International Journal of Finance, Insurance and Risk Management
Volume XIII, Issue 4, 2023

pp. 127-151

Challenges and Legal Aspects of Financing Projects Through Cryptocurrencies in Iran

Submitted 01/10/23, 1st revision 17/10/23, 2nd revision 20/11/23, accepted 30/11/23

Sayed Mohammad Mousavi[1], Yazdan Shahin Rad[2]

Abstract:

Purpose: *In this article, the objective is to clarify the uncertainty surrounding the significant elements of using digital currencies to fund national projects, especially infrastructure projects and the transfer of knowledge and technology to the country, a particular focus.*
Design/Methodology/Approach: *The present study utilizes a qualitative methodology suitable for descriptive and exploratory studies to accomplish its objectives. As a result of this approach, the researchers will be able to comprehensively analyze the existing literature on the operational and legal complexities associated with cryptocurrencies.*
Findings: *The legal part also aims to highlight the significant results and recommendations for the readers and policymakers to overcome the legal challenges and achieve the ultimate goal of this technology, taking into consideration the risks associated with this digital asset of exchange.*
Practical Implications: *Blockchain technologies offer new open source-based opportunities for developing new types of digital platforms and services. While research on the topics emerging, it has this far been predominantly focused to technical and legal issues. in continues pinpoints the most pressing legal issues concerning this virtual form of money.*
Originality/Value: *In this connection, researchers in different parts of the world have endeavored to reach and present their findings along with their suggestions and recommendations to improve the current status of this relatively nascent technology.*

Keywords: *Blockchain, cryptocurrency, financing methods, state policy, decentralized system, cybercrime.*

JEL Classification: *O1, G0.*

Paper type: *Research article.*

[1]*M.Sc. Graduated, Department of Project Management and Construction, South Tehran Branch, Islamic Azad University, Tehran, Iran, orcid.org/0009-0009-3909-1097, E-mail: Msvi.mhmd@gmail.com;*
[2]*M.A. Student, Department of International Trade Law, South Tehran Branch, Islamic Azad University, Tehran, Iran, orcid.org/ 0009-0008-5197-2674, E-mail: Yzn.pn72@gmail.com;*

1. Introduction

Due to the rapid advancement of digital technologies, it has become increasingly necessary for the global economy to construct a financial framework founded on the principles of widespread confidence and transparency (Haferkorn and Quintana Diaz, 2015). Historically, cryptocurrency, based on distributed ledger technology, commonly known as blockchain, has been predicted to drive digitalization in the financial sector. Cryptocurrency has ushered in an era of epoch in the global financial landscape (Nayak and Nayak, 2022).

Over the past decade, Cryptocurrencies have emerged as a disruptive force in the world economy (Guo *et al.*, 2020). They offer a distinctive category of currency fully decentralized and fundamentally distinct from other extant forms of currency (Ahmed *et al.*, 2022). In 2008, an anonymous entity or group using Satoshi Nakamoto unveiled a revolutionary electronic payment system that utilizes a peer-to-peer structure and a decentralized ledger called blockchain to eliminate the need for a middleman (Agyei, 2022). Eliminate the intermediary party engaged in transaction processing, licensing, and implementation.

In order to optimize the efficacy of this novel technology (Allen *et al.*, 2022), the white paper introduced the concept of "Bitcoin" as a means of facilitating currency exchange and circulation among users within the digital system (Abduraimova, 2022). In addition, it has implemented a decentralized financial system in parallel with blockchain technology (Yuan and Wang, 2018; Afzal and Asif, 2019; Houben, Snyers, *et al.* 2018). This has introduced a novel business model currently being examined by numerous banks globally. Since its inception, Bitcoin has garnered a substantial following, particularly in the aftermath of the financial crisis.

This event profoundly impacted individuals' attitudes toward traditional banking institutions and governmental bodies (Ghosh *et al.*, 2020). This resulted in significant financial losses and decreased trust in conventional banking transactions ((Lee, 2023; Haferkorn and Quintana Diaz, 2015). System manipulation or corruption is not possible because a centralized organization or government does not issue cryptocurrencies (Tredinnick, 2019; DuPont, 2017).

However, the protection the government considers for the official currency does not occur in cases of legal dispute or deception. Cryptocurrencies and their potential ramifications have varied across nations. Despite their widespread usage, there exists a general lack of awareness among the populace regarding the operational intricacies, associated hazards, and legal dimensions of Cryptocurrencies (Campbell-Verduyn, 2017).

Infrastructure requires significant investment, particularly in extensive undertakings in Iran. In recent decades, the imposition of financial, banking, and economic sanctions on the country has put significant pressure on public resources

(Mahdavieh, 2022). Additionally, the construction budget has steadily decreased over time due to the economic priorities of past and present governments (Rezaeinejad, 2021). Infrastructure requires financial initiatives to fund projects. The issue at hand has prompted the emergence of the notion of an "infrastructure market" within academic and managerial circles of the country (Ismael, 2021).

This refers to using Cryptocurrencies as payment and receipt in project financing. The local infrastructure market involves funding infrastructure projects by exchanging production services for creating value (Ranjbar Fallah and Foroughi, 2020). This market enables infrastructure projects to secure long-term and dependable financing through Cryptocurrencies, even in competition from other financial markets.

This article seeks to explain the mechanism used for decentralized Cryptocurrencies in financial payment systems in projects in such a way that was creating a suitable platform to understand how Cryptocurrencies work will provide a more precise idea to regulators and, on the other hand, the ecosystem of currencies fully understands digital and on the other hand provide ways to address and interact with such technologies rather than ignore them.

This article also identifies the most important international legal issues and Iran's internal legal issues and challenges that Cryptocurrencies are facing. This essential information aims to give the reader a deep understanding of virtual currency and the underlying payment system and methods (Ranjbar Fallah and Foroughi, 2020).

Despite the wide range of Cryptocurrencies in terms of type and structure, each of which requires a deep investigation, in this research, "Bitcoin" is used as the oldest and most popular type of digital currency to explain the common mechanism and expand the issues raised in it to almost all Cryptocurrencies (Mnif and Jarboui, 2022).

2. Research Methodology

The present study utilizes a qualitative methodology suitable for descriptive and exploratory studies to accomplish its objectives. As a result of this approach, the researchers will be able to comprehensively analyze the existing literature on the operational and legal complexities associated with cryptocurrencies (Benigno et al., 2022; Rubinacci, 2022).

In order to address the research inquiries and achieve the study's objectives, the data obtained through this analysis will be scrutinized. An overview of blockchain technology will be presented in this section, including its definitions (Jalan and Matkovsky, 2023). Afterward, we will examine the burgeoning literature (Almaqableh *et al.,* 2022) on the practical implementation of blockchain technology, namely Bitcoin (Fernandes *et al.,* 2022).

Although numerous systematic literature reviews have been published on various aspects of digital payments, the literature review presented in this paper is deliberately brief (Sahoo and Sethi, 2022).

2.1 Project Financing Methods

The provision of funds and financing mechanisms for infrastructure projects poses a significant challenge to developing countries with adequate capital but limited implementation capacity. A variety of sectors are involved in these projects, including exploration and extraction, transportation, upstream industries (Gatti, 2023), and service provision.

Thus, governments should explore private sector financing as a means of involving private entities in infrastructure and public initiatives (Tavakolan and Nikoukar, 2022) while avoiding permanent ownership of infrastructure projects (Chen *et al.*, 2022). In developing countries, financial crises and institutional inefficiencies exacerbate the challenge of allocating sufficient capital for the implementation of large projects (Tinsley, 2022; Norena-Chavez and Thalassinos, 2023).

As a result, choosing an appropriate methodology that is aligned with the financial circumstances and institutional characteristics of each organization within various regions is of utmost importance. There are a number of methods that can be used to finance a project, including:

Project financing: A notable distinction arises from this particular approach, which is often referred to as self-governing finance in the context of Iran. The absence of any prerequisites imposed by the country or lending institution for credit approval is a critical characteristic (Desalegn and Tangl, 2022).

Moreover, the government is responsible for ensuring that the revenue generated by the project will be used to repay the loan. The economic evaluation of the significant undertaking is the primary determinant for foreign creditors of financial capital (Taghizadeh-Hesary *et al.,* 2022). The foreign lender may provide capital without direct involvement if the project is deemed feasible. The project will receive the goods produced in exchange for repayment.

Finance: In the context of investment, the term "finance" refers to the use of internal resources or the acquisition and use of a loan denominated in a foreign currency (Khan *et al.,* 2022). It is a temporary means of transferring capital to a foreign country in which a foreign financial institution receives the principal and sub-credit provided through a contract or bank guarantee without being involved in other matters (Mittal, 2022).

Usance: Usance investment refers to the practice of borrowing short-term funds, typically facilitated by developed nations' monetary and financial markets, to

promote exports. The borrowing country agrees to repay the loan with its financial resources as part of this arrangement (Nguyen and Doan, 2022).

BOT (Build, Operate, Transfer): According to this approach, a foreign investor enters into a contract to provide financial resources, supervise construction, and manage the operation of an industrial facility according to predetermined terms (Pawlik *et al.,* 2022). Once the contract has been fulfilled, the host country becomes the project owner (Almashhadani and Almashhadani, 2022).

ROT (Restoration, Operation, Handover): An analogy can be drawn between this approach and the BOT method, except that the intended design already exists but must be revitalized (Curi *et al.,* 2022).

BOO (build, operate, own): Unlike the previous approach, the present method involves the transfer of facility rights to the host nation upon completion of the contract. Ultimately, it is up to the investing nation to decide whether or not to transfer ownership (Boo and Chan, 2022).

ROO (Restoration, Operation, Ownership): Rather than constructing a new facility, the investor revitalizes an existing facility under the Build-Own-Operate (BOO) framework (Monteiro *et al.,* 2022).

BLT (build, lease, transfer): Investing nations finance and develop infrastructure projects and then lease these facilities for a specific period. As soon as the lease term expires (Maresti *et al.,* 2023), ownership and management of the facility are transferred to the host country.

BLO (build, lease, operate): Partnerships in this form are similar to those in the previous paragraph but with the distinction that ownership is transferred (Hassan *et al.,* 2022).

DBOM (Design, Build, Operate, Maintain): In all cases, the ownership transfer is governed by contractual agreements and is usually either Build-Operate-Transfer (BOT) or Build-Own-Operate (BOO). According to this approach, the project implementing company is responsible for project design (Brady *et al.,* 2022).

2.2 Blockchain

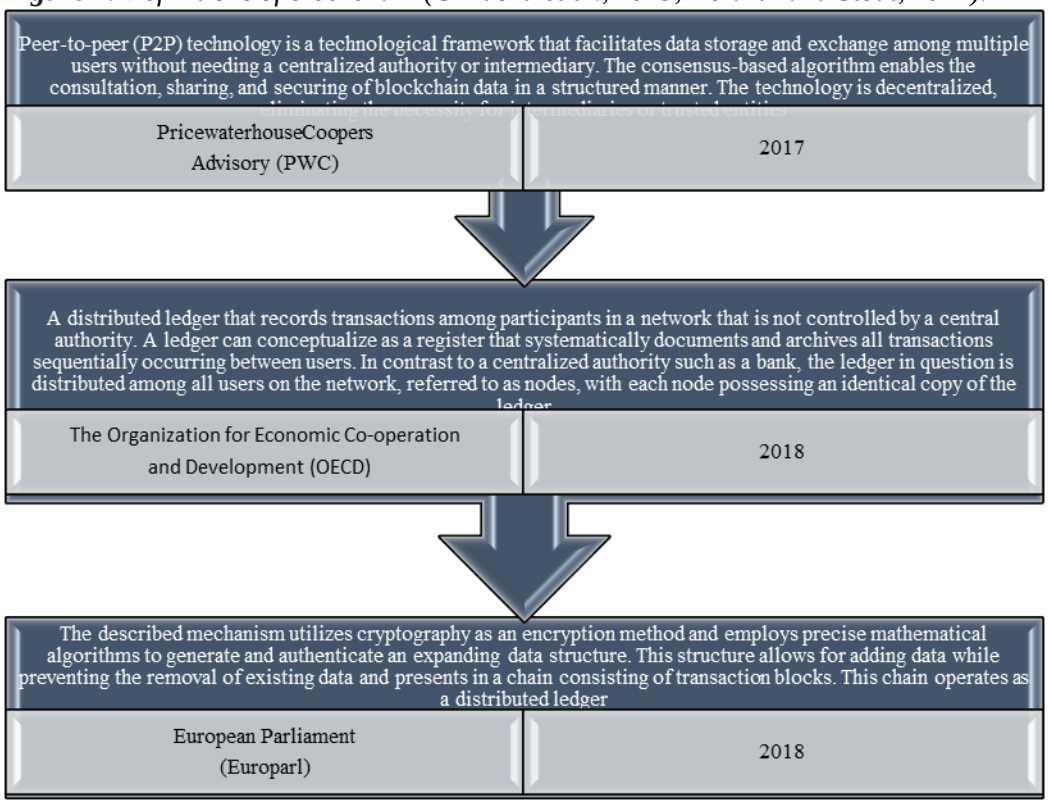
The blockchain serves as the fundamental building block of cryptocurrency (Gadekallu *et al.,* 2022; Rabbani *et al.,* 2020) and is responsible for its inception. Blockchain technology's distinctive (Pasdar *et al.,* 2023) and highly innovative characteristics have garnered significant interest and investment from global investors and researchers (Laurence, 2023). Numerous reports have been produced at both the domestic and global levels. The Table below illustrates that the

blockchain concept has proffered multiple definitions. Each of these definitions has emphasized a significant point or facet (Zhu *et al.*, 2023).

The initial definition of blockchain technology presented by the European Parliament emphasizes encryption and security (Nofer *et al.*, 2017), whereas the following definitions emphasize the technical components of blockchain technology, such as decentralization and peer-to-peer functionality (Sen Gupta, 2017; Rupeika-Apoga and Thalassinos, 2020; Thalassinos *et al.*, 2015).

Based on the above-mentioned definitions, scholars have defined the "Blockchain" as a distinct type of Distributed Ledger Technology (DLT) that utilizes a communal ledger (Mohanta *et al.*, 2018) that stores information in interconnected blocks, forming a chain through cryptography and hashing (Hewa *et al.*, 2021). Cryptocurrencies work on a peer-to-peer basis, eliminating the need for intermediaries such as central banks and financial institutions (Wang *et al.*, 2019).

***Figure 1**. Definitions of blockchain (Chhabra et al., 2019; Boiardi and Stout, 2021).*



***Source:** Own study.*

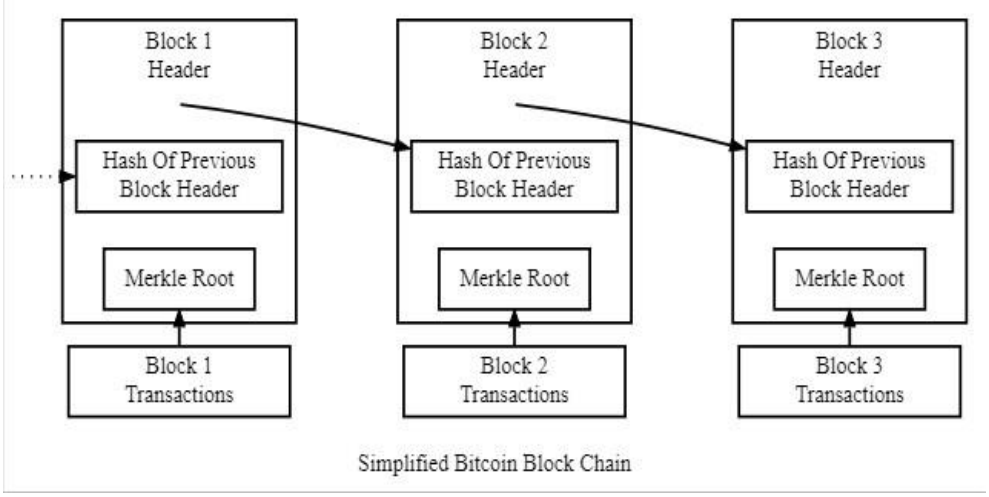
In order for blockchain technology to function effectively, cryptography science is utilized, as it is used to encrypt the regulations governing the cryptocurrency within

the system itself. To achieve widespread acceptance and usage (Cong and He, 2019), cryptocurrency must maintain stability, security, and resistance to counterfeiting (Ante, 2021).

The use of cryptography plays a crucial role in safeguarding the cryptocurrency system, overseeing its issuance, and verifying transactions to achieve this objective (Smales, 2020).

The blockchain technology is characterized by its complete decentralization and transparency (Daoud, 2019). The ledger of the blockchain is continuously updated with each transaction that is included in it (Meunier, 2018). The provided information is incomplete. Almost all data stored within the blockchain, such as account names and transactions, is encrypted. With blockchain technology, data can be rapidly transferred between devices at a nominal cost through a network of nodes, commonly referred to as the "Mining Process." (Yousefi and Tosarkani, 2022; Singh *et al.,* 2022; Krichen *et al.,* 2022)

Figure 2. *The blocks in the blockchain (Krichen et al., 2022)*



Source: *Own study.*

The reference above (Krichen *et al.,* 2022, Figure 2) illustrates that all transactions recorded on the blockchain ledger are publicly accessible. When a data block is appended to another block, its contents become immutable and cannot be modified (Rajasekaran *et al.,* 2022).

Any attempts to manipulate them will be promptly identified. Using cryptographic hash functions within the blockchain framework ensures that any modification to a specific block will likely disrupt the consensus mechanism established among the remaining blocks (Di Vaio *et al.,* 2023).

The purpose of hashing in cryptography is to convert a conventional form of data into an encrypted form. It is explicitly incorporated into the consensus mechanism of the system, whose primary function is to accept inputs and convert them into numerical values (Vujičić *et al.,* 2018).

An alteration to the data contained within the block would significantly alter the signature assigned to the block, thus invalidating the entire blockchain (Wright and De Filippi, 2015). Modifying a data feed within a block requires modifying all subsequent blocks' signatures until its termination, which is generally considered impossible (Crosby *et al.,* 2016). An individual block consists of a hierarchical structure of encrypted data resembling a tree.

Each of the eight documented transactions in a block has been hashed separately (Treleaven *et al.,* 2017) resulting in a unique hash value for each. Thus, the resulting hash value is obtained by combining this hash value with another value. In the above-mentioned procedure, a singular hash value, known as the "Merkle root," is obtained through iteration (Underwood, 2016).

2.3 Cryptocurrency

The term "cryptocurrency" is a compound word that comprises two distinct morphemes, namely "crypto" and "currency." (Liu and Tsyvinski, 2021). The term "crypto" indicates the significant impact cryptography has had since its inception (DeVries, 2016). The market encompasses an estimated 8,548 cryptocurrencies, collectively with a market capitalization of approximately $ 1,170,535,305,158 (Maese *et al.,* 2016).

Cryptocurrencies are non-physical entities that lack a tangible presence in the real world. Rather than being physical (Ahamad *et al.,* 2013) these assets are digital and are stored on the internet using a distinct electronic wallet (Farell, 2015).

Access to this wallet is restricted to the wallet owner, who possesses both a public and private key. Bitcoin, the progenitor of all cryptocurrencies, is an open-source system that operates decentralized, avoiding any singular ownership or control by a specific entity or individual (Wang *et al.,* 2023).

Cryptocurrencies are accessible to all who wish to participate in the network. Within the realm of open-source software, developers can alter Bitcoin security codes to generate their own cryptocurrency initiatives (Zohuri *et al.,* 2022).

Although a vast array of cryptocurrencies exists on the market, a significant proportion of them are founded on Bitcoin's fundamental protocol. Since its inception, numerous national and international organizations have released reports analyzing cryptocurrencies and their underlying technology (Ahamad *et al.,* 2022).

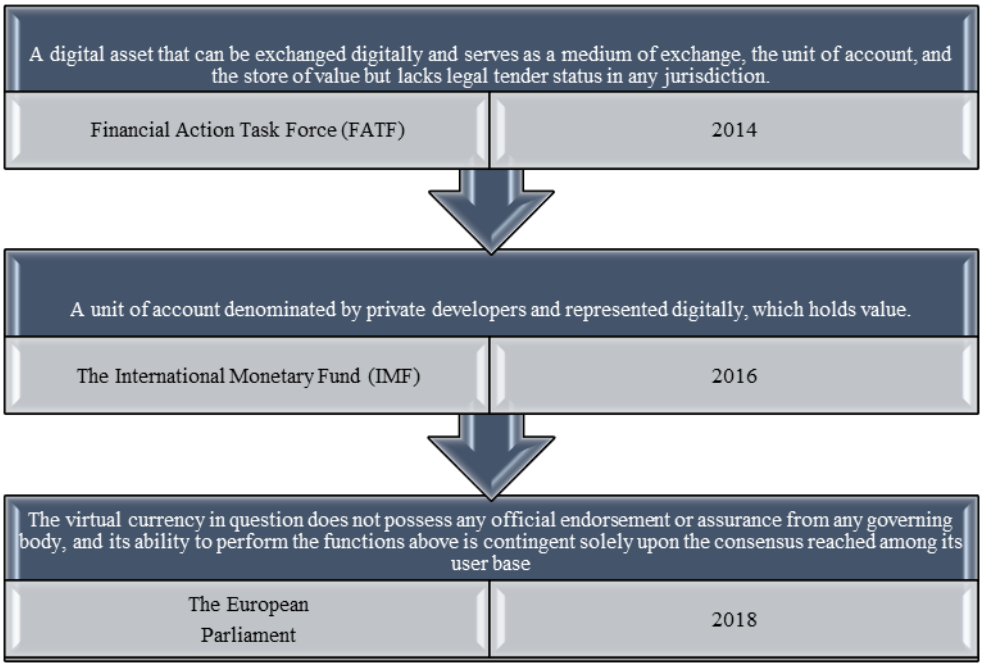
Most of these reports define the term "cryptocurrency" and other associated terminology. The following table gives a number of values for the earlier definitions.

As shown in Figure 1 above, international organizations have a wide range of definitions of cryptocurrency (Sultan *et al.*, 2023). They agree that cryptocurrency is a "digital representation of value,"; however, their definitions differ. For example, the Financial Action Task Force (FATF) defines cryptocurrency as a digital manifestation of value that does not have legal tender status within any established jurisdiction (Choithani *et al.*, 2022).

According to the International Monetary Fund, these are subsets of virtual currencies generated by private developers and denominated in their account units (Shah *et al.*, 2023). Furthermore, the European Parliament directed its attention toward the mechanism and convertibility of cryptocurrencies.

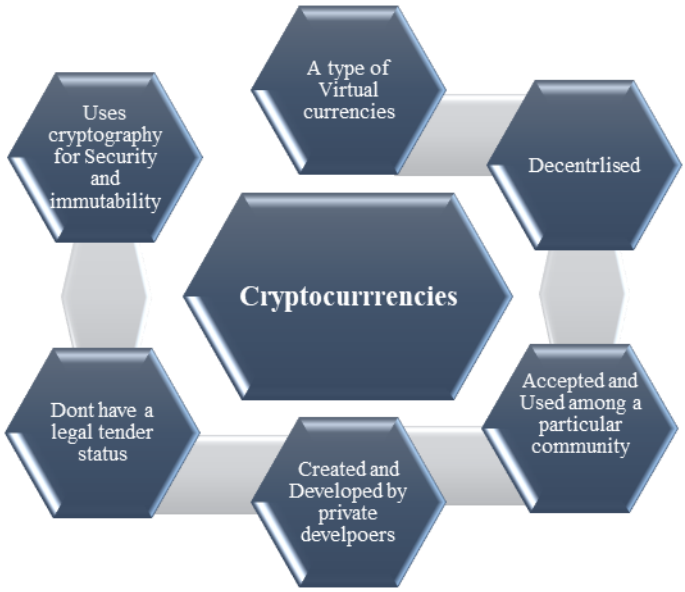
Accordingly, the abovementioned definitions indicate that these international organizations have yet to offer a comprehensive and standardized definition of cryptocurrency (Islam *et al.*, 2023). Based on the definitions above, cryptocurrency's characteristics align with the delineations presented in Figure 4.

Figure 3. *Definitions of cryptocurrency*



Source: *Own study.*

Figure 4. *Cryptocurrency's characteristics constructed based on the definitions*



Source: *Own study.*

3. The Legal Issues Associated with Cryptocurrency

3.1 Cybercrime Using Cryptocurrencies

Cryptocurrencies must be addressed legally to be widely accepted and acknowledged. Due to their anonymity, cryptocurrencies are a beautiful instrument for criminals seeking severe criminal activity. Governments worldwide have been paying close attention to cryptocurrency regulation to monitor and control cryptocurrencies (Brown, 2016).

One example of how cryptocurrencies are misused is the Silk Road problem on the dark web. Illegal goods and items were available for purchase on the "Silk Road" dark-web marketplace. Criminals worldwide could purchase and sell all kinds of illegal goods, including drugs and weapons, using cryptocurrency as a form of payment. 2013 the American government shut down the website and detained the owner.

The Silk Road is an example of how cryptocurrency can be used to conduct illegal activities such as money laundering, terrorism financing, tax evasion, and bribery (Pessa *et al.*, 2023). These illegal activities, such as decentralization and anonymity, can be carried out using cryptocurrencies.

Another example is United States of America v. Michael Mancal Brown (Christin, 2013) where the defendant was found guilty of extortion against former presidential candidate Mitt Romney. The criminal asked Romney to send him $1 million in Bitcoin in exchange for not disclosing any sensitive information that could harm Romney's campaign (Vasek, 2015).

3.2 Cryptocurrency System with a Decentralized Control System

According to prevailing legislation in numerous nations, currency must be issued exclusively by a central authority authorized by law. Its purpose is to ensure that it is recognized as a valid official tender. Implementing a specific entity's printing and minting procedures will challenge counterfeit currency (Thayer, 1987). The issuance and circulation of a national currency grants legal authority to the central authorities responsible for its issuance.

This is outlined in the Central Bank Act. This authority enables them to exercise control over the currency following the adopted monetary plan, safeguarding and sustaining economic stability (Goodfriend and King, 1988).

The primary legal concern surrounding cryptocurrencies pertains to their decentralized nature, wherein any central authorities do not control the issuance of cryptocurrencies and the monitoring of transactions within the ecosystem. This particular issue has heightened the complexity and intricacy of regulatory and monitoring effort (du Plessis, 2014).

Cryptocurrency's decentralized nature significantly impacts various aspects, including tax allocation, volatility, criminal activity, market manipulation, and other related issues (Bunjaku *et al.*, 2017).

3.3 Deficiency of Legal Framework

All currencies around the world, including the US dollar, Euro, and Ringgit Malaysia, are recognized as official legal tender (Von Bogdandy and Ioannidis, 2014). The currencies in question are subject to regulation and enjoy high trust among the resident population. In contrast, most nations need to improve cryptocurrency regulation (Usman *et al.*, 2022).

As previously mentioned, the lack of a comprehensive legal framework that effectively addresses all pertinent criminal matters may lead to various criminal activities (Von Bogdandy, 2020). Moreover, the establishment of a comprehensive legal framework is imperative for the preservation of rights and safeguarding of interests for both investors and companies concerning this innovative invention (Margariti, 2011).

Moreover, the lack of a comprehensive legal framework will lead to numerous issues and uncertainties about matters such as law classification, taxation, inheritance, insolvency, Know Your Customer (KYC) policy, cyber-security, litigation disputes, contracts, intellectual property, and numerous other aspects (Malloy *et al.*, 2015). The significance of cybersecurity is widely acknowledged in light of the substantial number of attacks on exchanges resulting in financial losses.

A comprehensive legal framework that establishes rights, obligations and enforces penalties and punishments is necessary to address the various issues (Zhang and Diao, 2013). Another concern is the need for a cohesive legal framework or structure for overseeing cryptocurrencies and their associated operations. Various countries and international organizations worldwide hold distinct perspectives regarding cryptocurrency governance, categorization, and oversight (Gjems-Onstad, 1996).

This scenario gives rise to an illegal loophole that enables illicit cross-border operations and aids criminals in circumventing laws, such as tax evasion, by relocating to jurisdictions with relatively lax regulations.

3.4 Volatility of Virtual Currency Values

The matter of volatility represents a significant financial and legal concern for cryptocurrency users due to their intangible nature and lack of backing from tangible assets or precious metals (Sapovadia, 2015). The primary determinant of cryptocurrency value is the supply and demand principle. This indicates the level of trust individuals place in a given cryptocurrency (Giudici and Abu-Hashish, 2019). The volatility of this standard renders it unfavorable for regulators and policymakers, as its value can experience significant declines in response to statements made by influential individuals or national and international authorities (Bouoiyour *et al.*, 2016).

Figure 5. *The volatility of the bitcoin price in a day*

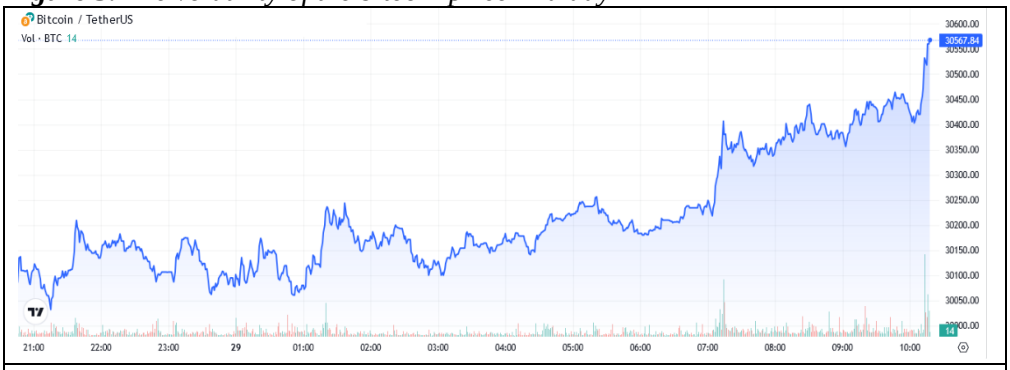


Figure 6. *The volatility of the bitcoin price in a month*

Figure 7. *The volatility of the bitcoin price in a year*

Source: *Own study.*

It can sometimes be possible for bitcoin's value to drop by more than a thousand dollars in a week, as illustrated in (Bouoiyour *et al.*, 2016, Figure 5). Those nations that accept or regulate cryptocurrency are at risk from this issue (Guadamuz and Marsden, 2015). In addition, cryptocurrencies have a significant influence on the acceptance and regulation of cryptocurrencies by regulators.

3.5 Security in Cyberspace

In a report published in 2020 by Chainalysis, a firm specializing in Blockchain analysis, it was revealed that cryptocurrency scammers managed to amass $4.3 billion in digital currency during the year 2019 (Katterbauer *et al.*, 2022). This amount represents a significant increase of more than three times the amount obtained in the previous year, 2018 (Reddy and Minnaar, 2018).

With the imperative to ensure secure and protected internet access (Higbee, 2018), cyber security has gained significant importance and is now recognized as a critical issue with profound implications for contemporary societies (Șcheau *et al.*, 2020).

Nowadays, it is increasingly difficult to imagine individuals, government agencies, and other entities operating effectively and fulfilling their daily duties. The computer system is not connected to a reliable and secure internet network. As a result, the internet has become an integral part of human existence that cannot be replaced. Cryptocurrencies lack regulations, and their anonymity has contributed significantly to the substantial rise in criminal activities connected with them (Bray, 2016).

Cryptocurrencies have thus emerged as a dual-purpose asset that serves both as a means and as a target for criminal elements to commit a variety of cybercrimes. Numerous cyberattacks have been perpetrated against cryptocurrency exchanges and individuals since cryptocurrency was invented (Zimba *et al.,* 2019).

There have been several instances of cybersecurity attacks, including one that led to the bankruptcy of the Japanese exchange company known as "Mt. Gox." From the digital vaults of the aforementioned company, approximately 473 million U.S. dollars worth of bitcoin, equivalent to approximately 850 bitcoins, was illicitly acquired (Decker and Wattenhofer, 2014).

In another notable incident, hackers stole approximately 120 thousand bitcoins from the Hong Kong-based exchange known as "Bitfinex," equivalent to approximately US$72 million at the time (Cong *et al.,* 2023). Bitcoin prices decreased by nearly 23% following the dissemination of news regarding this incident (Hu *et al.,* 2020). Furthermore, a significant attack was launched against the South Korean exchange Youbit. Following the theft of approximately 17% of the exchange's bitcoin assets, the exchange was forced to cease operations and declare bankruptcy (Nicholls *et al.,* 2021).

Several grave transgressions continue to occur throughout the world, as illustrated by the following examples. As a result of these cyberattacks, we are reminded of the weaknesses inherent in cryptocurrency platforms (Brenner and Schwerha IV, 2001) and the importance of their security measures. There are many forms of cybercrime. The act of phishing is a form of cybercrime in which perpetrators use various strategies to deceive individuals and organizations (Maras *et al.,* 2015).

As a result, they believe that they are interacting with a legitimate and authentic entity (Makam, 2023). After successfully deceiving the target, the criminal proceeds by requesting the disclosure of personal information, such as login credentials, bank account details (including debit and credit card information), address, or identification number, from the individual or entity involved (Alfieri, 2023). The wallet address is the specific information that is sought after by individuals engaged in phishing activities related to cryptocurrency.

The official announcement issued by Coincheck, a prominent Tokyo-based cryptocurrency exchange operating in Asia, on May 31, 2020, is an example of phishing. Multiple phishing attempts have been made against the company's

clientele, as acknowledged in the statement. In accordance with the company's statement, there has been a breach that has resulted in the unauthorized disclosure of various customer details. Names, addresses, birth dates, and telephone numbers are included in these details (Edwards, 2021).

Therefore, there have been no instances of theft or compromise of digital assets. Malware is another tool criminals may use to facilitate illicit activities. There are various types of malicious software, such as viruses, ransomware, and spyware, which are specifically designed to harm computer data or systems. It is also possible for malware to be used to infiltrate a targeted network or device in order to steal information stored therein (Cong *et al.*, 2023). As a result of a cyberattack perpetrated by hackers on July 11, 2020, Cashaa, a peer-to-peer trading platform, lost 336 bitcoins.

In Cashaa's account, the hackers successfully inserted malware into an exchange computer system, granting them access to the system. Ponzi schemes are notable cybercrime examples characterized by deceptive investment schemes. A substantial return is offered with minimal or no risk in order to encourage individuals to invest their funds. Ponzi schemes generate returns for older investors by obtaining funds from new investors. Therefore, funds are not allocated to a specific investment (Zagaris and Mostaghimi, 2023).

4. Discussion and Results

A number of grave transgressions continue to take place around the world as illustrated by these examples. As a result of these cyberattacks, we are reminded of the vulnerabilities inherent in cryptocurrency platforms as well as the importance of maintaining robust security measures. In addition to cybercrime, there are numerous other forms of criminal activity. In phishing, perpetrators use various strategies to deceive individuals and organizations into believing that they are engaged with legitimate organizations.

Upon successfully deceiving the target, the criminal requests personal information from the individual or entity referred to as "Phisher" including login credentials, bank account details (including debit or credit card information), address, or identification number. A Phisher's primary focus within the cryptocurrency arena is the wallet address, which becomes the subject of their malicious intent. The official statement issued on May 31, 2020, by Coincheck, a prominent Tokyo-based cryptocurrency exchange, is an example of phishing.

It is acknowledged in the statement that a number of malicious actors have launched targeted attacks against customers of the company in question. In accordance with the organization's statement, unauthorized disclosures of customers' names, addresses, birth dates, and phone numbers occurred due to a breach.

However, no digital assets have been stolen or compromised. Criminals may use malware to facilitate illicit activities.

The term malware refers to a variety of malicious software, such as viruses, ransomware, and spyware, that are designed with the intention of damaging computer systems or compromising the security of a network or device. A peer-to-peer trading platform, Cashaa, announced on July 11, 2020, that 336 bitcoins had been lost in a cyberattack perpetrated by hackers.

According to Cashaa, the hackers successfully inserted malware into the exchange's computer system, gaining unauthorized access to it. Ponzi schemes are examples of cybercrime, characterized by deceptive investment schemes. Individuals are encouraged to invest their funds by offering them substantial returns with minimal or no risk. Ponzi schemes generate returns for older investors by obtaining funds from new investors. Therefore, funds are not allocated to any specific investment.

In Iran, the current legal framework governing the transfer of digital currencies lacks comprehensiveness and adequacy. The Iranian legal framework does not contain any codified or explicit legislation pertaining to this matter. However, certain intellectuals have expressed concerns about the compatibility of these practices with Shariah principles.

Additionally, the board of ministers has established protocols to regulate the extraction of encrypted products and cryptocurrencies. The 2018 approval has been rescinded. According to Article 12 of the Code of Extraction of Assets, in 1401, instructions must be issued by the Central Bank within a three-month period to regulate the conditions of transactions. To date, no such resolution has been officially sanctioned.

The aforementioned by-laws are insufficient to address intricate legal relationships and transactions, despite the provisions outlined in Article 12. It is necessary to consult the overarching regulations that govern payment in domestic law and international conventions when conducting a legal analysis. Thus, according to Amendment 2023, Iran's legal system contains rules regarding what types of transactions are permitted, as detailed in Article 12 of the regulation.

The Central Bank, however, imposes certain conditions on transactions that are subject to its directives. As a matter of fact, there is legal negligence in the implementation of court orders and the implementation of the rules of the Civil Judgments Enforcement Law, such as auctions and procedures for executing the convicted party. As a result, the application of these provisions is not currently feasible until the instructions of the Central Bank have been approved.

5. Recommendation

The article presents several suggestions aimed at identifying potential solutions based on the information presented above and the significant challenges facing banks and related industries.

- Legislators in each country should enact targeted regulations or amend existing laws and regulations in order to maximize benefits and minimize risks.
- Governments should establish a dedicated entity to investigate the various concerns pertaining to cryptocurrencies, including both centralized and decentralized exchanges, Initial Coin Offerings (ICOs), and cyber-security issues. Furthermore, it is imperative that governments engage in further scholarly research in this area.
- Establish competent adjudicators who understand the nuances pertaining to cryptocurrencies and their associated technologies, thereby facilitating expeditious and secure legal proceedings.
- It is important to increase awareness about the potential risks associated with investing in or using these assets, including their volatility and susceptibility to cyberattacks.
- National cryptocurrencies may be developed by countries, subject to appropriate regulation and supervision. It is the goal of this approach to safeguard and preserve the decentralized nature of these currencies while also maximizing the advantages they provide to individual nations.
- The legal and financial aspects of cryptocurrency need to be further investigated in order to gain a deeper understanding of the issue and come up with more effective solutions.
- As a result, cryptocurrency has become a permanent feature of the financial landscape. Several sectors, including finance and other industries, were intended to be revolutionized by the technology in question.

6. Conclusion

In the past decade, cryptocurrency has emerged as one of the most significant innovations. It is the creators of these entities who have positioned them as potential substitutes or alternatives to the existing financial system. Although cryptocurrencies offer numerous benefits and advantages, a significant number of individuals worldwide continue to view them as a trendy concept, particularly as a result of their benefits, risks, and underlying mechanisms, as discussed in 30BiLD Law Journal 7(1).

A cryptocurrency is a digital currency that operates within a decentralized framework, using cryptographic techniques to ensure transparency and security of the system as well as oversee the creation of currency units known as "blockchains." Throughout the world, blockchain has emerged as a leading topic, representing a

technological advancement that has attracted the attention of governments, financial institutions, and multinational corporations.

To enhance the general public's understanding of this emerging technology, which encompasses transaction validation and mining, it is imperative to explain the workings of the cryptocurrency mechanism. Individuals will be able to contribute to the blockchain by appending blocks and subsequently receiving corresponding rewards as a result of this understanding. Being a novel innovation, cryptocurrencies are endowed with a number of advantages that have the potential to enhance the lives of individuals by providing a greater level of convenience and security.

Nevertheless, cryptocurrencies, like other emerging technologies, face a variety of legal complexities and impediments that must be resolved efficiently in order to enhance and secure the use of these assets. Market demand for low-volatility digital instruments that function as effective risk hedges has driven the emergence of stablecoins. There is now a new philosophy governing the interaction between the various entities involved in financial transactions as a result of this development.

They exhibit low levels of volatility, which is one of their most notable characteristics. There are, however, several potential initiatives for the advancement of stablecoins, both on a national and global scale, depending on the ecosystem participants, the developers' strategic blueprints, and the inherent characteristics of the assets involved in provisioning.

Regardless of the specific concept proposed, it is inherently burdened with a number of significant legal challenges due to the limited capacity of the law to effectively accommodate emerging digital trends.

Bitcoin is not officially legal in Iran, but using it is not a crime. As the highest legal institution in the country, the judiciary monitors and follows up on the law's implementation. After passing laws and resolutions in Parliament, the judiciary usually supervises the implementation of a law after it has been passed. Article 2 of the General Penalty Law states, "Any act or omission that is punishable by law or requires preventative or educational measures is considered a crime, and nothing can be considered a crime without punishment or preventative or educational measures being determined for it according to the law."

Consequently, it is deemed a crime." Consequently, since digital currencies cannot be punished for buying and selling or keeping them, these actions cannot be considered crimes. However, other institutions under the supervision of this organization, such as the police force, are responsible and able to prevent fraud in this area. As well as discussing digital currencies as a technology, the law can provide the necessary follow-up. Earlier this month, the Chairman of the Iranian House of Representatives Economic Commission announced that the Government's Economic Commission had approved Bitcoin's recognition.

The central bank, however, repeatedly prohibits digital currencies entry into the country's payment system. As a general rule, purchasing, selling, and keeping bitcoins is not a crime. However, no special permission has been granted on a large scale and in the field of large payments in the country.

Digital currencies are developing rapidly around the world. In the meantime, a country that can quickly adapt to the changes of the modern world will be less affected by these revolutionary changes. The use of legislation and the coordination of all government agencies to implement these laws are essential for economic dynamism and flexibility.

Taking advantage of this opportunity in developing countries and advancing the process of financial payments for industrial projects, especially those to transfer technology to the destination country, is an objective of Iran, which is not an exception to this rule. There is a need to adopt a set of laws in this field as soon as possible and to implement them in coordination with all of the elements of the system.

References:

Agyei, K.S. 2022. Does volatility in cryptocurrencies drive the interconnectedness between the cryptocurrencies market? Insights from wavelets. Cogent Economics & Finance, vol. 10, no. 1, 2061682.

Afzal, A., Asif, A. 2019. Cryptocurrencies, blockchain and regulation: A review. Lahore J. Economics, vol. 24, no. 1, 103-130.

Ahamad, S., Nair, M., Varghese, B. 2013. A survey on crypto currencies. In: 4th International Conference on Advances in Computer Science, AETACS, pp. 42-48.

Ahamad, S., Gupta, P., Acharjee, B.P., Kiran, P.K., Khan, Z., Hasan, F.M. 2022. The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market. Mater. Today Proc., vol. 56, 2070-2074.

Ahmed, S.W., Mehmood, A., Sheikh, T., Bachaya, A. 2022. Unveiling the linkages between emerging stock market indices and cryptocurrencies. Asian Acad. Manag. Journal, vol. 27, no. 2, 189-209.

Alfieri, C. 2023. Cryptocurrency and National Security. Semantic Schoolar, Corpus ID: 247142739. DOI:10.18278/ijc.9.1.3.

Almaqableh, L., et al. 2022. Is it possible to establish the link between drug busts and the cryptocurrency market? Yes, we can. Int. J. Inf. Management, p. 102488.

Allen, F., Gu, X., Jagtiani, J. 2022. Fintech, cryptocurrencies, and CBDC: Financial structural transformation in China. J. Int. Money Finance, vol. 124, 102625.

Almashhadani, A.H., Almashhadani, M. 2022. The Impact of Financial Technology on Banking Performance: A study on Foreign Banks in UAE. Int. J. Sci. Manag. Res., vol. 6, no. 01, 1-21.

Ante, L. 2021. Smart contracts on the blockchain--A bibliometric analysis and review. Telemat. Informatics, vol. 57, p. 101519.

Benigno, P., Schilling, M.L., Uhlig, H. 2022. Cryptocurrencies, currency competition, and the impossible trinity. J. Int. Econ., vol. 136, p. 10360.

Boiardi, P., Stout, E. 2021. To what extent can blockchain help development co-operation actors meet the 2030 Agenda? OECD, Paris. In: Development Co-operation Working Papers, No. 95. https://doi.org/10.1787/11857cb5-en.

Boo, L.H., Chan, H.T. 2022. Dividend Payout Policy and Global Financial Crisis: A Study on Asian Non-Financial Listed Companies. Asian Econ. Financ. Rev., vol. 12, no. 10, pp. 848-863.

Bouoiyour, J., Selmi, R., Tiwari, K.A., Olayeni, R.O., et al. 2016. What drives Bitcoin price. Econ. Bull., vol. 36, no. 2, pp. 843-850.

Brady, A.S., Goetz, R.A., Jonas, G.E.A. 2022. Public-private partnerships in Denver, CO: analysis of the role of PPPs in the financing and construction of transportation infrastructure in the USA. Handbook Public Priv. Partnerships Transp. Vol I Airports, Water Ports, Rail, Buses, Taxis, Finance, pp. 195-222.

Bray, J. 2016. Anonymity, Cybercrime and the Connection to Cryptocurrency. Eastern Kentucky University.

Brenner, W.S., Schwerha IV, J.J. 2001. Transnational evidence gathering and local prosecution of international cybercrime. J. Marshall J. Comput. & Info. L., vol. 20, p. 347.

Brown, D.S. 2016. Cryptocurrency and criminality: The Bitcoin opportunity. Police J., vol. 89, no. 4, pp. 327-339.

Bunjaku, F., Gjorgieva-Trajkovska, O., Miteva-Kacarski, E. 2017. Cryptocurrencies--advantages and disadvantages. J. Econ., vol. 2, no. 1, pp. 31-39.

Campbell-Verduyn, M. 2017. Bitcoin and beyond: Cryptocurrencies, blockchains and global governance. Taylor & Francis.

Chen, J., Siddik, A.B., Zheng, W.G., Masukujjaman, M., Bekhzod, S. 2022. The effect of green banking practices on banks' environmental performance and green financing: an empirical study. Energies, vol. 15, no. 4, p. 1292.

Chhabra, V., Bathla, S., Maheshwari, H. 2019. An overview of blockchain technology and comparison between various cryptocurrencies. J. Emerg. Technol. Innov. Res, vol. 6, 68-71.

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., Shah, M. 2022. A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. Ann. Data Sci., pp. 1-33.

Christin, N. 2013. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd international conference on World Wide Web, 2013, pp. 213-224.

Cong, W.L., Harvey, C.R., Rabetti, D., Wu, Y.Z. 2023. An anatomy of crypto-enabled cybercrimes. Available at SSRN: https://ssrn.com/abstract=4188661 or http://dx.doi.org/10.2139/ssrn.4188661.

Cong, W.L., Grauer, K., Rabetti, D., Updegrave, H. 2023. Blockchain Forensics and Crypto-Related Cybercrimes. Available at SSRN 4358561.

Cong, W.L., He, Z. 2019. Blockchain disruption and smart contracts. Rev. Financ. Stud., vol. 32, no. 5, 1754-1797.

Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al. 2016. Blockchain technology: Beyond bitcoin. Appl. Innov., vol. 2, no. 6-10, p. 71.

Curi, F.M., de Pinto, F.J.P., da Cunha, D.P.J., de Freitas, R.R. 2022. Economic and financial analysis of a grid-connected PV system in Rio de Janeiro for residential and commercial supply. Int. J. Sustain. Econ., vol. 14, no. 4, pp. 411-428.

Daoud, E. 2019. Decentralizing of transparency: using blockchain to reduce counterfeiting. In: 17th International Conference e-Society 2019At: Utrecht, The Netherlands. DOI: 10.33965/es2019_201904L011.

Decker, C., Wattenhofer, R. 2014. Bitcoin transaction malleability and MtGox. In: Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11. Proceedings, Part II 19, 2014, pp. 313-326.

Desalegn, G., Tangl, A. 2022. Enhancing green finance for inclusive green growth: a systematic approach. Sustainability, vol. 14, no. 12, 7416.

DeVries, D.P. 2016. An analysis of cryptocurrency, bitcoin, and the future. Int. J. Bus. Manag. Commer., vol. 1, no. 2, pp. 1-9.

Di Vaio, A., Hassan, R., Palladino, R. 2023. Blockchain technology and gender equality: A systematic literature review. Int. J. Inf. Manage., vol. 68, p. 102517.

du Plessis, P. 2014. The Nature of Decentralized Virtual Currencies: Benefits, Risks and Regulations. Master Int. Law Econ. World Trade Inst.

DuPont, Q. 2017. Cryptocurrencies and blockchains. John Wiley & Sons.

Edwards, M. 2021. Cybercrime and the Asia-Pacific Region. The Aracari Project. https://washingtonstateinvestigators.com/wp-content/uploads/2023/01/Cybercrime-and-Scams-in-the-Asia-Pacific-Region.pdf.

Farell, R. 2015. An analysis of the cryptocurrency industry. Scholarly Commons. https://repository.upenn.edu/handle/20.500.14332/49177.

Fernandes, S.H.L., Bouri, E., Silva, L.W.J., Bejan, L., de Araujo, A.H.F. 2022. The resilience of cryptocurrency market efficiency to COVID-19 shock. Phys. A Stat. Mech. its Appl., vol. 607, p. 128218.

Gadekallu, R.T., et al. 2022. Blockchain for the metaverse: A review. arXiv Prepr. arXiv2203.09738.

Gatti, S. 2023. Project finance in theory and practice: designing, structuring, and financing private and public projects. Elsevier.

Ghosh, A., Gupta, S., Dua, A., Kumar, N. 2020. Security of Cryptocurrencies in blockchain technology: State-of-art, challenges, and future prospects. J. Networks. Computer Applications, vol. 163, p. 102635.

Giudici, P., Abu-Hashish, I. 2019. What determines bitcoin exchange prices? A network VAR approach. Financ. Res. Lett., vol. 28, pp. 309-318.

Gjems-Onstad, O. 1996. The legal framework and taxation of Scandinavian non-profit organisations. Volunt. Int. J. Volunt. Nonprofit Organ., vol. 7, no. 2, pp. 195-212.

Goodfriend, M., King, G.R. 1988. Financial deregulation, monetary policy, and central banking. Fed. Reserv. Bank Richmond Work. Pap., no. 88-1.

Guadamuz, A., Marsden, C. 2015. Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. First Monday, vol. 20, no. 12-7.

Guo, K., Zhang, X. Kuai, X., Wu, Z., Chen, Liu, Y. 2020. A spatial Bayesian-network approach as a decision-making tool for ecological-risk prevention in land ecosystems. Ecol. Modelling, vol. 419. doi: 10.1016/j.ecolmodel.2019.108929.

Haferkorn, M., Quintana Diaz, M.J. 2015. Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and namecoin in Enterprise Applications and Services in the Finance Industry: 7th International Workshop, FinanceCom 2014, Sydney, Australia, December 2014, Revised Papers 7, 106-120.

Hassan, A., AlMaghaireh, I.A., Islam, S.M. 2022. Islamic Financial Markets and Institutions. Taylor & Francis.

Hewa, T., Ylianttila, M., Liyanage, M. 2021. Survey on blockchain based smart contracts: Applications, opportunities and challenges. J. Netw. Comput. Appl., vol. 177, p. 102857.

Higbee, A. 2018. The role of crypto-currency in cybercrime. Comput. Fraud & Secur., vol. 2018, no. 7, pp. 13-15.

Houben, R., Snyers, A., et al. 2018. Cryptocurrencies and blockchain. Legal Context Implications, Financial crime, Money Laundering tax Evasion. European Parliament, Policy Department for Economics, Scientific and Quality of Life Policies, 1-86.

Hu, J., Luo, Q., Zhang, J. 2020. The fluctuations of bitcoin price during the hacks. Int. J. Appl. Res. Manag. Econ., vol. 3, no. 1, pp. 10-20.

Islam, M.M., Islam, K.M., Shahjalal, M., Chowdhury, Z.M., Jang, M.Y. 2023. A low-cost cross-border payment system based on auditable cryptocurrency with consortium blockchain: Joint digital currency. IEEE Trans. Serv. Comput., vol. 16, no. 03, pp. 1616–1629.

Ismael, R. 2021. Challenges and Opportunities Cryptocurrency in Iran Economy & E-Businesses. Вестник Российского университета дружбы народов. Серия: Экономика, vol. 29, no. 4, pp. 689-698.

Jalan, A., Matkovsky, R. 2023. Systemic risks in the cryptocurrency market: Evidence from the FTX collapse. Financ. Res. Lett., vol. 53, 103670.

Katterbauer, K., Hassan, S., Cleenewerck, L. 2022. Financial cybercrime in the Islamic finance metaverse. J. Metaverse, vol. 2, no. 2, pp. 56-61.

Khan, A., Goodell, W.J., Hassan, K.M., Paltrinieri, A. 2022. A bibliometric review of finance bibliometric papers. Financ. Res. Lett., vol. 47, p. 102520.

Krichen, M., Ammi, M., Mihoub, A., Almutiq, M. 2022. Blockchain for modern applications: A survey. Sensors, vol. 22, no. 14, p. 5274.

Laurence, T. 2023. Blockchain for dummies. John Wiley & Sons.

Liu, Y., Tsyvinski, A. 2021. Risks and returns of cryptocurrency. Rev. Financ. Stud., vol. 34, no. 6, pp. 2689-2727.

Maese, A.V., Avery, W.A., Naftalis, A.B., Wink, P.S., Valdez, D.Y. 2016. Cryptocurrency: A primer. Bank. Lj, vol. 133, p. 468.

Mahdavieh, R. 2022. State Adoption of Cryptocurrency: a Case Study Analysis of Iran, Russia, and Venezuela. Am. J. Undergrad. Res., vol. 19, no. 1.

Makam, G. 2023. Cybercrime and Electronic Evidence in India: A Comprehensive Analysis. Available at SSRN 4475784.

Malloy, H.T., Osipov, A., Vizi, B. 2015. Managing diversity through non-territorial autonomy: Assessing advantages, deficiencies, and risks. Oxford Academic; Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198738459.001.0001.

Maras, H.M., et al. 2015. Computer forensics. Jones and Bartlett Learning.

Maresti, D., et al. 2023. The Role of Sustainability Accounting in Realizing The Ward's Sustainable Development Goals (SDGs): A Case Study on Utilizing of Ward Budget Direct Cash Assistance (BLT-DD) in Agam District. Asia Pacific J. Bus. Econ. Technol., vol. 3, no. 01, 31-42.

Margariti, S. 2011. The deficiencies of the International legal framework in the protection of children from recruitment and use in hostilities. UCL Hum. Rts. Rev., vol. 4, p. 90.

Meunier, S. 2018. Blockchain 101: What is blockchain and how does this revolutionary technology work? In: Transforming climate finance and green investment with Blockchains, pp. 23-34. Elsevier.

Mittal, K.S. 2022. Behavior biases and investment decision: theoretical and research framework. Qual. Res. Financ. Mark., vol. 14, no. 2, pp. 213-228.

Mnif, E., Jarboui, A. 2022. Resilience of Islamic cryptocurrency markets to Covid-19 shocks and the Federal Reserve policy. Asian J. Account. Res., vol. 7, no. 1, 59-70.

Monteiro, A., Cepêda, C., Silva, A. 2022. EU Non-Financial Reporting Research. Int. J. Financ. Accounting, Manag., vol. 4, no. 3, pp. 335-348.

Mohanta, K.B., Panda, S.S., Jena, D. 2018. An overview of smart contract and use cases in blockchain technology. In: 2018 9th international conference on computing, communication and networking technologies (ICCCNT), 2018, pp. 1-4.

Nayak, C.S., Nayak, K.S. 2022. A Hybrid ANN with Rao Algorithm Based Optimization (RA+ ANN) for Short Term Forecasting of Crypto Currencies. In: Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2021, 362-373.

Nicholls, J., Kuppa, A., Le-Khac, A.N. 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access, vol. 9, pp. 163965-163986.

Nguyen, T.V., Doan, T.N. 2022. Open account, import decision and financial constraints: A cross-country firm-level study. Int. J. Financ. & Economics, 28(4), 3918-3937.

Nofer, M., Gomber, P., Hinz, O., Schiereck, D. 2017. Blockchain. Bus. & Inf. Syst. Eng., vol. 59, 183-187.

Norena-Chavez, D., Thalassinos, I.E. 2023. Impact of big data analytics in project success: Mediating role of intellectual capital and knowledge sharing. Journal of Infrastructure, Policy and Development, Vol 7, Issue 3, Article ID: 2583. https://doi.org/10.24294/jipd.v7i3.2583.

Pasdar, A., Lee, C.Y., Dong, Z. 2023. Connect API with blockchain: A survey on blockchain oracle implementation. ACM Comput. Surv., vol. 55, no. 10, pp. 1-39.

Pawlik, L., Płaza, M., Deniziak, S., Boksa, E. 2022. A method for improving bot effectiveness by recognising implicit customer intent in contact centre conversations. Speech Commun., vol. 143, pp. 33-45.

Pessa, B.A.A., Perc, M., Ribeiro, V.H. 2023. Age and market capitalization drive large price variations of cryptocurrencies. Sci. Rep., vol. 13, no. 1, p. 3351.

Rabbani, M.R., Khan, S., Thalassinos, E.I. 2020. FinTech, blockchain and Islamic finance : an extensive literature review. International Journal of Economics and Business Administration, 8(2), 65-86.

Rajasekaran, S.A., Azees, M., Al-Turjman, F. 2022. A comprehensive survey on blockchain technology. Sustain. Energy Technol. Assessments, vol. 52, p. 102039.

Ranjbar Fallah, R.M., Foroughi, M. 2020. Analysis of Opportunities and Threats in the Process of Legislating Blockchain Technology and Cryptocurrencies in Iran Based on the PEST Model. Def. Econ., vol. 5, no. 17, pp. 133-158.

Reddy, E., Minnaar, A. 2018. Cryptocurrency: A tool and target for cybercrime. Acta Criminol. African J. Criminol. & Vict., vol. 31, no. 3, pp. 71-92.

Rezaeinejad, I. 2021. Challenges and opportunities cryptocurrency in Iran economy \& e-businesses. Rudn J. Econ., vol. 29, no. 4, 689-698.

Rubinacci, C. 2022. Cryptocurrencies and stablecoins: a potential harm to ECB monetary policy: is a digital euro the solution? Tesi di Laurea in Macroeconomic analysis, Luiss Guido Carli, relatore Pietro Reichlin, pp. 140. Master's Degree Thesis.

Rupeika-Apoga, R., Thalassinos , E.I. 2020. Ideas for a regulatory definition of FinTech. International Journal of Economics and Business Administration, 8(2), 136-154.

Sahoo, K.P., Sethi, D. 2022. Market efficiency of the cryptocurrencies: Some new evidence based on price--volume relationship. Int. J. Finance & Economics. DOI:10.1002/ijfe.2744. Corpus ID: 254956513.

Sapovadia, V. 2015. Legal issues in cryptocurrency. In: Handbook of Digital Currency, 253-266. Elsevier.

Șcheau, C.M., Cruaciunescu, L.S., Brici, I., Achim, V.M. 2020. A cryptocurrency spectrum short analysis. J. Risk Financ. Manag., vol. 13, no. 8, p. 184.

Sen Gupta, S. 2017. Blockchain. IBM Online. http//www.IBM.COM.

Singh, J., Sajid, M., Gupta, K.S., Haidri, A.R. 2022. Artificial Intelligence and Blockchain Technologies for Smart City. Intell. Green Technol. Sustain. Smart Cities, pp. 317-330.

Shah, S.M.F.A., et al. 2023. On the Vital Aspects and Characteristics of Cryptocurrency: A Survey. IEEE Access, vol. 11, pp. 9451-9468.

Smales, A.L. 2020. One cryptocurrency to explain them all? Understanding the importance of Bitcoin in cryptocurrency returns. Econ. Pap. A J. Appl. Econ. policy, vol. 39, no. 2, 118-132.

Sultan, N. Mohamed, N., Martin, M., Latif, M.H. 2023. Virtual currencies and money laundering: existing and prospects for jurisdictions that comprehensively prohibited virtual currencies like Pakistan. J. Money Laund. Control.

Taghizadeh-Hesary, F., et al. 2022. Green finance and the economic feasibility of hydrogen projects. Int. J. Hydrogen Energy, vol. 47, no. 58, pp. 24511-24522.

Tavakolan, M., Nikoukar, S. 2022. Developing an optimization financing cost-scheduling trade-off model in construction project. Int. J. Constr. Manag., vol. 22, no. 2, pp. 262-277.

Tinsley, R. 2022. Advanced Project Financing Structuring Risk. Euromoney Institutional Investor PLC.

Thalassinos, I.E., Venediktova, B., Zampeta, V. 2015. Applications of M-GARCH Model for the Selection of Securities of Banks' Investment Portfolio. Applied Economics and Finance, 2(2), 1-13.

Thayer, B.J. 1987. Legal Tender. Harv. L. Rev., vol. 1, p. 73.

Tredinnick, L. 2019. Cryptocurrencies and the blockchain. Bus. Inf. Rev., vol. 36, no. 1, 39-44.

Treleaven, P., Brown, G.R., Yang, D. 2017. Blockchain technology in finance. Computer (Long. Beach. Calif)., vol. 50, no. 9, 14-17.

Vasek, M. 2015. The age of cryptocurrency. American Association for the Advancement of Science. Science, Vol 348, Issue 6241, pp. 1308-1309. DOI: 10.1126/science.aab2001.

Von Bogdandy, A., Ioannidis, M. 2014. Systemic deficiency in the rule of law: what it is, what has been done, what can be done. Common Mark. Law Rev., vol. 51, no. 1.

Von Bogdandy, A. 2020. Principles of a systemic deficiencies doctrine: how to protect checks and balances in the member states. Common Mark. Law Rev., vol. 57, no. 3.

Vujičić, D., Jagodić, D., Randjić, S. 2018. Blockchain technology, bitcoin, and Ethereum: A brief overview. In: 2018 17th international symposium infoteh-jahorina (infoteh), pp. 1-6.

Underwood, S. 2016. Blockchain beyond bitcoin. Commun. ACM, vol. 59, no. 11, pp. 15-17.

Usman, A., Hassan, M., Rehman, U.Z., Sial, Q.A. 2022. Legal framework in aid of biological diversity and statutory deficiencies in Pakistan. Brazilian J. Biol., vol. 84.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, Y.F. 2019. Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans. Syst. Man, Cybern. Syst., vol. 49, no. 11, 2266-2277.

Wang, Y., Wei, Y., Lucey, M.B., Su, Y. 2023. Return spillover analysis across central bank digital currency attention and cryptocurrency markets. Res. Int. Bus. Financ., vol. 64, p. 101896.

Wright, A., De Filippi, P. 2015. Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664.

Yousefi, S., Tosarkani, M.B. 2022. An analytical approach for evaluating the impact of blockchain technology on sustainable supply chain performance. Int. J. Prod. Econ., vol. 246, p. 108429.

Yuan, Y., Wang, Y.F. 2018. Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Trans. Syst. Man, Cybern. Systems, vol. 48, no. 9, 1421-1428.

Zagaris, B., Mostaghimi, A. 2023. Cybercrime and Transnational Organized Crime. IELR, vol. 39, p. 90.

Zimba, A., Wang, Z., Chen, H., Mulenga, M. 2019. Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks. KSII Trans. Internet Inf. Syst., vol. 13, no. 6, pp. 3258-3279.

Zhang, C., Diao, W. 2013. Deficiencies of China's general aviation law and its Improvement. Korean J.
Air Sp. Law Policy, vol. 28, pp. 145-181.

Zhu, J. Cao, J., Saxena, D., Jiang, S., Ferradi, H. 2023. Blockchain-empowered federated learning: Challenges, solutions, and future directions. ACM Comput. Surv., vol. 55, no. 11, pp. 1-31.

Zohuri, B., Nguyen, T.H., Moghaddam, M. 2022. What is the Cryptocurrency? Is it a Threat to Our
National Security. Domest. Glob., 1-14.