ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 13 (2023) No. 5, pp. 276-293
DOI:10.33168/JSMS.2023.0518

The Potential Risks of Mining and Investment in Digital Currencies based on Financial Technology Applications

Mohammad Yousef

Jordan University, Amman, Jordan

moh.yousef@ju.edu.jo

Abstract. The objective of this study was to explore the potential risks associated with mining and investing in digital currencies through financial technology (fintech) applications. The research approach employed a combination of quantitative and qualitative methods, utilizing an inductive-deductive framework. The researcher conducted online surveys, and interviews with professors and experts, and analyzed the collected data using Microsoft Excel and NVIVO software. The study also utilized illustrative graphs of digital currency markets, computing power charts, and energy consumption indexes related to digital currency mining. The findings revealed various potential risks of mining and investing in digital currencies, impacting individuals, businesses, and ecosystems. These risks encompass environmental concerns, excessive energy consumption, security vulnerabilities, and financial losses. Additionally, investing in digital currencies through fintech applications can lead to inadequate investor protections, market volatility, regulatory challenges, fraudulent activities, lack of transparency, and insufficient investor understanding. The value of this study lies in its ability to analyze the potential risks associated with mining and investing in digital currencies, offering valuable insights for individuals, businesses, and policymakers. It can aid stakeholders in making informed decisions, developing risk management strategies, and enhancing their overall understanding of the potential implications on individuals, businesses, and the ecosystem.

Keywords: digital currencies, mining, investing, fintech applications, risks.

1. Introduction

With the spread of digital currency trading globally, especially the Bitcoin currency, it has become an obsession for many individuals to invest in, especially since the price of Bitcoin has risen rapidly since the beginning of October 2020, exceeding 2000%, bringing its market price to nearly $65,000 in mid-April 2021. The (JOPACC) Foundation, a non-governmental organization affiliated with the World Bank, had the greatest impact in the direction of many individuals to trade online, through its development of the financial technology system, such as the development of electronic payment methods and electronic wallets that were not present strongly before the Corona pandemic. This coincided with the fact that international companies such as (Tesla), (Dell) and (Microsoft) Corporations pumped huge funds to support the Bitcoin currency, which gave it wide popularity at the global and local levels. As a result, Arab governments, including Jordan, began to fear the potential risks of trading digital currencies, as Jordan is a developing country with a weak economy and infrastructure that barely serves the local community.

Jordan is among the Arab countries that have illegalized forex trading and trading digital currencies over the Internet, although it imposes a strict control system on brokerage firms that work in this field through the Jordan Securities Commission (JSC), which is the official body entrusted with approving this category of companies. Digital currency trading companies in Jordan are not licensed and approved locally. In fact, they are global trading companies that are not officially represented by offices or headquarters within Jordanian territory, but they managed to attract a large segment of Jordanian traders as the only outlet for those wishing to invest in digital currency trading Online.

In 2014 the Central Bank of Jordan issued a circular prohibiting local banks and all other financial institutions under its supervision and control from dealing with digital currencies in any way, exchanging them for other currencies, opening accounts for customers and investors to deal with them, sending or receiving remittances against them or for the purpose of purchasing or selling it; Being currencies that are not legal because there is no obligation on the central bank to exchange their value against money issued by the government or against globally traded commodities such as gold. In the same context, the Jordan Telecommunications Regulatory Commission (JTRC) has imposed strict control over the circulation of digital currency mining devices inside the Kingdom.

Based on the previous explanation, this study aimed to shed light on the potential risks of mining and investment in digital currencies based on financial technology Applications, where the researcher drew a visualized model that shows the risks reflected on individuals, businesses, and ecosystems. These potential risks were summarized by financial, technical, and law/societal risks aspects, where the researcher answered the following questions:

1- What are the potential risks associated with mining in digital currencies based on Fintech applications on (individuals, businesses, and ecosystems)?

2- What are the potential risks associated with an investment in digital currencies based on Fintech applications on (individuals, businesses, and ecosystems)?

2. Theoretical Framework

This study is based on several models and figures to provide a deep insight into the potential risks of mining and investing in digital currencies through financial technology applications. This study used the Diffusion of innovative spread (DOI) as a theoretical framework. Digital innovation (DI) is present in various stages of IT projects, such as design, implementation, operation, and maintenance. Recent studies indicate that DI incorporates sociotechnical elements that relate to users' understanding and utilization of specific features in digital technology (Tung et al., 2022). This theory was developed by Professor Everett Rogers starting in 1962. This theory has been refined and widely used to explain the process of any innovative technology adoption. Its main objective is to support individuals and organizations in the process of adopting new innovative technologies. Diffusion is a process by which

"innovation" is communicated through "certain channels" within the "time" of members of a "community". (Odeh and Yousef, 2021). The innovation-decision process consists of five phases: knowledge, persuasion, decision, implementation, and confirmation phase (Dube and Gumbo, 2017), these phases are represented as shown in Figure 1.

In the knowledge stage, individuals or organizations become aware of the existence and potential benefits of mining and investment in digital currencies through various sources such as media, research articles, or word-of-mouth. The risks can be studied by examining the available knowledge about the technology, its underlying principles, security vulnerabilities, regulatory frameworks, historical incidents, and expert opinions. Therefore, this stage is very useful for the author to identify potential risks associated with mining and investing in digital currencies.

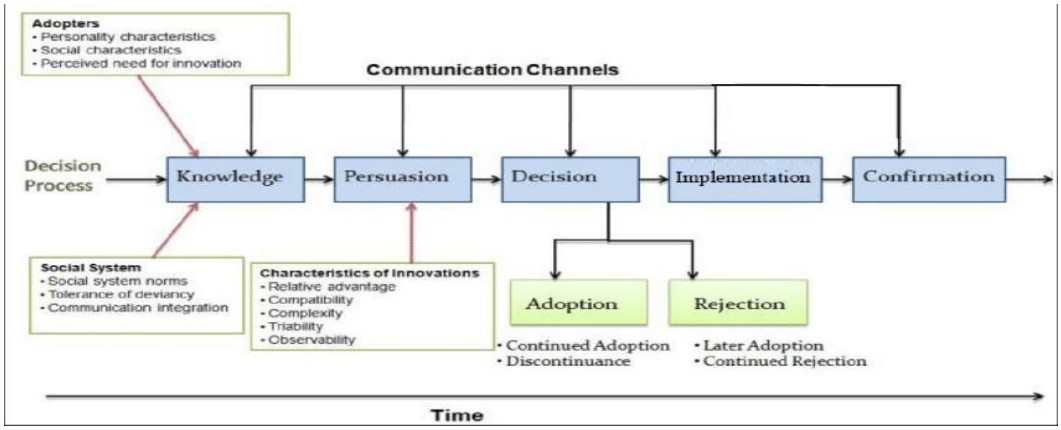

Fig. 1: The Innovation Diffusion Process., Source: Rogers (2004) and Chang (2010).

In the persuasion stage, once individuals or organizations acquire knowledge about mining and investment in digital currencies, the persuasion phase comes into play. During this phase, potential adopters evaluate the advantages and disadvantages of the innovation and its associated risks. Surveys, interviews, or focus groups can be conducted to understand the perceptions and attitudes of individuals toward digital currencies. This phase helps in identifying the concerns, doubts, and risk perceptions that potential investors and miners may have. In the decision stage, individuals or organizations make a choice regarding whether to adopt mining and investment in digital currencies. This phase can be studied by examining the factors influencing the decision-making process. Moreover, analyzing the decision criteria, risk assessment methods, and risk management strategies employed by potential adopters. This phase provides insights into how individuals weigh the risks and benefits and make decisions related to mining and investment in digital currencies. In the implementation stage, after the decision to adopt mining and investment in digital currencies is made, the implementation phase begins. This phase involves the practical application of the decision, such as setting up mining rigs, establishing investment portfolios, and engaging with cryptocurrency exchanges. The actions taken by individuals or organizations can be analyzed in this phase to mitigate the identified risks. Moreover, can examine the security measures implemented, compliance with regulatory requirements, and the overall operational strategies employed during the implementation process. In the confirmation stage, the confirmation phase occurs after the implementation, where individuals or organizations evaluate the outcomes and consequences of their decision to adopt mining and investment in digital currencies. Analyzing the performance of digital currency investments, assessing the effectiveness of risk mitigation strategies, and monitoring the occurrence of any unexpected risks can be conducted in this phase. Not to mention understanding the long-term impact and risks associated with mining and investment in digital currencies.

3. Literature Review

3.1. Digital currency overview

Digitization has reached the monetary system through the emergence of encrypted assets such as (Bitcoin and Ether), as it revealed many features that can be provided by these digital assets based on distributed ledger technologies (DLTs), where the use of (DLTs) can lead to Enhancing sensitive financial transaction data as well as increasing the speed of transactions through faster processing and settlement, and automating many business processes through smart contracts (Klein et al., 2020). (DLT) has started as one of the most disruptive technologies in the past decade. This technology promises to change the way people do business, track their products, and manage their personal data (Chowdhury et al., 2019). In addition, (DLT) can be referred to as a consensus on the digital data that are copied, shared, concurrent, and geographically dispersed across several locations, countries, or multiple institutions. Where the database of (DLT) is spread across several nodes (devices) on (peer-to-peer) networks, where each of them duplicates and saves an identical copy of the ledger and updates itself independently (Ward and Rochemont, 2019). However, mentioned potential benefits and implications of using distributed ledger technologies (DLTs), such as Bitcoin and Etherthe need further investigation to enhance financial transactions, increase transaction speed, automate business processes, and change the way people conduct business, track products, and manage personal data.

Key characteristics of DLT include encompassing, security (depending on the laws in each jurisdiction), and privacy (monitoring of transactions to prevent fraud due to its centralized design) (Ward and Rochemont, 2019). Making DLT suitable for addressing the needs of several industries and applications that require these characteristics (Klein et al., 2020). Depending on the application domains, different ledger deployment strategies can be pursued. Relying on these strategies; there are two predominant ledger types, Public (non-permissioned ledger) and Private (permissioned ledger). In addition, a distributed ledger provides several properties that make it a suitable candidate for several application domains including the digital evidence chain. Such as distributed consensus on the ledger state, immutability and irreversibility of the ledger state, data (transaction) persistence, data provenance, distributed data control, accountability, and transparency (Chowdhury et al., 2019). However, further investigation and understanding of the specific application domains and deployment strategies of distributed ledger technology (DLT) are necessary in order to effectively address the needs of different industries and applications requiring characteristics such as security, privacy, distributed consensus, immutability, and transparency.

The proliferation of private-sector digital currencies and their potential risks to financial stability and monetary policy. in addition the response of central banks and monetary authorities, who are conducting research and experiments on central bank-issued digital currencies (CBDCs) to address these concerns. there are many research provides a comprehensive survey of completed CBDC experiments using distributed ledger technology (DLT), which would provide insights into motivations, best practices, technical feasibility, and challenges of implementing DLT-based CBDCs (Opare and Kim, 2020). Blockchain technology gained popularity with the introduction of Bitcoin in 2009, which was the first widely adopted cryptocurrency. Blockchains have the ability to store transaction records securely and transparently, while also introducing the development of consortium blockchains as a hybrid form of public and private methods for increased fairness and scalability (Seo et al., 2022). Cryptocurrencies like Bitcoin are the most popular blockchain application. There are services similar to currencies that can rely on blockchains, such as securities transactions, loyalty point services, prepaid cards, gift card exchanges, and e-vouchers. However, due to its structure and application, blockchain has many benefits such as anonymity, persistence, and decentralization and can be applied to various fields and problems (Juričić et al., 2020).

Hyperledger Fabric, and Corda, are two popular blockchain platforms, that cater to enterprise needs by offering features like privacy, scalability, flexibility, and confidentiality. Hyperledger Fabric focuses on executing smart contracts and supporting consensus algorithms, while Corda prioritizes secure and

private transactions between businesses, emphasizing the concept of "smart contracts" and addressing legal validity concerns. some research suggests hybrid approaches that combine blockchain platforms with NoSQL data stores to enable the support of previously infeasible financial services. However, a need to further research and development to explore hybrid approaches that combine Blockchain platforms with NoSQL data store systems, enabling the storage and management of large volumes of data while ensuring temporal integrity, thereby expanding the potential for supporting a wide range of financial services with blockchain technology (Garcia Bringas et al., 2020, Opare and Kim, 2020).

3.2. Central bank digital currencies (CBDCs) issues

The basis of the monetary system used is physical cash, which is printed only by the central bank to give it a legal character. Since the repeal of the gold standard in the early seventies of the last century, cash is no longer backed by gold. Rather, it is only issued by central banks either through lending or through purchasing assets such as government bonds. Central banks do not issue cash proactively, but rather reactively in response to the expansion of commercial banks 'funds and driven by customer demand (Klein et al., 2020). Extending the last century, financial innovations and technologies are ongoing in new forms such as banknotes, coins, and checks issued by Central Bank (Auer et al., 2020).

The central bank aims to maximize social welfare, defined as the sum of household utilities $W = \int_{i\in[0,1]} U_i(j^*(i))di$,

where $j^*(i)$ denotes the payment instrument selected by household i In doing so, the central bank decides whether to introduce a CBDC, and if introduced, its design characteristics (θ, r_{cbdc}). If a CBDC is introduced, the central bankís design problem is given by

$$\max_{\theta\in[0,1],r_{cbdc}} \int_{i\in[0,1]} U_i(j^*(i))di,$$

subject to a design constraint $s_{cbdc} \geq \bar{s}$, which ensures that there is sufficient uptake of the CBDC to overcome network effects (Agur et al., 2021). The recent debate about monetary reform has taken a new turn with the development of technology and techniques that use digital currencies compared to the first principles of money and finance and the state of financial regulation to ensure the provision of a secure monetary asset and a stable supply of credit within a financial system that is unstable in nature (Dow, S., 2019).

The CBDC provides safer currency for transactions and deposits than those that are dealt with by a bank that has commercial risks. Commercial banks are usually not fully backed by reserves as part of their loan-making and market operations role. These risks became significantly higher during the global financial crisis as people moved to withdraw their money and preferred to keep it rather than deposit it (Ward and Rochemont, 2019). The central bank can issue tokens for cryptocurrencies (it refers to a type of digital asset that uses distributed ledger, or blockchain, technology to enable a secure transaction) that are restricted in use among a narrow subset of financial companies, as this use is confined to the core of the financial system, such as large-value payments and settlements between select groups of financial institutions. Some central banks (such as the Central Bank of Canada and the Monetary Authority of Singapore) have tested a prototype token-based CBDC "Wholesale" transaction (Duffie, D., 2019).

CBDCs rely on four characteristics: issuer of money (central bank or not); forms (digital or physical); accessibility (widely or restricted) and technology (account-based or token-based) (Opare and Kim, 2020). There are some potential drivers for developing CBDC linked to a number of factors that affect a country's technological capacity to develop and deploy CBDC. Focusing on the following indicators: Digital infrastructure: such as mobile phones or the internet, Innovation capacity like the new CBDC ecosystem, and Institutional quality. On the other hand, countries vary in their perceived needs for digital currencies issued by central banks, thus requirements are represented by the following indicators: Development and financial inclusion, Public interest in CBDCs, and Cross-border transactions (Auer et al., 2020).

3.3. Financial Technology Applications

The financial technology (FinTech) market is developing quickly alongside the development of new companies or data innovation-based organizations that can straightforwardly execute with clients or providers without going through direct financial administrations. The worldwide watchdog and strategy proposals supplier on the worldwide monetary framework, the Financial Stability Board (FSB) divides FinTech into four categories based on the type of innovation: 1) Payment, Settlement, and Clearing, 2) Market Aggregator, 3) Risk and Investment Management, and 4) Crowdfunding and Peer to Peer (p2p) Lending (Abdillah, L., 2019).

Technological change that produces financial innovations in banking has implications for improvements in fintech. Non-intermediated peer-to-peer (P2P) loaning, digital currencies, and smart agreements are altogether parts of an arising new mosaic of innovation that helped altered monetary administrations (Thakor, A. V., 2020). For example, M-Pesa, Bitcoin, and blockchain were accompanied and followed by many other financial innovations in a wide range of areas, from payments and peer-to-peer lending, through crypto-assets and Robo-advisors, to regulatory technology. Thousands of start-ups, funded by tens of billions of US dollars, focused on such innovations and have sprung up around the world in developed, emerging, and developing economies (Knight and Wójcik, 2020).

Historically, the applications of financial technology developed during three phases until they reached the form that we know today. Figure 2 has been suggested that there have been three phases of fintech. By the Figure 2 historical scheme, many people might be astonished to hear that fintech truly began around the late nineteenth century, when promising finance innovators attempted to propel how financial information is imparted to their local area. The connection made between monetary establishments and public transport changed the manner in which banks had the option to speak with their clients and permitted extensions for a bigger scope. The improvement of mainstream telephone and broadband communication took into account better approaches to sending and receiving money, with the first electronic fund transfer occurring in 1918. Global transport and communication frameworks were solidified by 1950, making an establishment by which the world could begin building advanced financial institutions and products to change the manner in which we communicate with our money (Sofie and Robert , 2018).

Using financial technology has achieved many advantages such as Lower search expenses of matching transacting parties, accomplish economies of scale in get-togethers and utilizing enormous information, achieving cheaper and more secure information transmission; and reducing verification costs (Thakor, A. V., 2020). There are many characteristics that give institutions, investors, and individuals a unique opportunity to benefit from financial technology platforms, and these characteristics are as follows: Cyber security (Hardware or software used to protect financial privacy), Mobile transactions such as smartphones, Data analytics (algorithms that facilitate the analysis of consumer financial data), Blockchain, Peer-to-peer (P2P) (platforms that facilitate consumer-to-consumer financial transactions), Robo-advising (programs that provide automated investment advice to customers or portfolio managers), and Internet of things (IoT) (Technologies relating to smart devices that gather data in real-time and communicate via the internet) (Chen et al., 2019).

The complexity of fintech ecosystems arises from the interplay between various stakeholders, technologies, regulations, and market dynamics. the lack of knowledge regarding their emergence needs more Navigating this complexity requires a deep understanding of both financial services and technology, as well as the ability to utilize complex adaptive systems theory to changing landscapes and regulatory environments (Muthukannan et al., 2020).

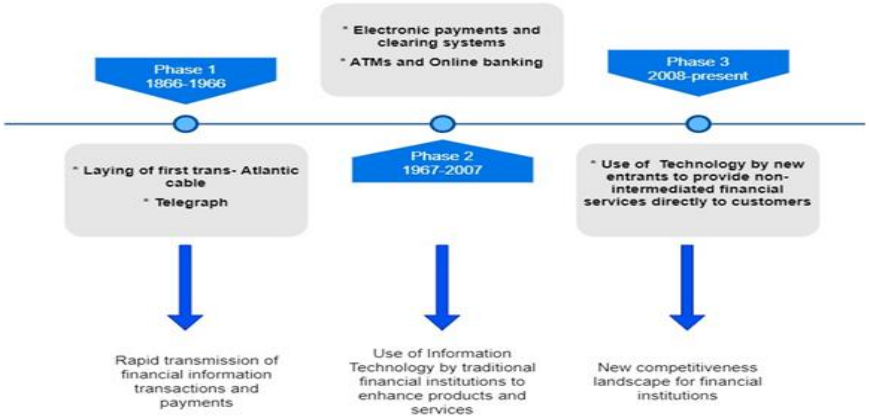

Fig. 2: Phases of financial technology (Blakstad and Allen, 2018)

4. Research Methodology

4.1. Proposed Model and Research Hypotheses

Jordan has made forex trading and online trading of digital currencies illegal, with the Central Bank of Jordan considering encrypted digital currencies as a threat to the national economy. Consequently, digital currency trading companies in Jordan operate globally without local licenses, attracting Jordanian traders who seek to invest in digital currency trading via the Internet, which is deemed risky by the government and the Central Bank. Based on the foregoing in this study, Figure 3 represents a model that proposed the Potential Risks of Mining and Investment in Digital Currencies based on Financial Technology Applications as the following:

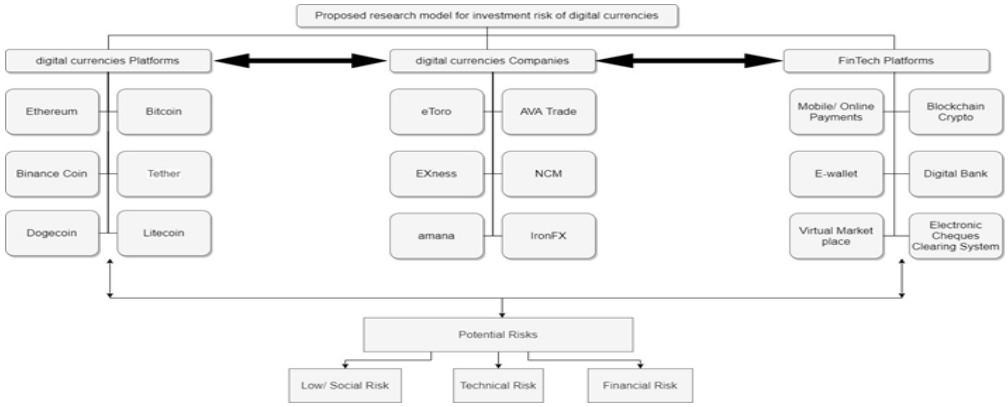

Fig. 3: Proposed model shows the potential risks of mining and investment in digital currencies based on Fintech applications.

Several key areas can be explored related to financial technology applications employed for mining and investment in digital currencies to shed light on the potential risks involved through the following:

- *Cryptocurrency Exchanges*: These platforms facilitate the buying, selling, and trading of digital currencies. They provide individuals and businesses with access to a wide range of cryptocurrencies and trading pairs (Xia, P et al., 2020). However, there are risks associated with exchanges, such as hacking and security breaches leading to the loss of funds. Additionally, some exchanges may lack proper regulatory oversight, increasing the potential for fraudulent activities.
- *Crypto Wallets*: Digital wallets allow users to store and manage their cryptocurrencies securely. There are different types of wallets, including software-based wallets, hardware wallets, and online wallets. However, if proper security measures are not followed, wallets

can be vulnerable to hacking, phishing attacks, or loss of access. This could result in the loss of funds for individuals or businesses [Code V9].

- *Initial Coin Offerings* (ICOs): ICOs enable companies to raise funds by issuing new digital tokens or coins. While ICOs offer an alternative method of fundraising, they are highly speculative and can carry substantial risks. Many ICOs lack regulatory oversight, making them prone to scams, fraud, and failed projects. Investors may face challenges in assessing the viability and legitimacy of ICO projects [Code V2].
- *Smart Contracts*: Smart contracts are self-executing contracts with predefined rules encoded on a blockchain. They automate and facilitate transactions, eliminating the need for intermediaries (Zheng, Z et al., 2020). However, smart contracts are not immune to coding errors or vulnerabilities. If there are flaws in the contract's code, it could lead to financial losses or exploitation by malicious actors [Code V5].
- *Decentralized Finance* (DeFi): DeFi platforms offer financial services like lending, borrowing, and trading, all powered by blockchain technology. While DeFi has the potential to democratize financial services, it also introduces risks. Smart contract vulnerabilities, hacking incidents, and liquidity risks within DeFi protocols can result in substantial financial losses for users and investors [Code V8].

Based on Figure 3 and the previous explanation, the researcher built two main hypotheses as follows:

a) Hypothesis 1: The increased tendency to mine in digital currencies based on Fintech applications has negative impacts on (individuals, businesses, and ecosystems).
b) Hypothesis 2: The increased tendency to invest in digital currencies based on Fintech applications has negative impacts on (individuals, businesses, and ecosystems).

4.2. Sample and data collection

This study employed an inductive-deductive approach, employing a combination of quantitative and qualitative methods. To address the research problem, the researcher utilized Microsoft Excel and NVIVO software. Additionally, the study relied on illustrative graphs depicting digital currency markets, computing power charts, and an energy consumption index used in digital currency mining. To enhance the insights obtained from interviews, a total of 587 participants were successfully administered online questionnaires. The distribution of participants across sectors and demographic characteristics are depicted in Figures 4 and 5 as follows:

The responses of participants from different sectors in Jordan to the questionnaire questions are depicted in Figure No. 4. Among the participants, the highest percentage of answers to the questions in the electronic questionnaire, which focused on their perceptions of the potential risks associated with mining and investing in digital currencies through financial technology applications, came from the education sector (colleges and universities) at 36% of the total responses. Following closely behind, participants from the financial and banking sectors provided answers with a percentage of 35%. In contrast, the responses from respondents in the telecom and commercial sectors showed a relatively weak representation, as indicated by the percentages shown in Figure 4.

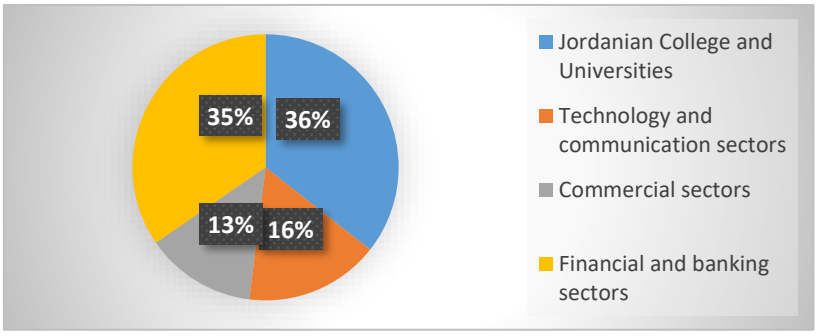

Fig. 4: Distributing the participants for the online survey to the different sectors.

Figure 5 displays the demographic characteristics of participants who responded to the questionnaire addressing the research problem, categorized by the sectors mentioned in Figure 4.

Among the respondents, there were 316 males and 271 females, indicating a higher number of male participants. The age range of the questionnaire respondents varied from 25 years to over sixty. Notably, the age group with the highest response rate was 25-30, followed closely by the 31-40 age group. The number of responses in these age groups correlated with the participants' respective areas of expertise and occupational fields, with 163 and 137 responses recorded, respectively.

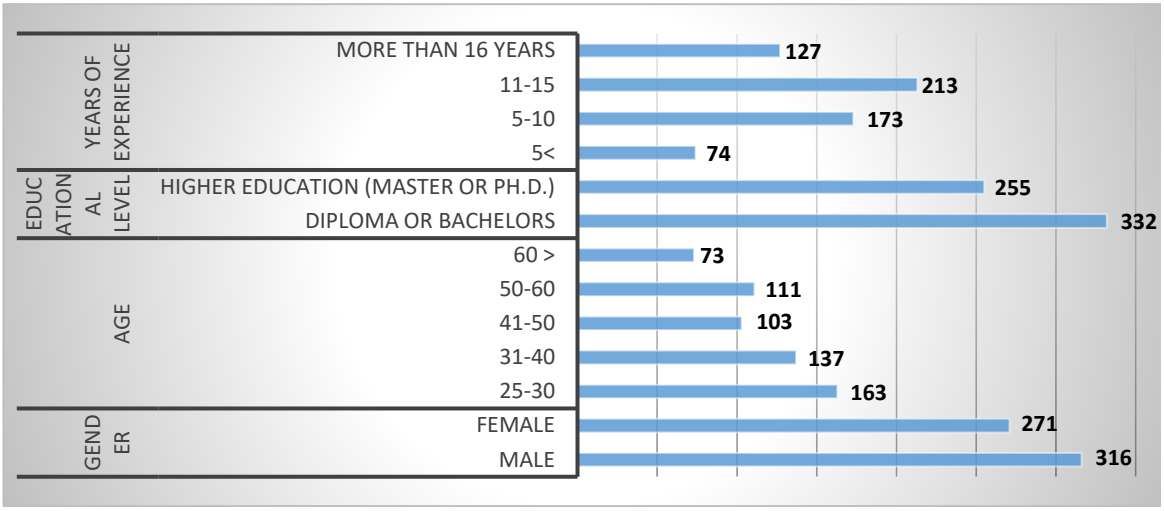

Fig. 5: The demographic characteristics

Conversely, the contributions from individuals above 60 years of age were the least. The academic degrees obtained by participants also influenced the number of responses received, with a significant portion coming from those holding bachelor's degrees and diplomas, as they constituted the largest segment across the various sectors mentioned in Figure 4. Furthermore, the number of years of professional experience impacted the response rate. Specifically, 213 responses were received from individuals with 11-15 years of experience, while 173 responses came from those with 5-10 years of experience.

Furthermore, a total of 55 semi-structured interviews were carried out with academic professionals who specialize in various disciplines such as economics, business, law, and technology within Jordanian universities. The interviewees included experts in various fields such as financial markets, economics, law, information, and communication technology. Detailed information about the interviewees can be found in Table 1:

Table 1: Interviewee profile

#	Code	Position	No. of experience
1	**V1**	Associate Professor of Econometrics	15
2	**V2**	Associate Professor of Finance	17
3	**V3**	Assistant Professor in Commercial Law	11
4	**V4**	Associate Professor of Business Technology and the Internet	13
5	**V5**	Associate Professor of Information Technology	14
6	**V6**	Assistant Professor in Communications Engineering	10
7	**V7**	Financial market analyst	9
8	**V8**	Expert in the digital economy	6
9	**V9**	Expert in electronic commerce	10
10	**V10**	Network and information security expert	11
11	**V11**	Branch bank manager	13
12	**V12**	Economic Analyst	14
13	**V13**	Digital marketing expert	18
14	**V14**	Cyber-crime expert	10

5. Results and Discussions

The data analysis procedure utilized in this examination followed the three stages proposed by Miles and Huberman (2018): data condensation, data display, and drawing/verifying conclusions. To present the findings, Microsoft Excel and Nvivo software were employed, revealing important factors, nodes, frequencies, and statistics. The study discovered numerous risks associated with the adoption and increased investment in the digital currency market, capitalizing on the advancements in financial technology platforms. These findings were categorized into three main areas: financial risks, technical risks, and social/ law risks. The subsequent discussion will delve into the outcomes by answering the research questions as follows:

The potential risks associated with mining digital currencies based on FinTech applications.

Figure 6 illustrates the responses of the contributors to the questionnaire dimensions associated with the first research question. A total of 587 valid questionnaires were collected for statistical analysis.

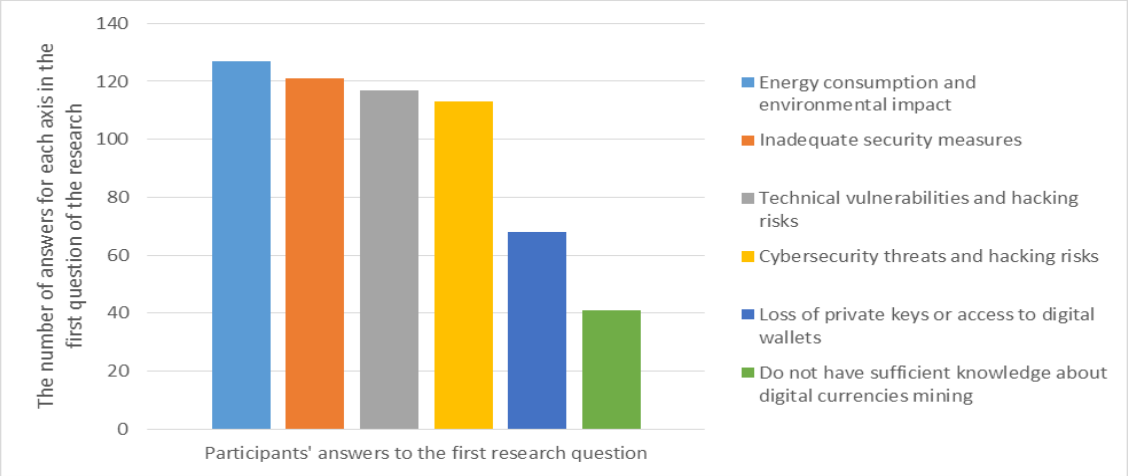

Fig. 6: The potential risks associated with mining digital currencies based on FinTech applications.

According to Figure 6, 127 respondents express their support for the notion that mining digital currencies using financial technology applications carries potential risks related to "energy consumption and environmental impacts." This finding aligns with the insights obtained from interviews conducted with faculty members and experts, stated in Table 1, who provided the following observations:

Energy Consumption: Mining digital currencies, such as Bitcoin, involves solving complex mathematical problems using powerful computers. This process requires a significant amount of computational power, which in turn consumes a substantial amount of electricity. As the mining difficulty increases and more miners participate, the energy consumption associated with mining also increases. This high energy consumption has raised concerns about the environmental sustainability of mining operations." [Code V9]. .*Environmental Impact*: The energy consumed in mining digital currencies often comes from non-renewable sources, such as fossil fuels. The reliance on these energy sources contributes to greenhouse gas emissions and exacerbates climate change. Additionally, the mining process generates a substantial amount of heat, requiring cooling systems that further consume electricity. Furthermore, the hardware used in mining, such as specialized mining rigs or graphics processing units (GPUs), requires the extraction of raw materials, which can have environmental consequences, including habitat destruction and pollution." [Code V6].

furthermore, an Associate Professor of Business Technology and the Internet mentioned that " According to Cambridge Centre for Alternative Finance report, (CCAF), shown in figure 7, succeeded in developing an interactive dashboard called Bitcoin Electricity Consumption Index (CBECI), where this dashboard displayed the data about the alternative finance industry collected by the center,

including the mining map, in addition to other visualizations. Based on this information, the CCAF can figure out the energy sources miners were utilizing by country, and sometimes, by territory. In any case, their dataset does exclude all mining pools, nor is it up to date, leaving us still to a great extent in obscurity about Bitcoin's real energy blend. Besides, some high-profile investigations sum up energy blend at the nation level, prompting a wrong picture of nations like China, which has a very assorted energy scene." [Code V4].

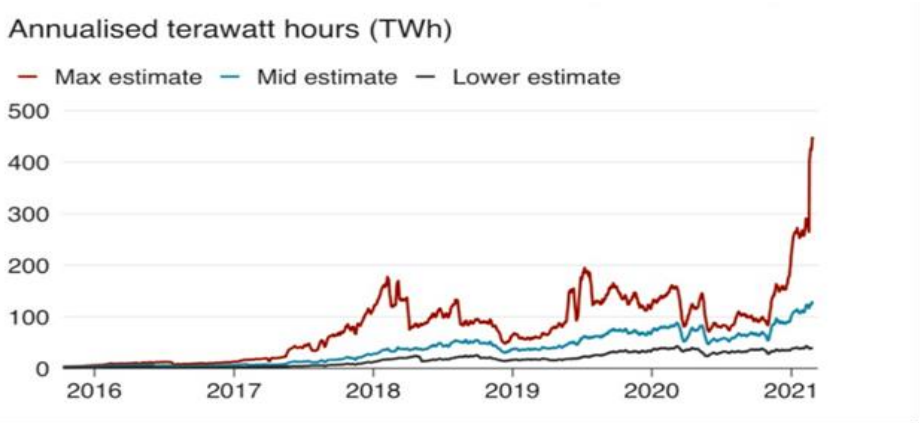

Fig. 7: Bitcoin Electricity Consumption Index (CBECI), Cambridge Centre for Alternative Finance (CCAF).

Thus, gauges for which level of Bitcoin mining utilizes renewable energy fluctuate generally. In December 2019, one report recommended that 73% of Bitcoin's energy consumption was carbon impartial, to a great extent because of the abundance of hydropower in significant mining center points like Southwest China and Scandinavia. Then again, the CCAF assessed in September 2020 that the figure is nearer to 39%. Moreover, the massive power consumption of the Bitcoin network could cause a significant carbon footprint because the regions where most of the mining facilities are located use coal power and thus face serious environmental consequences in the long term (Juričić et al., 2020), [Code V5, 6].

Additionally to Figure 6, the second-ranked responses further reinforce the notion that "Inadequate security measures" stand as a potential risk associated with digital currency mining. This observation is supported by the input of 121 participants in the research questionnaires. As network and information security experts mentioned that "This refers to a lack of sufficient safeguards or protective measures to secure the mining process and the digital assets involved. Inadequate security measures can make the mining operation vulnerable to various risks, such as hacking, theft, fraud, or unauthorized access." [Code V10].

Furthermore, upon revisiting the statistical analysis depicted in Figure 6, it becomes evident that 117 responses corroborated the notion that "Technical vulnerabilities and hacking risks" are indeed among the consequences of digital currency mining. Numerous participants elaborated on the detrimental impacts of these vulnerabilities and risks, affecting both individuals and businesses, as detailed in the remarks below:

1- Implications for Individuals: Individual miners who use FinTech applications to mine digital currencies may face significant risks. If their mining operations are compromised or their wallets are hacked, they could lose the cryptocurrencies they have mined or even other personal information. This can result in financial losses and potential damage to their reputation. Individuals may also face legal implications if their mining activities involve illegal activities or violate regulations.

2- Implications for Businesses: Mining digital currencies can also be conducted by businesses or organizations using FinTech applications. These entities may be targeted by hackers aiming to gain control over their mining operations or steal the cryptocurrencies they have accumulated.

Such attacks can disrupt the business's operations, lead to financial losses, compromise customer data, and harm their reputation. Additionally, businesses involved in mining may need to comply with specific regulations and legal requirements, and any security breaches or vulnerabilities can have severe consequences.

In fact, Digital currency mining involves complex computational processes that require specialized hardware and software. These systems can have vulnerabilities that hackers can exploit to gain unauthorized access or disrupt the mining operation. For example, there may be weaknesses in the mining software or flaws in the underlying blockchain technology that can be targeted by malicious actors. Moreover, the number of miners has increased dramatically, especially recently (from December of the year 2020 until now), and consequently, the total power of computers has increased. The graph in Figure 8 shows the calculation of hashes growth per second. Although there are downside trends, one of which is very sharp at the end of April of this year, the overall strength of the network is increasing, and it is clear that a network like (Bitcoin) represents a huge source of energy [Code V5].

Fig. 8: Estimated Number of Terahashes per second in the Bitcoin Network (linear scale), source: Blockchain.com

Bitcoin mining is to gather and affirm the exchange information that has not been affirmed by the organization since the last block, and afterward bundle it into an exchange block that cannot be altered, to finish an organization's perceived exchange record and save it for quite a while. The mining interaction is to track down the x that makes the accompanying equation valid:

$$SHA256(SHA256(version + prev\_hash + merkle\_root + ntime + x)) < TARGET$$

The range of (x) above is 0 to , and TARGET can be calculated based on the current difficulty. As per the plan of the bitcoin framework, there are just 21 million bitcoins in the framework. An exchange block can be delivered each 10 min and the reward for bitcoin will be halved each four years until the mining reward is finished (Ren et al., 2020).

Also Figure 6 shows, 113 participants identified Cybersecurity threats and hacking risks as one of the risks associated with mining digital currencies through financial technological applications. Their explanations in the remarks area in the questionnaire can be summarized as follows: Digital currencies, such as Bitcoin or Ethereum, are stored and transferred electronically. This means that they are susceptible to various cybersecurity threats, including malware, phishing attacks, and data breaches. Cybercriminals may attempt to exploit vulnerabilities in the FinTech applications used for mining digital currencies, gaining unauthorized access to personal or financial information, stealing funds, or disrupting the mining process. In addition, the interviews conducted with experts in the field of cybercrime corroborate this finding, as one of them reported: “Mining digital currencies involve solving complex mathematical problems to validate and record transactions on the blockchain. Hackers may try to compromise the mining process by targeting the mining software, hardware, or networks. They can

attempt to hijack mining operations, manipulate transaction records, or steal the digital currency being mined. Such attacks can lead to financial losses, operational disruptions, or reputational damage for individuals and businesses involved in mining. Additionally, mining digital currencies through FinTech applications exposes individuals and businesses to cybersecurity threats and hacking risks, which can result in financial losses, data breaches, and operational disruptions. It is crucial for miners to implement robust security measures, keep their systems and applications updated, and stay vigilant against potential threats to mitigate these risks [Code V14].

In addition, 68 respondents highlighted the potential risks associated with mining digital currencies through FinTech applications on individuals and companies, specifically mentioning the loss of private keys or access to digital wallets, as stated by a participant in the remarks section the following: “Private keys are cryptographic codes that are used to access and control digital wallets, which hold digital currency assets. Private keys serve as a form of digital signature, allowing individuals or businesses to prove ownership and authorize transactions. whereas, Digital wallets are software applications or online platforms that store and manage digital currencies. They provide a secure environment for users to store their digital assets and facilitate transactions. However, if individuals or businesses lose access to their digital wallets, either due to technical issues, forgotten passwords, or compromised accounts, they may be unable to access their digital currency holdings. This loss of access can result in the inability to use or transfer the digital assets stored in the wallet”. The aforementioned outcome was further substantiated through an interview carried out with a digital economy specialist, who expressed the following viewpoint:” These risks are particularly relevant when mining digital currencies through FinTech applications. Mining involves the process of verifying and adding transactions to a blockchain, the underlying technology behind most digital currencies. Miners are rewarded with newly created digital currency units for their computational efforts. However, to receive these rewards, miners need to have a digital wallet and corresponding private keys. If the private keys or access to the digital wallet are lost, the rewards earned through mining may become inaccessible” [Code V9].

The potential risks associated with investing in digital currencies based on FinTech applications.

Figure 9 illustrates the responses of the contributors to the questionnaire dimensions associated with the second research question. A total of 587 valid questionnaires were collected for statistical analysis.

According to Figure No. 9, 103 respondents confirmed that the lack of investor protection and safeguards is a significant potential risk when investing in digital currencies. This finding aligns with the response from one of the participants who mentioned in the notes section of the research questionnaire the following: "Investor protection refers to the measures and regulations put in place to safeguard the interests of investors and ensure fair and transparent investment practices. These protections may include legal frameworks, oversight by regulatory authorities, and mechanisms for dispute resolution". Additionally, a faculty member specializing in commercial law supported this finding and expressed the following viewpoint: “In the event of fraudulent activities or disputes, investors may face challenges in seeking legal recourse. The decentralized and borderless nature of many digital currencies can make it difficult to trace and recover lost funds or hold accountable those responsible for wrongdoing” [Code V3].

101 respondents shed light on the area of Market volatility and price fluctuations as critical risks facing investors in the digital currency market. This was one of the focus of the second question in the research questionnaire. Here is a summary of some of the responses they provided: "Price fluctuations refer to the unpredictable changes in the value of digital currencies. These fluctuations can be substantial and can occur due to various factors, such as market sentiment, economic events, technological advancements, regulatory announcements, or even social media trends. Additionally, Digital currencies, such as Bitcoin and Ethereum, are known for their high levels of volatility. Unlike traditional currencies, which are often influenced by stable economic factors and central bank policies, digital currencies are driven by a range of factors including market demand, speculation, regulatory changes, and investor sentiment. This can lead to rapid and significant price movements, creating a volatile market

environment. As a result, the value of digital currencies can fluctuate greatly within short periods, leading to potential gains or losses for investors".

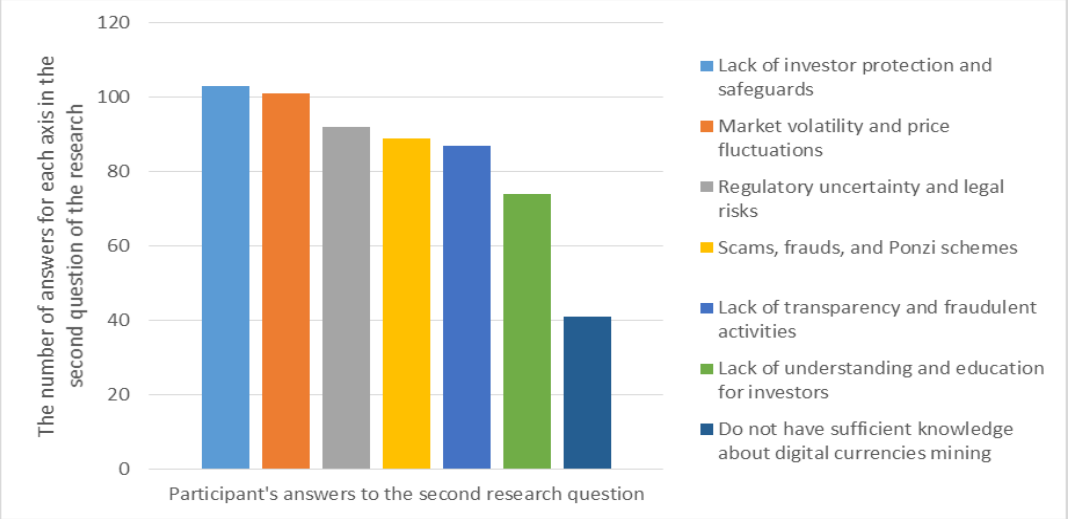

Fig. 9: The potential risks associated with investing in digital currencies based on FinTech applications

Associate Professor of Econometrics confirmed this result through the following statement: "Both market volatility and price fluctuations pose risks to investors in digital currencies through FinTech applications. These risks can affect the profitability and stability of investment portfolios. It's important for investors to carefully assess their risk tolerance, conduct thorough research, and consider the potential impacts of market volatility and price fluctuations before engaging in digital currency investments through FinTech platforms" [Code V1].

The research questionnaire gathered input from 92 participants, who engaged in a focused discussion on regulatory uncertainty and legal risks. The key points derived from this discussion can be summarized as follows: Digital currencies, such as cryptocurrencies, often operate in a relatively new and evolving regulatory landscape. Governments and financial authorities worldwide are still in the process of formulating and implementing regulations specifically tailored to digital currencies. This regulatory uncertainty creates a risk for investors as it can lead to sudden changes in rules and regulations, which may affect the value and viability of digital currencies. Additionally, regulatory actions or restrictions imposed by authorities can impact the functionality and accessibility of FinTech applications, potentially limiting investment opportunities or making them more challenging to navigate. Furthermore, Investing in digital currencies through FinTech applications involves engaging with complex legal frameworks. There may be legal ambiguities or discrepancies in different jurisdictions regarding the status, taxation, and ownership rights of digital currencies. The lack of uniformity in legal treatment across countries poses a risk for investors, as the legal landscape may change, leading to unexpected consequences or challenges related to ownership, trading, and taxation of digital assets. Moreover, the emergence of fraudulent schemes, scams, and illicit activities in the digital currency space can expose investors to legal risks, such as potential legal disputes or loss of funds.

The summary of 89 participant responses to the research questionnaire revolved around the topic of cheating and fraud, with many answers addressing this aspect. In summary, the participants highlighted the prevalence and concerns related to cheating and fraudulent activities through the following points"Scams: In the digital currency space, there are fraudulent schemes that aim to deceive investors. These scams can take various forms, such as fake initial coin offerings (ICOs), where individuals or entities raise funds for a new cryptocurrency that doesn't actually exist or doesn't have the promised functionality. Scammers may also create fake exchanges or wallets to trick people into sending their digital currencies to them, resulting in financial loss, and Frauds: Digital currencies can

be subject to fraudulent activities. This can involve manipulating market prices, using false information to attract investors, or misrepresenting the value or potential returns of a particular cryptocurrency. Fraudulent schemes can be operated by individuals, groups, or even organizations, making it crucial for investors to exercise caution and conduct thorough research. The following findings were supported by an interview conducted with an economic analyst in the financial sector and a manager of a banking branch, who reported the following: "These risks are associated with investing in digital currencies through FinTech applications because such applications have made it easier for individuals to participate in the digital currency market. While FinTech platforms have brought several benefits and opportunities for investors, they have also provided a fertile ground for scammers and fraudsters to exploit unsuspecting individuals who may lack sufficient knowledge or experience in the digital currency space. Also, they shed light on the Ponzi schemes: Ponzi schemes are described as a specific type of fraud in which early investors are paid returns with the money invested by later investors, rather than from legitimate profits. The scheme relies on a constant influx of new investors to sustain the promised returns. Eventually, when new investors dry up or withdrawals exceed new investments, the scheme collapses, causing significant financial losses to those involved (Bartoletti et al., 2020), [Code V11,12].

During the research questionnaire, 87 participants addressed the lack of transparency and fraudulent activities as key topics for discussion when answering the second question. A summary of their responses is as follows: Digital currencies, such as cryptocurrencies, operate on decentralized systems that are not governed by traditional financial institutions or regulations. While this decentralization brings advantages like enhanced privacy and security, it also creates a lack of transparency. Transactions conducted using digital currencies may not be as transparent as traditional financial transactions, making it difficult to trace and verify the flow of funds. This lack of transparency can be concerning for investors who rely on clear and reliable information to make informed investment decisions. Moreover, expert in the digital economy explicit that " The emergence of digital currencies has provided opportunities for fraudsters to exploit unsuspecting investors. Due to the relative anonymity associated with digital currencies, it becomes easier for scammers to create fraudulent schemes, such as Ponzi schemes, initial coin offering (ICO) scams, or fake cryptocurrency exchanges. These fraudulent activities can lead to significant financial losses for investors who fall victim to these scams. Additionally, the lack of regulatory oversight and investor protection mechanisms in the digital currency space can make it challenging to recover funds lost to fraud"[Code, V8].

The lack of understanding and education among investors was identified as one of the potential risks associated with investing in digital currencies, according to the input of 74 respondents who participated in the questionnaire. Their collective discussions led to the following conclusions: Digital currencies, such as cryptocurrencies, can be complex and have unique features compared to traditional financial instruments. Many investors may not fully grasp the intricacies of how digital currencies work, their underlying technology (like blockchain), or the associated risks. This lack of understanding can lead to uninformed investment decisions and potential losses. Additionally, This finding was corroborated by a financial market analyst during an interview, who expressed the following observations: "Education plays a crucial role in empowering investors to make informed decisions. In the case of digital currencies, investors need to be familiar with concepts like wallet security, private keys, transaction fees, and the overall volatility of the crypto market. Without proper education, investors may be susceptible to scams, fraudulent schemes, or poor investment choices" [Code V7].

6. Conclusive Remarks

This study aimed to shed light on the Potential Risks of Mining and Investment in Digital Currencies based on Financial Technology Applications through ask two main questions: What are the potential risks associated with mining in digital currencies based on Fintech applications on (individuals, businesses, and ecosystems)?, and What are the potential risks associated with an investment in digital

currencies based on Fintech applications on (individuals, businesses, and ecosystems)? This study employed an inductive-deductive approach, employing a combination of quantitative and qualitative methods. To address the research problem, the researcher distributed online surveys and made interviews with professors and experts, and analyzed results utilizing Microsoft Excel and NVIVO software.587 participants were successfully administered online questionnaires. these participants were distributed across four sectors (educational, technology and communication, commercial, and banking). Where the main results of the first question of the research were the following: Energy consumption and environmental impact, Inadequate security measures, Technical vulnerabilities and hacking risks, Cybersecurity threats and hacking risks, and Loss of private keys or access to digital wallets. In summary, the risks associated with mining digital currencies through FinTech applications can have implications ranging from environmental concerns and energy consumption to security vulnerabilities and financial loss. Individuals and businesses must prioritize security, sustainability, and proactive measures to address these risks effectively. Additionally, the main results of the second question of the research were the following: lack of investor protection, market volatility, regulatory challenges, fraudulent activities, lack of transparency, and inadequate investor understanding. Addressing these implications requires a collaborative effort between individuals, regulatory bodies, and the broader financial ecosystem to establish robust investor safeguards, regulatory frameworks, and educational initiatives.

In my perspective, there are several limitations to this study, which can be summarized as follows: *Firstly*, the study is constrained by a scarcity of data sources due to the relatively recent emergence of investment and mining in digital currencies. Insufficient information is available even among educational, financial, and commercial institutions. *Secondly*, this study cannot be generalized on a large scale, as the study was limited to a specific geographical area, which is Jordan, and in specific sectors, in addition to a specific type of digital currencies such as (Bitcoin and Ethereum), and that the risks and market dynamics can change over time. Therefore, the conclusions drawn from the study may have limited generalizability to different contexts or future scenarios. *Thirdly*, the research methodology predominantly relies on qualitative analysis and self-reported data gathered through questionnaires and interviews, which may introduce subjectivity and potential response biases. Furthermore, the chosen analysis method may not adequately capture the intricate complexities of the digital currency ecosystem. *Fourthly*, Scope and Focus: The study may focus in particular on some of the risks associated with mining and investing in digital currencies, which may lead to the omission or underestimation of other related risks. Different digital currencies, blockchain technologies, or mining practices may have unique risks that are not extensively explored in the study. Therefore, the results may not fully capture the full range of risks in the digital currency ecosystem. *Fifthly*, the lack of a longitudinal analysis: the study focused on potential risks for a quick overview of risks at a specific point in time. However, understanding the long-term trends and dynamics of these risks requires a longitudinal analysis that tracks changes over time. The results of the study may not fully reflect the evolution and interaction of risks in the digital currency ecosystem. *Lastly*, Bias and Subjectivity: Researchers' biases, assumptions, or prior knowledge of digital currencies and financial technology applications may inadvertently influence study design, data interpretation, or conclusions.

References

Abdillah, L. (2019, December). An Overview of Indonesian Fintech Application. In The First International Conference on Communication, Information Technology and Youth Study (I-CITYS2019), Bayview Hotel Melaka, Melaka (Malacca), Malaysia.

Auer, R. A., Cornelli, G., & Frost, J. (2020). Rise of the central bank digital currencies: drivers, approaches and technologies (No. 8655). CESifo Working Paper.

Bartoletti, M., Carta, S., Cimoli, T., & Saia, R. (2020). Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. Future Generation Computer Systems, 102, 259-277.

Blakstad, S., & Allen, R. (2018). FinTech revolution. Cham, Switzerland: Springer, 121, 132.

Blockchain.com. (2021, June 11). Mining Information (2021), "Total Hash Rate (TH/s)", available at https://www.blockchain.com/charts/hash-rate

Chang, H. C. (2010). A new perspective on Twitter hashtag use: Diffusion of innovation theory. Proceedings of the American Society for Information Science and Technology, 47(1), 1-4.

Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. IEEE Access, 7, 167930-167943.

Dow, S. (2019). Monetary reform, central banks, and digital currencies. International Journal of Political Economy, 48(2), 153-173.

Dube, C., & Gumbo, V. (2017). Diffusion of innovation and the technology adoption curve: Where are we? The Zimbabwean experience. Business and Management Studies, 3(3), 34-52.

Duffie, D. (2019, May). Digital currencies and fast payment systems: Disruption is coming. In Asian Monetary Forum, May, mimeo.

Garcia Bringas, P., Pastor-López, I., & Psaila, G. (2020). BlockChain Platforms in Financial Services: Current Perspective. Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy, 11(3), 110-126.

Juričić, V., Radošević, M., & Fuzul, E. (2020). Optimizing the Resource Consumption of Blockchain Technology in Business Systems. Business Systems Research: International journal of the Society for Advancing Innovation and Research in Economy, 11(3), 78-92.

Klein, M., Gross, J., & Sandner, P. (2020). The Digital Euro and the Role of DLT for Central Bank Digital Currencies. FSBC Working Paper, Frankfurt School Blockchain Centre.

Knight, E., & Wojcik, D. (2020). FinTech, economy and space: Introduction to the special issue. Environment and Planning A: Economy and Space, 52(8), 1490-1497.

Miles, M. B., Huberman, A. M., & Saldana, J. (2018). Qualitative data analysis: A methods sourcebook.

Muthukannan, P., Tan, B., Gozman, D., & Johnson, L. (2020). The emergence of a fintech ecosystem: A case study of the Vizag Fintech Valley in India. Information & Management, 57(8), 103385. https://doi.org/10.1016/j.im.2020.103385

Odeh, M., & Yousef, M. (2021). The effect of Covid-19 on the electronic payment system: usage level trust and competence perspectives. Indonesian Journal of Electrical Engineering and Computer Science, 22(2), 1144-1155.

Opare, E. A., & Kim, K. (2020). A compendium of practices for central bank digital currencies for Multinational financial infrastructures. IEEE Access, 8, 110810-110847.

Ren, Y., Zhu, F., Sharma, P. K., Wang, T., Wang, J., Alfarraj, O., & Tolba, A. (2020). Data query mechanism based on hash computing power of blockchain in internet of things. Sensors, 20(1), 207.

Rogers, E. M. (2004). A prospective and retrospective look at the diffusion model. Journal of health communication, 9(S1), 13-19.

Seo, A., Son, Y., Lee, Y., & Jeong, J. (2022). A Blockchain Enabled Personal Donation System Development Scheme.

Thakor, A. V. (2020). Fintech and banking: What do we know?. Journal of Financial Intermediation, 41, 100833.

The Cambridge Centre for Alternative Finance. (2021, June 1). Cambridge Bitcoin Electricity Consumption Index (CBECI), https://www.jbs.cam.ac.uk/insight/2019/cambridge-bitcoin-electricity-consumption-index-cbeci

Tung, S. S., Dorasamy, M., & Ab Razak, R. (2022). Cognitive Interview for Knowledge Creation in IT Projects to Accelerate Digital Innovation. Journal of System and Management Sciences, 12(4), 115-129.

Ward, O., & Rochemont, S. (2019). Understanding Central Bank Digital Currencies (CBDC). Institute and Faculty of Actuaries.

Xia, P., Wang, H., Zhang, B., Ji, R., Gao, B., Wu, L., ... & Xu, G. (2020). Characterizing cryptocurrency exchange scams. Computers & Security, 98, 101993.

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475-491.