International Journal of Law and Public Policy
p-ISSN: 2721-6934, e-ISSN: 2721-6942

Research Paper

Criminal Liability for Crimes Committed Using Cryptocurrencies

Ameer Majeed Dahdouh Al-Alili[1*], Zaid Salam Abdullah[2]

[1] *College of Administration and Economics, University of Al-Kufa. Kufa, Iraq.*
[2] *Department of Legal Affairs, Nahrain University. Baghdad, Iraq.*

Article History
Received:
08.01.2026

Revised:
22.01.2026

Accepted:
05.02.2026

***Corresponding Author:**
Ameer Majeed Dahdouh Al-Alili
Email:
ameerm.alaliele@uokufa.edu.iq

Abstract: This research aims to clarify the actual works of criminal liability for crimes committed using cryptocurrency and to highlight the flaws of Iraqi legislation about this modern type of crime. Accordingly, an attempt has been made to analyse the elements, kinds, and difficulties of evidence, leading up to determining the legal system in which to protect from and suppress this type of crime, of which cyberspace is a part. This research is descriptive-analytical in nature, where legislation has been examined. The research indicates that the wide scope of risks involving cryptocurrency crimes makes it difficult to subject them to existing laws on movable property, especially since the legislator has omitted the criminalization of certain attacks like wallet hacking, while the sophisticated nature of making inquiries and collecting evidence complicates establishing a definitive link between the perpetrator and the transaction. All in all, this study finishes off with the need to develop or amend legislation to extend the definition of digital assets and criminalise attacks against them, strengthen investigative capacity in electronic tracking, establish units for cryptocurrency crimes, and regulate digital seizures and confiscation mechanisms. This further highlights the importance of modernising legislation in light of the criminal threat's cryptocurrencies pose to upholding economic and legal security.

Keywords: Blockchain Crime, Criminal Liability, Cryptocurrencies, Digital Assets, Iraqi Legislation.

1. Introduction

Cryptocurrencies represent one of the most visible aspects of the digital revolution we are experiencing in the modern world, Iraq included. Blockchain and encryption technologies led to the creation of fresh financial models based on decentralisation and independence from traditional banks. With its increased use, these currencies brought with them difficult legal questions about their nature and how to regulate and control them, lacking as they do an official issuing authority and a set of common laws. This has made its use shrouded in ambiguity for all involved on both a technical and legal level. Being based on disguising people's identities and allowing that trading can take place through these currencies via third-party platforms, often unsupervised by the laws of any particular country. Into this environment, various crimes using cryptocurrency are spilling over, either as new crimes or as new ways of committing old crimes. The Iraqi digital environment is rife for money laundering, cyber fraud, and digital extortion, avoiding payment of debts, and funding illicit activities. The main problem is really one of complexity: many crimes are executed through interconnecting networks, committing them often across international jurisdictions, which clutters investigations and evidence gathering, militating against jurisdiction, and forcing a consideration of the bounds of criminality.

With the growth of encryption and blockchain, the question of criminal liability for crimes committed using cryptocurrencies is not incidental to contemporary discourse; it is the priority. Given the difficulties it raises for legally classifying criminal conduct, identifying perpetrators and accomplices, and the connection between digital acts and criminal outcomes. Legislators and the judiciary are called upon to answer how to prosecute perpetrators of these acts in the manner most unobtrusively and smoothly possible. The problem is that the digital environment provides users with a far-reaching ability of concealment and rapid movement from one platform to another. Tackling the question of criminal liability in this context could benefit from a more complete awareness of the technical nature of cryptocurrencies and their mechanisms of use, and legal awareness of the risks arising from a lack of oversight.

The problem that this research seeks to address is that our Iraqi legal system, in its original concept, was not formulated for crimes committed through the cryptocurrency procedure. In the absence of legislation regulating the use and the nature of the currency, it becomes difficult to determine the appropriate classification for what are considered related criminal acts. In addition, the decentralised scope of cryptocurrencies, difficulty in tracking them, and anonymity of users create hurdles in establishing proof, ascertaining responsibility, and reaching the punitive provisions supplied by the legislature that, in certain ready-made texts, have not provided for ongoing raised procedural matters. Thus, this research seeks to answer the question: “To what extent do the rules of criminal liability in Iraqi law apply to crimes committed using cryptocurrencies, and what are the legal and procedural foundations that can be adopted in dealing with such crimes in the absence of legislation” The importance of the research: The importance of this research is because, at a time when dealing with cryptocurrencies and legislating against their use jurisprudentially has not yet developed enough, and there are no clear legal (legal) texts related to it, our Iraqi legislator has not been able to regulate the legal position due to the modernity of the subject and the difficulty of describing and determining his criminal position illustrates the legislative gaps in our criminal legislation. And reveal to us the difficulties faced by the investigative and judicial authorities in proving this crime and catching its perpetrators. Its significance also lies in attempting to find a legal framework that helps to perceive the criminal risks of the exploitation of cryptocurrencies, as well as providing a basis upon which legislators can issue future legal regulations, which will contribute to the strengthening of economic and digital security in Iraq and decrease the exploitation of the virtual environment to perpetrate crimes harmful to society and the state.

This research will depend on analysing the Iraqi criminal legislation in light of the birth of what is known as crimes committed using cryptocurrencies, and the extent could such provisions stand to fit this kind of emerging crime and to clarify the legislative loopholes that investigating and adjudicating authorities are facing concerning these crimes. Also, to clarify the technical and legal difficulties to verify and prove digital transactions, explain the nature of cryptocurrency, and its effect on determining criminal liability. Finally, to take what has been reached and to deduce some usable interpretation approaches or methods that would assist in the development of a methodology that protects Iraq from the hazards derived from the misuse of these technologies.

2. Literature Review

2.1. The Conceptual and Legal Framework of Cryptocurrencies

The conceptual and legal underpinnings include a range of general and specific concepts, including how crypto “is defined”, how they are “classified”, and how cryptocurrencies function as financial instruments. This section also illustrates the facial resemblance/difference that the technical characteristics of cryptocurrencies bear or fail to bear to traditional assets, and creates some examples of regulatory and legal challenges where an underlying characteristic would potentially implicate current Iraqi law.

2.2. The Nature and Technical Nature of Cryptocurrencies

Currency, by which we mean the legal form of circulating money, includes coins and banknotes. Historically, the term "currency" referred to various means of exchange, including precious stones and certain commodities such as tobacco, sugar, and others. It is the unit of commercial exchange and varies from one country to another. Currency represents a form that facilitates trade compared to the old world's system, based on the direct exchange of goods. The word "currency" comes from the word "transaction," and it refers to the form of money used in commercial transactions. This currency can be traded with other currencies in the foreign exchange market, thus giving it value relative to other currencies [1].

Digital currency is an electronic financial store of monetary value that can be used by entities other than the issuing authority. Technology is used in the creation of these currencies through hardware and software that store monetary value [2]. It is also known as electronic money, which is non-physical money in the form of electrons stored on a computer's hard drive in a location called an electronic wallet.

Financial and commercial transactions can be conducted online, including purchasing daily necessities and making payments, using electronic money [3].

Digital money is legally defined as electronically operated numbers, where each number represents a monetary value. These values are used to pay for products and goods purchased by consumers instead of physical cash. Debtors can use it to settle their debts, provided the consumer consents to its use and the merchant accepts it as a means of payment [4].

Therefore, virtual currency has acquired several names, including "cryptocurrency," "crypto-currency," "digital currency," [5] [6] "crypto-money," "digital money," and "electronic money." While some early Arab laws and legal scholarship adopted the term "virtual currencies," a debate arose among researchers regarding the distinction between these terms. "Cryptocurrencies" rely on encryption to secure and verify transactions and are decentralised, whereas "virtual currencies" are digital and do not require legal backing [7]. The researcher points out that this distinction cannot be rigidly defined, as all digital currencies are encrypted and do not represent a physical entity. Furthermore, digitisation and encryption encompass both electronic money and virtual currencies [8]. However, what distinguishes virtual currencies is their purely digital existence, lacking any representation of traditional money, making the term "virtual currency" more accurate and appropriate.

They have also been defined as encrypted digital units that do not possess a physical existence or intrinsic value, lack centralisation and a system of protection and oversight, and operate exclusively over the internet as a currency, according to the definition provided by proponents [9]. They have also been defined as (decentralised digital currencies in issuance, development, and control that perform credit functions) and as intangible, decentralised electronic currencies traded through internet platforms and networks, relying on encryption in their software system [10].

The researcher believes that encrypted or virtual currencies are encrypted digital units that do not possess a physical existence or independent intrinsic value, operate exclusively electronically over the internet, and lack centralisation and a traditional system of protection and oversight. These currencies rely on encryption to ensure the security and verification of transactions. They allow trading between individuals via digital platforms without the need for legal backing or a central financial intermediary, making the term "virtual currencies" the most accurate and applicable to their digital and virtual nature.

Examples of cryptocurrencies include:

- Bitcoin

International Journal of Law and Public Policy, vol. 8, no. 1, pp. 25-37, March 2026. DOI: 10.36079/lamintang.ijlapp-0801.1023

The most widespread and accepted cryptocurrency, it is obtained through mining according to specific mechanisms or purchased from specialised markets. It is characterised by a limited supply and is managed automatically through pre-programmed processes without a board of directors or a central authority. Transactions are final and cannot be reversed except by making a new transfer [10].

- Litecoin
  Similar to gold in relation to Bitcoin, it was created by Charlie Lee and is valued at around $60. It attracted widespread interest after mid-2018. It is characterised by faster transaction speeds compared to Bitcoin, despite the latter's higher price [11].
- Ripple
  Created in 2013 by OpenCoin, headed by Chris Larsen, with support from a large number of investors and international companies. Bitcoin is similar in that it is digital, limited in number, transferable, and mineable, and features digital security. What distinguishes it from others is the requirement to provide documentation to activate accounts and ensure the credibility of users [12].
- Ethereum
  This is an open-source software platform based on blockchain technology that enables smart contracts. It was created by Vitalik Buterin and launched in July 2015. It is characterised by having no fixed limit on the number of coins, its mineability, and a market capitalisation of approximately $27 billion, with significant liquidity available through its own digital wallet [13].
- Dash
  This is an open-source cryptocurrency that offers features similar to Bitcoin, in addition to instant and private transactions and decentralised management. It was created in 2014 by Evan Duffield under several names before adopting the name Dash. It is distinguished by its speed of transfer, which does not exceed three minutes, and the confidentiality of all transactions made through a masternode system, for which accounts cannot be tracked. These qualities have made Dash the seventh largest virtual currency in the worldwide market [14].
- Monero
  Created in 2014 by the mysterious “Nicola van Saberhagen,” it is notable for its privacy and decentralisation, where information on account and on balance is hidden automatically by the system without requiring user action. Its market capitalisation is about $1.25 billion with a circulating supply of almost 17 million units, putting it twelfth on the list [15].

3. Methodology

This research relies on a descriptive-analytical legal approach. It examines the relevant Iraqi criminal texts and how to apply them to those crimes committed using those currencies. It explains the technical nature of those currencies and their operating mechanisms, showing the technical problems affecting the aspect of determining criminal responsibility as well as the rules of collecting evidence. It uses inductive reasoning to reach possible ways to remedy those crimes and a legislative approach that suits them in the Iraqi society.

4. Finding and Discussion

4.1. The Legal Status of Cryptocurrencies in Iraq

Article 7 of the Central Bank of Iraq Law No. 56 of 2004 (as amended) gives the exclusive right to issue paper and coin currency for circulation in Iraq to the Central Bank, and labelling them the ‘National Currency’ placing it under guarantee of the assets of the Central Bank [16], while requiring the Bank to make arrangements for their issuance. From this, one can infer that in current legislation, there is no enabling authority for the Central Bank or any other to issue virtual/ cryptocurrencies since the wording is limited to ordinary coins and notes (i.e., paper currencies). Consequently, for an issuance of virtual currency to be permitted lex lata in Iraq, it would be necessary to amend the provisions of the law to widen the scope of the authority of the Central Bank or other competent bodies, so that it extended to the issue of digital currencies, and included them within the existing laws and regulations of the State.

Iraqi law recognises the freedom of the parties to choose the currency by which they will discharge their obligations [17]; however, the Central Bank of Iraq, on the 17th of May 2014, issued a circular, which encouraged all financial institutions to comply, prohibiting all dealings in Bitcoin and thus subjecting the violators to severe penalties. The Bank supported the prohibition because Bitcoin is a

currency that is not issued by a central Bank, falls within those provisions of the law concerning the aspect of money laundering, circulates beyond the territory of the monetary authorities, and is accompanied by risks of hacking and cyber fraud [18]. Further, a circular on the 3rd of October 2017 clarified that Bitcoin is just a virtual electronic currency with no physical existence, which could be used to purchase items online or converted to real currencies [19].

This circular further stated that being traded in bitcoins makes the customer liable to the Anti-Money Laundering Law No. 39 of 2015 and other relevant laws. However, the Bank has not taken a clear position on virtual currencies. It says that it does not have and will not have any desire or intent to issue or trade in digital currencies, a view that it would be correct to say simply reflects a lack of certainty or strategy concerning these currencies. The law technically provides for, i.e., freedom of choice. However, the Central Bank of Iraq has banned bitcoin and subjects those dealing in it to the anti-money laundering laws, with no clear position or official policy on it.

Consequently, simple currency has often been made the object of all kinds of crime committed against it. The Legislator then has to afford it appropriate protection, particularly against counterfeiting, or rather against the circulation of imitation or forged notes, enhanced that protection on account of those crimes, to which it might, in this respect, be exposed. The monetary institutions, or for the most part, the banks of issue of different countries, possess the exclusive right to issue the currency of the nation, and to protect it under the law. Nations, on the other hand, conclude treaties for the protection granted to them against crimes of this nature. Yes, every currency issued in opposition to the authority of these banks is considered a crime against which law-inflicted punishments [20] are denounced.

It is worth mentioning that the Central Bank has drafted a “Payments Law” [21] in which it emphasises its explicit right to issue digital currency. Thus, facilitating the way the bank could issue a virtual currency dreamed of appeared, once the law is approved, in this regard, the researcher suggests to the Iraqi legislature to choose the term “virtual currency” instead of “digital currency” because it is appropriate for these currencies. As for the position of the Iraqi legislator with respect to the act of issuance, he provides that whosoever issues: (a) a paper or metallic currency not issued in accordance with the provisions outlined in Paragraph (1) of Article (32); or (b) any other document or token currency intended to circulate within Iraq as money, in contravention of what is authorized by law, is guilty of a crime punishable by imprisonment not exceeding ten years [22]. One might suppose that Paragraph (b) includes virtual currency, as it is encrypted and digital, and that its issuance would be a crime if circulated within Iraq. Such a conclusion, however, is unsustainable, as it lies beyond the intent and contemplation of the legislator when the law was promulgated. Indeed, when the legislator spoke of "forged symbolic currencies," the intention was to refer to counterfeit stamps, forging postage stamps or other signs of a fixed value through fraud and deception, whether by any technical or rudimentary means, as well as genuine non-monetary paper and metal tokens [23]. Virtual currencies cannot be included in such a definition; this interpretation must therefore be rejected.

Thus, it can be stated that the Iraqi legislator has not criminalised the issuance and mining of virtual currencies [24], nor has any legal provision been issued by the Central Bank of Iraq that prohibits such acts. Otherwise, the circular issued by the Central Bank on May 17, 2014, which instructed licensed banks not to trade in Bitcoin in any shape or form, and the Securities Commission's warning issued through letter No. (121/7) on January 17, 2021, urging citizens to beware of brokerage financial investment firms that purport to engage in trading stocks and commodities, in addition to digital and foreign currencies. Such a letter is purely administrative 27.

Neither the Bank nor the Commission is entitled either to usurp the legislator’s right, and thus to limit the liberty of the subject in declaring what offences shall be crimes, and what punishments they shall be made liable to by the sole authority of law; and that would be to violate the principle of legality.

Since the above-cited circular was directed only at licensed banks in Iraq and only at one of the thousands of virtual currencies in existence, it cannot be interpreted as a general restriction on the issuance or mining of virtual currencies. At the same time, the letter from the Securities Commission is nothing more than a friendly warning to protect investors’ funds, something confirmed by the Central Bank´s latest initiative to launch a “Digital Onboarding” service, following a short statement published on the central bank’s website.

4.2. Crimes Committed Using Cryptocurrencies

This section captures those crimes carried out using a cryptocurrency, be it financial or digital, where the virtual aspect of the currency is exploited for crime, often exposing the difficulty of proof for the courts and for an investigator.

1) Financial Crimes Related to Cryptocurrencies

Money Laundering

The act of using illicit resources, whether in national or overseas territory, for legitimate uses, thus disguising the illegal source if intent accompanies, by getting into the economic projects, having pressures in them, and then allocating those resources gainfully to reinvest them as funds that have been legalised through this act. The money laundering has for target illicit funds produced for the markets from serious crimes like human trafficking or human organs sale, drug running, tax evasion, managing prostitution rings, illegal trafficking in weapons and nuclear materials, counterfeiting and forging currency, and other forms of contemporary organised crime [25].

The Iraqi legislator defines money laundering as a crime based on its material element, which refers to the physical acts committed by the perpetrator that constitute the basis for the crime. These acts include, firstly, the transfer, movement, or exchange of funds by a person who knows or should know that they are proceeds of a crime, to conceal or disguise their illicit origin, or to assist the perpetrator of the original crime or anyone who contributed to it in evading legal responsibility [26]. The material element also includes concealing or disguising the true nature, source, location, condition, method of disposal, transfer, ownership, or related rights of the funds, making it difficult for regulatory and judicial authorities to trace them, with the knowledge or having the right to know that they are proceeds of a crime. Furthermore, anyone who commits the crime by acquiring, possessing, or using funds, knowing or having the right to know upon receiving them that they are proceeds of a crime, is considered to be benefiting from the proceeds of illicit acts committed by others [27].

In general, the material element of the crime of money laundering focuses on the tangible criminal conduct related to funds obtained from crimes, whether through their transfer, concealment, or use, with the condition of knowledge or the obligation to know that they are illicit. This makes these acts criminalizable and punishable under Iraqi law.

The Iraqi legislator clarified that the funds subject to the crime of money laundering include all assets and properties obtained by any means, such as national and foreign currency, securities and commercial papers, deposits and current accounts, financial investments, and instruments and documents of all forms, including electronic and digital, in addition to precious metals, gemstones, commodities, and anything of financial value, including real estate and movable property, and the rights related to them, and any interest and profits arising therefrom, whether inside or outside Iraq, and any other type of funds that the Council specifies for this law and publishes a statement of which in the Official Gazette [27].

Accordingly, the Iraqi legislator divided the funds subject to the crime into two categories: the first is what the text explicitly defined, which included digital currencies, which are considered to be inclusive of virtual currencies, as evidenced by the legislator's intent from the phrase "(...including electronic or digital...)" [28]. The second part of the law was left to the Anti-Money Laundering and Counter-Terrorism Financing Council to define through an official statement published in the Official Gazette [29]. To date, the Council has not issued any statement regarding virtual currencies, which confirms what was mentioned in the first part of this paragraph and reinforces the opinion that these currencies should not be included among the current prohibited items without an explicit legal provision.

The mental element of the crime of money laundering is based on intent and criminal will. It is considered an intentional crime, requiring the perpetrator to be aware, or presumed to be aware, of the nature of the funds obtained from a crime, and to intend to commit the related act. The specific intent is to achieve the goal defined by the legislator, which is to use the funds to conceal or disguise their illicit origin, or to assist the perpetrator of the original crime or anyone who contributed to it in evading responsibility, thus achieving the legally stipulated criminal objective [29].

Crimes of Financing Terrorism

The Iraqi legislator defined the crime of financing terrorism as any act committed by any person, by any means, whether direct or indirect, and of their own volition, to provide, collect, or attempt to do

so, whether these funds are from a legitimate or illegitimate source. For the crime to be committed, the perpetrator must be aware that the funds will be used, wholly or partially, in carrying out a terrorist act, or by a terrorist or terrorist organization, whether the crime actually occurs or not, and regardless of the country in which the act takes place or in which the terrorist or terrorist organization is located [30].

2) Cybercrimes and Emerging Criminal Activities

Two Parties

As stated earlier, virtual currency or cryptocurrency is permanently exchanged between two parties directly involved in a transaction, rendering it virtually impossible to decrypt data while in transmission, a characteristic that differentiates it from electronic money. Swindles commonly conducted with electronic money by making a purchase with a credit card and then reneging on the debt or, making a transaction with a credit card and a second transaction of the same amount at the same time is not possible with virtual currency. A transaction cannot be completed unless the digital wallet has been loaded in advance with enough of the currency. The correct application of the transactions is performed by "miners," a process that prevents the same blocks of data from being validated twice. This is one of the benefits that distinguishes virtual currency over e-payment.

The actus reus (material element) of this crime requires that fraudulent means are used to obtain the handing over or transfer of possession of movable property of another party. Considering the hypothetical fraud scenarios in which virtual currency is used, one attempts a fraud against the underlying software system, while the other attempts to fraudulently use the victim's personal computer system, perhaps not involving a direct material loss for them.

The mens rea (mental element) of the fraud is based upon intention and wickedness; as a result, the crime cannot be proven unless such intent is shown to exist in the mind of the offender. This involves general intent as shown by knowledge of the act, and the desire to gain the property of another and also specific intent - the intent to gain possession of the virtual currency. In this area the offender desires to possess and utilize the currency with the knowledge and intention not to return it to its rightful owner.

The Crime of Electronic Theft

Electronic theft describes a series of acts performed to the end that a computer serving as the object of the crime or the tool used to perpetrate it, injures a rightful interest, whether material or not. Such crimes take many forms: the unlawful copying of data, particularly, data stored in the memory of a device attached to the same network as the thief's computer and copied after breaking through the security barriers, such as a numerical code or a password, or through an active software measure.

The material element (actus reus) of the crime of misappropriation is considered as comprising two components: the actual act of misappropriation and the fact that the owner has not consented to the appropriation. Having established the second component, the fact that the appropriation was without consent (whether in the context of simple theft or electronic theft) the enquiry is directed more closely at the first component, the act of misappropriation itself and to what extent that extends to virtual currencies. Misappropriation is defined as the seizure of property through any means that effectively transfers both its physical and intangible possession.

Misappropriation typically occurs in two scenarios: The first arises when the property remains in the owner's possession, whereupon the offender proceeds to transfer it into their own possession, as occurs, for instance, when an owner's electronic wallet is breached, and the virtual currency is transferred to the offender's wallet with the intent to exercise full proprietary rights over it. The second scenario occurs when the offender holds only limited or partial possession of the property, yet subsequently alters their intent to one of full ownership, such as when an employee of a company or a digital platform transfers wallet codes or private keys to their own digital wallet (or to that of a third party) with the specific intent to steal the associated assets. However, he exercises control over it as if he were its owner. In all instances, cyber-theft is perpetrated solely through the unauthorised or, in some cases, authorised breach of an electronic wallet. This issue of unauthorised access has been addressed by the Iraqi legislator in the draft Law on Combating Cybercrimes; however, this legislative treatment in no way removes the need to expressly criminalise the cyber-theft itself, bearing in mind that the access to another's property is an aggravating factor for theft and that theft entails the act of unauthorised entry in itself. It may thus be said that the appropriation applies to the v.c. currencies as

much as to any other form of property; the actus reus (material element) of the crime is perpetrated from the moment the v.c. The currency is hacked, and the owner's electronic wallet is compromised.

Returning to the mens rea (mental element) of the crime of misappropriation, it consists essentially of the accused's specific intent to take possession of the property for himself permanently, a constitutive elements of all crimes of theft or larceny, for which there must be first the general intent, as indicated by the offender's knowledge of what he is doing, and the specific intent, indicated by his intention to acquire ownership and permanent dominion over it. To comprehend the full import of this element, recourse might be had in a treatise on the subject of Special Criminal Law to some of the commentaries and works of those authorities devoted to crimes of theft and misappropriation.

3) Criminal Liability and Evidentiary Challenges

The immensely important and difficult topic of liability for crimes committed in connection with cryptocurrencies, and, particularly, the evidentiary difficulties around such crimes. The problem arises because the digital currency is encrypted, which makes it very hard to track transactions. The importance of this section lies in explaining the difficulties, both technical and legal, faced by the police and the courts in trying to piece together the facts of the case and link them to the suspects.

The Legal Characterisation of Criminal Liability for Crimes Committed Using Cryptocurrencies

Iraqi law prescribes prison for a term not exceeding fifteen years and a fine not less than the value of funds constituting part of the crime, not exceeding five times that value. This allows enough room for the courts to ensure that penalties are proportionate to the scale of the criminal profits that have been made. Applying those provisions to crimes that are committed using cryptocurrencies, those cryptocurrencies are considered by those courts to be on a spectrum of "digital assets" with a financial value that can be traded, whether they be virtual currency or encrypted currency, as secondary instruments used to embed intent or not. They are subjected to anti-money laundering rules because the legislator has defined "digital asset" as a property for offences.

More specifically, the actus reus (material element) of the crime of terrorist financing consists of the overt acts of the accused in the form. of providing or collecting funds with the intent that they be used, whether wholly or in part, to support the criminal enterprise. The Iraqi legislator has restricted the offence to these two forms of conduct. The terrorist organisation ISIS has issued virtual currencies as a vehicle to finance its operations; it solicited donations in Bitcoin and justified this as the most preferred means of hiding the movement of its money. The mental element of the crime of terrorism financing is based on intent; indeed, this crime was an intentional crime which consists of the presence of general intent, that is, the awareness of the accused that his act is unlawful and is done of his own free will and volition. It is also necessary for the offender to hold a specific intent, given that an offender must also intend to furnish terrorist organisations or a particular terrorist enterprise funds to facilitate the attainment of their criminal aims and ventures.

The penalties that are provided by the Iraqi law for terrorism financing cases are those which would be attached to an eventuality where virtual currencies are being used for the crime to be achieved. Under the Counter-Terrorism Law No. 13 of 2005, the penalty can be capital punishment or at least life imprisonment; whereas the Law on Combating Money Laundering and Terrorism Financing No. 39 of 2015 provides for life imprisonment only. The last law, being the most recent and particularly dedicated law related to offences against financial and terrorism crimes, is the most likely to be employed. And more because the penalty it has inscribed is lighter than that of the previous law, thereby giving effect to the guarantee of the rights of the accused.

In its enactment, the application of such provisions to crimes perpetrated through the use of cryptocurrency is accepted as the method of collecting or transmitting property which is to be expended for an enterprise of terrorism, wherein the perpetrator acts with the requisite intention; it falls clearly within the two elements, both material and mental, of the crime as defined by law. However, under the provisions in respect to the reporting of criminal conspiracy or intimate details of co-conspiracy, to which court may grant exemption from punishment or pardon as an adequate reward for information rendering possible the apprehension of the criminal and the confiscation of the property for a crime for which the passbook of this life has been the passbook of this life. In this manner, the law flexibly addresses the cryptocurrencies' associated crime and makes possible its legal definition and treatment on the same fundamentals as would monetary property.

Additionally, the penalties competitors would be liable to spontaneously compensate Iraqi fraud for the crimes that would be presented under Iraqi law. Crimes Committed Through Virtual

Currencies: As the provisions of general legal principles did not cover cases of fraud carried out through said currencies, the anti-cybercrime law proposed was presented to prescribe penalties consisting of temporary imprisonment lasting from more than five years up to fifteen years, as well as a fine ranging from ten million to thirty million dinars.

This law seems appropriate in the classification of crimes committed using cryptocurrencies, as digital currencies such as Bitcoin and more have been classified as assets of value that can be owned and exploited for fraudulent intentions and purposes, whether through deception or cynical manipulation of digital transactions. The law empowers the courts to impose penalties in proportionate with the amount of virtual assets involved and the nature of the cyber-fraud perpetrated, in effect adapting banal criminal liability to crimes borne of technology and cryptocurrencies.

The position taken by the Iraqi legislator may be summed up in this way: the laws in force are not deemed exclusively criminalising the invasions to the property of virtual currencies since the present texts of our general Penal Code pertain to “movable property” and “material things”: thus virtual “currencies” do not have any physical corporeity and their nature resides in being something encrypted in the network. Consequently, a theft or misuse of cryptocurrencies does not seem to fall in the area of application of laws on ordinary theft, pending any specific regulatory intervention.

Moreover, the pending Anti-Cybercrime Law will also help pave the way for crimes committed through the theft of things wandering in cyberspace, including virtual currencies. By penalising behaviour not conducted by “real-world” means, it seeks to make criminals of those who pilfer illicit cryptocurrency by improper means. Thus, observing this trend, it becomes apparent that the liability of the crypto-using criminal lies in having a larger definition of what constitutes things deserving of legal protection, as otherwise the action is not strictly criminal in contempt of the law as it stands.

Investigation Procedures and Evidence

Again, the technique of investigations varies with the nature of the crime or the law under which the crime is committed; thus, in cybercrimes, the investigation is of a purely electronic nature. Electronic investigation is defined, as the performance of those acts which an investigator may properly and lawfully perform through the agency of the Internet by use of surveillance devices, or directly on the computer itself, for the purpose of gathering information and identifying or explanatory information about persons, places and things, as the same applies to their respective natures, for detection and apprehension of computer and Internet related crimes.

The monitoring and tracing of cryptocurrencies occurs through use of technical means, hardware and software that enables the collection of data and tracing of its itinerary without those involved in the transaction being aware that there is a presence, typically by placing the information server of a service provider under observation by means of technical means, and monitoring the incoming and outgoing data, and collecting, storing and analysing whether it contains suspicious material or material of a criminal nature. Articles 20 and 21 refer to these as being “technical means” and meaning hardware and software that enable investigative agencies to detect and trace crimes committed by means of computer systems with great efficiency.

While the subject of a search in the case of a cybercrime may be a computer system or telecommunications network, in the case of cryptocurrency, a search may be for an electronic wallet contained in a computer, a tablet, a smartphone, or an external storage device containing the electronic wallet data. The goal of such a search, however, cannot be accomplished unless the investigators gain access to the electronic wallet by obtaining its primary digital key. Seizure of evidence in the category of cryptocurrency crimes assumes extraordinary importance because of the purely digital nature of the transactions and the difficulty in tracing them through traditional evidentiary tools. “In this class of crimes, evidence is not something that can be held or touched. Evidence is data, kept digitally within an electronic wallet, on the blockchain, and on the servers of trading platforms. Securitisation, therefore, requires technical steps taken to protect its integrity from tampering, such as data imaging, documentation of data transfer, and verification of the time of acquisition. The seizure process also includes the acquisition of encryption keys, transaction logs pertaining to the wallet, and access data (logins/logouts) from digital platforms. All of these steps must be executed by experts in digital forensics in order to make the nature and technical quality of the seized Cs material acceptable and convincing to the courts. This has to be done according to the standards of what the 'digital chain of custody' is, the linchpin safeguard against manipulation or substitution in the phase of investigation or in the surrender of data to the investigating arm. The red

step to the green in the informing of this kind of 'vulnerable matter' (and the crime it symbolises) then becomes the technical slaughter of the legal.

Such is the part which confiscation, disbursory exaction, as we shall prove it to be to be put to as a penal sanction. It is defined to be a violent dispossession of the ownership of moving property withoutstorge, by which it becomes the property of theState: it has also been described as a pecuniary punishment, bywhich the State or some other person takes possession of movables to which a crime (or a crime about to be committed) isannexed, actually disposing of it, though contrary to the wish oftheir owner.

Suspension is viewed as one of the most sinister penal consequences of the crimes of cryptocurrency, for these crimes are committed with the assistance of a property which is easily transported and difficult to hide. From the standpoint of its legal characterisation, confiscation under Iraqi law is said to be mandatory confiscation and supplementary confiscation. Confiscation may be mandatory or discretionary; either form may extend to crypto-assets whenever they are the object of the crime or the proceeds of an offence . . . Objects are subject to mandatory confiscation if they were used as remuneration for the commission of a crime, or constituted the subject of certain crimes (eg, crime relating to trading during wartime, or employment of specialised objects to carry out a crime). By analogy, cryptocurrencies that are delivered as consideration for crimes such as money laundering and cyber fraud could be said to be the direct price of a crime, and as such, immediately subject to mandatory confiscation. Regarding judicially obligatory supplementary confiscation mentioned in paragraph (1), Article 101 of the Iraqi penal code grants the court discretionary power to confiscate objects derived from or used in a crime, material and digital, as long as it does not prejudice bona fide third parties. In all probability, the content of paragraph 1 would cover digital wallets, keys or balances of cryptocurrencies of ill-got origins, as far as things can be kept in such a way that proves them to be connected to the crime.

4.3. Discussion

The research indicated that the digital and decentralised nature of cryptocurrencies makes them an attractive target for crime, in particular crime with financial theft (where, for example, a hacker drains a victim's cryptocurrency wallet), money-laundering and fraud. Using anonymity and the swift transfer of value across encrypted networks makes it difficult to identify the perpetrator and track where the money is moving to, and how much money changes hands.

It was found that the material element of theft can be applied to cryptocurrencies. The act of misappropriation is committed either by hacking into a digital wallet and transferring assets to the perpetrator's full possession, or by converting partial possession to full possession when an employee or platform administrator abuses their authority to access digital wallet keys and transfer them to themselves with the intent to possess them. This confirms that this behaviour can be classified under the traditional definition of financial crimes.

They concluded that the mental element in cryptocurrency crimes of theft is no different from that of traditional theft crimes in general. It is premised on general and specific intent, encapsulated in the perpetrator’s plan to appropriate the digital currency into his permanent possession. Indeed, gives rise to a general application of the general rules of criminal intent to cybercrimes where the intent to interfere with another’s property exists.

Even in Iraq, a legislative gap was revealed. The provisions of the Penal Code still limit the definition of property to that of tangible, movable property. Concerning this, we find that there is no way to criminalise the theft of ownership of cryptocurrency under the current provisions. It makes clear that we need a clear legislative amendment to replace the word "movables" with the word "thing" or add specific provisions that explicitly criminalise electronic theft and attacks on digital wallets.

The problem of proving cryptocurrency-related crimes, according to the researchers, can only be solved through advanced digital investigation and tracking techniques like server monitoring, data traffic tracking, virtual account identification and blockchain record analysis. This means that electronic investigation tools need to be developed and relevant authorities need to be trained and equipped with cutting-edge technical know-how to track, preserve and seize digital evidence suitable to modern-day procedures.

The study concluded that confiscation is an already-relevant form of punishment against cryptocurrency-related crimes, which it suggested should be developed as a mandatory punishment in relation to the cases envisaged by law or as an optional additional punishment for the property that is

used or obtained from the crime insofar as such punishment is not applied at the expense of the rights of bona fide third parties, which requires a modification of the law to accept the peculiarities of virtual currencies and the possibility of legally seizing, freezing or confiscating them.

4.4. Recomendation

The Iraqi Penal Code needs to be amended to include a contemporary definition of money, which includes digital assets and cryptocurrencies. This can be done through either the replacement of the term movable property with thing or by adding explicit provisions regarding attacks on digital wallets, cryptocurrencies and objective protection in line with these emerging technologies.

Let's pass the Cybercrime Law already, including the provisions related to crimes involving cryptocurrencies like digital fraud, electronic embezzlement, digital wallet theft, unauthorised access with intent to transfer virtual assets, etc., to equip the judiciary further to go after these crimes.

The investigative and technical capacity of the agencies responsible for electronic investigations could be improved through the provision of technology to assist tracking of movement of crypto assets and provision of specialised training for investigators and technical experts in digital data investigations, blockchain and wallet tracking and electronic evidence handling.

Creating specialised units within the judicial and security apparatus of the state about crimes of digital assets and cryptocurrencies. These units would have responsibility for investigation, technical analysis, and international judicial cooperation (these crimes have become borderless crimes, giving rise to a constant need for regional and international cooperation).

Drafting legal rules for the procedures of seizures, freezing and confiscating cryptocurrencies, to ensure their preservation and prevent their smuggling or concealment from the authorities in the course of investigations while protecting the rights of bona fide third parties, and also devising the technical and legal rules that process and authorities should develop and apply when it comes to handling digital wallets in a secure and judicially enforceable manner.

5. Conclusion

In conclusion, it is sufficient to point out that crimes committed by cryptocurrencies are becoming a greater challenge for traditional legal systems, given the digital, decentralised, and sometimes anonymous nature of these currencies, and also their cousin "virtual reality" (Vu, 2018). Until existing criminal liability rules can accommodate the technological advances, the upsurge of crime fuels the need for rules that apply to (i) acts of crime such as frauds, thefts, or terrorist financing methods, and (ii) methods of enforcement and treaty techniques regarding methods of evidence, investigation techniques, and seizure or confiscation. It has been observed in this study that dealing with these kinds of crimes calls for such a level of detail in the legislation that general provisions run the risk of being wholly ineffective, and thus legislation is required that is based on a right technical understanding of the cryptocurrency and its techniques. Such an approach is best suited to audit the crime and crime prevention, and protect our financial and social order without prejudice to our rights and freedoms, or the stability of digital transactions in a changing environment.

References

[1] M. Fratianni, "The Future International Monetary System: Dominant Currencies or Supranational Money? An Introduction," *Open Econ. Rev.*, vol. 23, no. 1, pp. 1–12, Feb. 2012. doi: 10.1007/s11079-011-9237-x.

[2] G. A. Walker, "Digital Money & Central Bank Digital Currency (CBDC) – New Opportunity, New Challenge," *Int. Law.*, vol. 55, no. 3, pp. 409–504, 2022.

[3] Q. Shuai, R. Huang, J. Liu, and L. Zhang, "Introduction to E-commerce and Financial Payments," in *Handbook of E-commerce in China*, Z. Qin and Q. Shuai, Eds. Singapore: Springer, 2025. doi: 10.1007/978-981-96-7629-3_11.

[4] N. Alsalmi, S. Ullah, and M. Rafique, "Accounting for digital currencies," *Res. Int. Bus. Finance*, vol. 64, p. 101897, Jan. 2023. doi: 10.1016/j.ribaf.2023.101897.

[5] L. Xia, T. Zhu, Z. Jing, Q. Wang, Z. Ma, Z. Huang, and Z. Yin, "A Two-Layer Transaction Network-Based Method for Virtual Currency Address Identity Recognition," *Cryptography*, vol. 9, no. 4, p. 72, Oct. 2025. doi: 10.3390/cryptography9040065.

[6] F. O. Ukwueze, "Cryptocurrency: Towards Regulating the Unruly Enigma of Fintech in Nigeria and South Africa," *Potchefstroom Electron. Law J.*, vol. 24, no. 1, pp. 1–35, 2021. doi: 10.17159/1727-3781/2021/v24i0a10743.

[7] A. M. Sharma, "Cryptocurrency and financial risks," Doctoral dissertation, School of Business, Liberty Univ., Lynchburg, VA, USA, 2020.

[8] U. Sadiqi, *Artificial Intelligence and Global Security: Future Trends, Threats and Legal Challenges*. Cham, Switzerland: Springer Nature, 2024.

[9] D. Broby, "Central bank digital currencies: policy implications," *Law Financial Markets Rev.*, vol. 16, no. 1-2, pp. 100–115, 2022.

[10] F. Alvarez, D. Argente, and D. Van Patten, "Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador," *Science*, vol. 382, no. 6677, p. eadd2844, Dec. 2023. doi: 10.1126/science.add2844.

[11] A. AbdulBasith, M. M. Elgammal, and B. Abuzayed, "Cryptocurrencies and Finance Theories," *Asia-Pacific Manag. Account. J.*, vol. 16, no. 2, pp. 315–365, Aug. 2021. doi: 10.24191/APMAJ.V16i2-12.

[12] C. Larsen, "Chris Larsen: Money Without Borders," *Stanford Graduate School of Business*, Oct. 2014. [Online]. Available: https://www.gsb.stanford.edu/insights/chris-larsen-money-without-borders. [Accessed: Jan. 4, 2026].

[13] N. Carter, "A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors," MSc Finance and Investment dissertation, Business School, Univ. of Edinburgh, Edinburgh, U.K., 2017.

[14] L. K. C. Cotrina, P. M. S. León, C. A. R. Reyes, and M. A. A. Ballesteros, "Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches," *J. Educ. Soc. Res.*, vol. 14, no. 5, p. 96, Sep. 2024, doi: 10.36941/jesr-2024-0124.

[15] N. Gandal, J. Hamrick, T. Moore, and T. Oberman, "Price manipulation in the Bitcoin ecosystem," *J. Monetary Econ.*, vol. 95, pp. 86–96, May 2018. doi: 10.1016/j.jmoneco.2017.12.004.

[16] S. A. Lee and G. Milunovich, "Beyond the breach: Bitcoin's response to exchange-related cyberattacks and closures," *Appl. Econ. Lett.*, pp. 1–5, 2024, doi: 10.1080/13504851.2024.2316141.

[17] C. Proctor, "Legal Tender: A Notion Associated with Payment in Central Bank Money," *The Evolution of Central Banking and Monetary Policy in the Asia-Pacific*, vol. 34. Washington, D.C., USA: IMF eLibrary, 2015.

[18] F. Stajano, F. Samaria, and S. Zi, "On the Nature and Security of Expiring Digital Cash," *J. Risk Financial Manag.*, vol. 18, no. 8, p. 334, Aug. 2025, doi: 10.3390/jrfm18080452.

[19] N. Albalawee and A. S. Al Fahoum, "Islamic legal perspectives on digital currencies and how they apply to Jordanian legislation," *F1000Research*, vol. 12, p. 288, Aug. 2023, doi: 10.12688/f1000research.128767.2.

[20] L. Y. Gelemerova, "The anti-money laundering system in the context of globalisation: a Panopticon built on quicksand?," Doctoral dissertation, Tilburg Univ., Tilburg, Netherlands, 2011.

[21] A. Verhage, "Global governance = global compliance? The uneven playing field in anti money laundering," *Routledge Handbook of White Collar and Corporate Crime in Europe*, J. van Erp, W. Huisman, dan G. Vande Walle, Ed. Oxford/New York, NY, USA: Routledge, 2015.

[22] S. Elsayed, "Cryptocurrencies, corruption and organised crime: Implications of the growing use of cryptocurrencies in enabling illicit finance and corruption," *U4 Helpdesk Answer*, vol. 2023, no. 8, Mar. 2023.

[23] H. Lasnouni, R. Belhadef, and N. Ghoual, "The virtual currency: its risk and legality Bitcoin as a model," *Financ. Bus. Econ. Rev.*, vol. 4, no. 3, pp. 248–266, Sep. 2020, doi: 10.58205/fber.v4i3.1442.

[24] R. A. Hameed and B. M. Kamal, "Legal regulation of Virtual Currencies in the Arab Countries 'Iraq and the United Arab Emirates as a Model'," *Amer. J. Social Humanitarian Res.*, vol. 5, no. 1, pp. 5–19, Jan. 2024, doi: 10.31150/ajshr.v5i1.2646.

[25] M. S. Utkina, O. M. Reznik, and O. S. Bondarenko, "The place and the role of financial monitoring in anti-money laundering system," *Eduvest – J. Universal Stud.*, vol. 3, no. 5, pp. 886–897, May 2023, doi: 10.59188/eduvest.v3i5.821.

[26] S. Farber, G. Amir, and S. Inbar, "Will You Sweep Away the Righteous with The Wicked?' Third-Party Rights in Forfeiture Law," *Crim. Law Forum*, vol. 36, pp. 549–600, 2025, doi: 10.1007/s10609-025-09513-6.

[27] *Law No. 13 of 2012 on Issuing the Law on Qatar Central Bank and the Regulation of Financial Institutions*, State of Qatar, Dec. 2012.

[28] FATF, "Anti-money laundering and counter-terrorist financing measures - Iraq, Mutual Evaluation Report," Financial Action Task Force, Paris, France, Jul. 2024.

[29] S. M. S. Uddin, "Cybersecurity and Financial Markets," Ph.D. dissertation, Research School of Finance, Actuarial Studies and Statistics, Australian Nat. Univ., Canberra, ACT, Australia, 2023.

[30] A. O. M. AL-Dulaimi, "The jurisprudential debate about the jurisdiction of the Federal Supreme Court in Iraq," *Social Sci. Humanities Open*, vol. 12, p. 102008, 2025, doi: 10.1016/j.ssaho.2025.102008.