Police Journal: Theory, Practice and Principles, Vol. 89, No.4, 2016.

6. Cousy, H., The Precautionary Principle: A Status Questionis. The Geneva Papers on Risk and Insurance, Vol. 21, No. 79, 1996.

7. Doguet, J.,"The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System", Louisiana Law Review, Vol. 73, 2013.

8. EBA, Opinion on virtual currencies, European Banking Authority, 2014.

9. Edward V. Murphy, Bitcoin: Questions, Answers, and Analysis of Legal Issues, congressional research service,informing the legislative debate since 2015.

10. FATF , Virtual Currencies, Guidance for a Risk-based Approach.2015.

11. Freestone, D., The Precautionary Principle in International law and Global Climate Change. Churchill, R. and Freestone, D.(eds), London, Boston, Graham and Trotman/Martinus Nijhoff, 1991.

12. Goldman, Zachary; Maruyama, Ellie; Rosenberg, Elizabeth; Saravalle, Edoardo & Solomon-Strauss, Julia, Terrorist use of virtual currencies, CNAS Publication, Washington, 2017.

13. Guo, J. & Chow, A, Virtual Money Systems: a Phenomenal Analysis. In E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, 2008.

14. Hak J. Kim, Virtual Currency Is Becoming Reality: Is It Opportunity or Disaster, 16 J. Int'l Bus. & L. 75, 2016.

15. Hoyer Jessica, SEX TRAFFICKING IN THE DIGITAL AGE: THE ROLE OFVIRTUAL CURRENCY-SPECIFIC LEGISLATION IN KEEPINGPACE WITH TECHNOLOGY; 63Wayne L. Rev. 83, 2017.

16. Husak, Douglas, and Peter de Marneff, The Legalization of Drugs, Cambridge University Press, 2005.

17. Jareborg, Nils, Criminalization as Last Resort (Ultima Ratio), OHIO state journal of criminal law, 2004.

18. Kemshall, Hazel, Understanding risk in criminal justice, Open University Press, 2003.

19. Kethineni, Sesha & Cao, Ying. , The Rise in Popularity of Cryptocurrency and Associated Criminal Activity, International Criminal Justice Review,2019.

20. Kethineni, Sesha,; Cao; Ying, Cassandra, Dodge, Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes; Southern Criminal Justice Association, 2017.

21. Kfir, Isaac, Cryptocurrencies, national security, crime and terrorism, Comparative strategy, vol. 39, NO. 2, 2020.

22. Likhuta, Vlad, Bitcoin Regulation: Global Impact, National Lawmaking, fork log research, 2017.

23. Luttenbergerger, A., The Role of Precautionary Principle in Environmental Protection of Coastal Area. 22nd Biennial International Congress Tourism and Hospitality Industry: Congress Proceedings Trends in Tourism and Hospitality Industry, Opatija, Croatia, 2014.

24. Mai Ishikawa, Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case; Journal of Financial Regulation, 2017.

25. Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme", US Department of Justice, May 2013.

26. McLeod. S., 'Bitcoin: The Utopia or Nightmare of Regulation,' Elon L. Rev. , Vol. 9, 2017.

27. Mishkin, Fredrick S., The Economics of Money Banking and Financial Markets, Pearson Education, 4 th Edition, 2004.

28. Nigh, B & Pelker, C (2015, September 8), Virtual Currency: Investigative Challenges and Opportunities, Viewed 19 March 2018.

29. Omri Y, Marian, A Conceptual Framework for The Regulation of Cryptocurrencies, UF Law Faculty Publications, 2015.

30. Pacy, Eric P., "Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes", NEW ENG. L. REV. vol. 121, 2014.

31. Paz, M. C., Precautionary Principle: Case Law in Colombia. Journal of Civil & Legal Sciences, Vol. 3, Issue 1, 2013.

32. Rev, Charleston L., Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation, 8Charleston L. Rev. 511, 2014.

33. Ritzer, George, Encyclopedia of Social Theory, Vol. II, London, Sage publication, 2005.

34. Schneider, Friedrich, "Macroeconomics: The Financial Flows of Islamic Terrorism". In: Masciandaro D., (ed.) Global Financial Crime: Terrorism, Money Laundering and Offshore Center, Routledge, 2004.

35. Senthilkumar Arun and Graham Naomi, Cryptocurrency Law Enforcement Challenges and Opportunities. A Risk Perspective, Australia &. New Zealand Society of Evidence Based Policing3, 2018.

36. Sereda A.V. , Settlements using virtual currencies in the Russian Federation: analysis of the first law enforcement experience, Modern Lawyer, No. 2, 2017.

37. Tara Mandjee, Bitcoin, its Legal Classification and its Regulatory Framework, Journal of Business & Securities Law,2019.

38. Umlauft, Thomas S., "Is Bitcoin Money? An Economic-Historical Analysis of Money, Its Functions and Its Prerequisites", 85th International Atlantic Economic Conference, At London, United Kingdom, June 2018.

39. UNODC, Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies, 2014.

40. Valeriane , Elizabeth M., IRS, Will You Spare Some Change: DefiningVirtual Currency for the FATCA, 50 Val. U. L. Rev. 863, 2016.

41. Weinstein, J (2015, May 12), How Can Law Enforcement Leverage the Block Chain in Investigations? Accessed 11 February 2019.

42. Xiong, Wanting, Fu, Han, Wang, Yougui , Money creation and circulation in a credit economy, journal Physica A 465, 2017.

43. Yaga, Dylan and others, Blockchain Technology Overview, U.S. Department of Commerce, National Institute of Standards and Report Internal Technol, 2018.

Site Resources

1. https://darikland.com/.

2. Https://Egmontgroup.Org/En/Content/Financial-Intelligence-Units-Fius.

3. Https://Fincen.Gov/What-We-Do (Accessed 12 February 2019.

4. https://tipaxco.com/blog.

5. https://www.mehrnews.com/news/.

Copyrights