Illuminating the dark corners: a qualitative examination of cryptocurrency’s risk

Kriti Mehta and Sonia Chawla

Abstract

Purpose – The study provides a comprehensive understanding of the issues and illegal activities related to cryptocurrencies and their negative repercussions. This study aims to identify and classify cryptocurrency downsides using grounded theory and in-depth interviews. The study also analysed investors’ reluctance to invest in cryptocurrency. This pioneering qualitative study illuminates a deep and multifaceted criminal aspect of cryptocurrency.

Design/methodology/approach – The study conducted in-depth interviews with respondents who have experience and knowledge of cryptocurrency investments. The interviews were recorded and transcribed. The analysis was performed using the NVivo 14 software in the study.

Findings – The study specified two major types of cryptocurrency’s negative aspects: barriers and illegal usage. Barriers to cryptocurrency investment include technological, security, trust, market-related and regulatory reasons. Terrorist funding, money laundering, fraud and ransom payments are all examples of illegal usage. The results of the word cloud analysis are consistent with the overall findings of the survey, which highlighted illegal usage as a prominent negative element of cryptocurrencies. It is a key reason why cryptocurrency is not included in investing portfolios by investors.

Originality/value – The study’s findings provide useful insights for policymakers to develop better methods for successfully mitigating risks and ensuring responsible and sustainable usage of cryptocurrencies. In addition, the study could serve as a stepping stone for more cryptocurrency-related studies, contributing to the development of a more complete and nuanced comprehension of this emergent technology and its societal effects.

Keywords Cryptocurrency, Barrier, Illicit use, NVivo 14, Qualitative study

Paper type Research paper

Introduction

The advent of the digital era has led to a significant transformation in various aspects of life, including the economy, particularly in the realm of digital transactions (Cha et al., 2023; Kala and Chaubey, 2023; Kantar and Bynum, 2021; Mubarak et al., 2020). Among the most notable changes in digital transactions is the emergence of virtual currency, also known as electronic or digital currency. Although virtual currencies have been around for many years, the emergence of cryptocurrencies in 2009 has propelled them into the limelight (Jalan et al., 2023; Ariska et al., 2022). Cryptocurrency is a sort of virtual money that uses blockchain or distributed ledger technology as a consensus method for recording transactions (Ozili, 2022), which drastically increases the currency’s value (Jurczyk, 2020).

Bitcoin, the first cryptocurrency, was created by an individual or group of individuals using the pseudonym Satoshi Nakamoto (Hassan et al., 2023). Its creator remains unidentified. Since its inception, cryptocurrency has had a significant impact on the financial sector. Cryptocurrency is a non-governmental currency that facilitates encrypted and anonymous transactions (Dabbous et al., 2022). Peer-to-peer cryptocurrencies eliminate the need for banks (Schaupp et al., 2022; Peters et al., 2015). The traditional fiat money backed by the central banks is frequently being challenged by cryptocurrency. Decentralisation, global
reach and anonymity or pseudo-anonymity are unique to cryptocurrencies (Mohsin et al., 2023; Narayanan and Clark, 2017; Mackenzie, 2022). It gives an innovative idea and an opportunity to build a digital economy platform.

Cryptocurrencies, although captivating and attractive, have often been connected to criminal activity and have been implicated in unlawful behaviours (Zhao et al., 2023a, 2023b; Butler, 2019). Their underlying value and classification are ambiguous as a result of the lack of government assistance and regulations (Iwamura et al., 2014; Vaz et al., 2020). Cryptocurrencies have been associated with money laundering, dark market payments and terrorism financing (Naheem, 2023; Houben and Snyers, 2018). Recently, future exchange, a Bahamas-based cryptocurrency exchange its founder, Bankman-Fried, has been accused of wrongdoing as leading to the company’s sudden failure and the loss of billions, wiping out $26bn of wealth (The Hindu, 2023). The Financial Action Task Force (FATF) warns that crypto assets could serve as a refuge for illicit and terrorist financial operations. This concern is exemplified by a recent Hamas attack in Israel, where cryptocurrency was used for the funding of terrorist financial activities (Reuters, 2023). As per Chainalysis survey findings, in the first half of 2023, criminal platforms, including darknet markets, malware, scams, fraud shops and ransomware operations, received a total of $2.8bn in cryptocurrency. The frequency of ransomware payments is on a notable rise, expected to reach the second-highest annual amount ever recorded (Howcroft, 2023). Governing bodies are attempting to limit such activities and establish guidelines for the sustainable and legal growth of cryptocurrency (Mackenzie, 2022). Despite its growing prominence, the issue is still shrouded in considerable ambiguity, and no clear solutions have been proposed.

Until now, a limited amount of qualitative research has been carried out on cryptocurrency, and even when such studies have been conducted, little or no attention has been given to their negative aspect. Previous research conducted by scholars such as Wronka (2022), Leuprecht et al. (2022) and Mackenzie (2022) has only investigated singular aspects, mainly the phenomenon of money laundering via cryptocurrency. Fonseca et al. (2020) examined only psychological barriers to cryptocurrency adoption, while Gurgun et al. (2022) explored the barriers to using cryptocurrency in managing the construction supply process using the empirical approach. Alqahtani and Sheldon (2022) conducted a systematic review of crypto-ransomware attack detection methodologies. Amsyar et al. (2020) focused on a comprehensive assessment of the challenges that cryptocurrencies pose, while Eigelsloven and Parry (2021) study concentrated on a thorough review of the manipulation of cryptocurrency markets. Similarly, Navamani (2021) research provides an analysis of the security aspect of cryptocurrency. Additionally, Desmond et al. (2019) conducted a systematic literature review that evaluates cryptocurrency laundering as a complex socio-technical system, most of them rely on analytical reviews. According to Fang et al. (2022), the fluctuating volatility of cryptocurrencies has a significant impact on investors’ decisions to include them in their portfolios. Furthermore, Charfeddine et al. (2020) proposed that because cryptocurrency is a relatively new idea, some investors may not completely understand its operation, possible hazards and benefits, making them unwilling to invest in it. However, all of these studies encapsulate a single dimension of the dark side of cryptocurrency. Hence to fill this gap the present study offers a complete and holistic overview of the domain through qualitative research.

This study aims to contribute to the current corpus of knowledge. Firstly, this research endeavours to fill a substantial gap in the literature by comprehensively examining the adverse attributes and intrinsic challenges of cryptocurrency. It uses grounded theory methodology and in-depth interviews to obtain innovative insights into this complex topic. Secondly, this study uses robust qualitative research methodologies to classify and examine data, with a particular focus on finding barriers and their illegal use as a detrimental aspect of cryptocurrency. Thirdly, a comprehensive understanding of interconnected hazards provides useful insight for policymakers seeking to formulate more efficient approaches to
manage risks and promote the responsible and sustainable utilisation of cryptocurrencies. Last, the study lays the groundwork for future research, to help better understand cryptocurrency and its social ramifications better.

The research questions of this study are:

RQ1. What are the dark sides of cryptocurrency?

RQ2. How can the dark sides of cryptocurrency be categorised into different dimensions?

RQ3. What are the primary reasons for investors to not incorporate cryptocurrency into investment portfolios?

Review of literature

Theoretical framework

Quantitative research is difficult to conduct due to the lack of scale and limited prior research (Tewksbury, 2015). In many disciplines, qualitative research has proved to be an effective method. Existing theories are lacking and insufficient, therefore, qualitative research is crucial when delving into complicated and largely unexplored topics like the darker realities of cryptocurrency. By tracking individual opinions, judgements and experiences, this technique offers a greater comprehension of the issue (Fischer and Guzel, 2023). Zhao et al. (2023a, 2023b) investigated the implications of COVID-19 on global financial markets, focusing on both developed and developing nations using the qualitative approach. Similarly, Bhatia et al. (2021) conducted a qualitative study to investigate robo-advisory services and analyse Indian individual investors’ awareness and perception of this FinTech innovation. The research undertaken by Kaur and Kumar (2021) used qualitative methods to investigate the utilisation of social media within the beauty and wellness sector in India. Sampat et al. (2023) recently used qualitative methods to investigate the dark sides of FinTech in financial services, with an emphasis on the perspectives of FinTech developers. Moreover, Kaczynski et al. (2014) used qualitative methodologies to examine financial practices and acknowledged this methodology as a crucial supplement to current practices. The examples shown here demonstrate the usefulness and versatility of qualitative research in a variety of settings. Taking all of these factors into account, it becomes clear that qualitative research is the best approach to investigate the negative aspects of cryptocurrency.

Qualitative research can be divided into five types, grounded theory, phenomenology, ethnography, narrative analysis and case studies (Kaya et al., 2020). Grounded theory has grown in popularity among these methodologies because of its practical focus on participant concerns and organised data processing. The sociologists Glasser and Strauss created a grounded theory in 1967, which enables researchers to identify issues and come up with answers by creating theories from data rather than testing pre-existing hypotheses (Al-Nuaimi et al., 2020; Charmaz, 2008a, 2008b). This strategy comprises categorising and analysing survey data, discovering correlations between categories and altering fundamental categories to generate hypotheses (Morgan, 2020; Rieger, 2019). Furthermore, it provides a structured and rigorous analytical technique that enables themes to emerge from the data.

This theory seems more appropriate for the present research since it permits researchers to build theories based on facts rather than starting with predetermined ideas or beliefs (Al-Nuaimi et al., 2020). Unlike quantitative research, qualitative work, such as in-depth interviews and grounded theory, does not aim at making broad generalisations for a larger population. Instead, it seeks to create categories from the data, analyse relationships between these categories, and understand the lived experiences of the research participants (Charmaz, 1990; Dworkin, 2012). This is particularly helpful when investigating a complicated and little-known topic, such as the dark aspect of cryptocurrency, where established theories are insufficient or inapplicable (Fischer and Guzel, 2023). Data collection, coding and analysis are iterated processes that enable researchers to gradually
improve their comprehension of the phenomena. This iterative technique is ideal for delving into the varied and dynamic nature of cryptocurrency’s negative aspects. Taking these factors into account, the grounded theory technique is best suited for the study. This study will use the analytical steps of grounded theory, as well as draw insights from the basic idea of Charmaz (2012) and Charmaz and Thornberg (2021), to investigate the factors or barriers that hinder investors from investing in cryptocurrency. It will also help to uncover the social, economic and political factors that contribute to the shortcomings of cryptocurrency, such as fraud and illicit activities.

**Research methodology**

**Research paradigm and approach**

The research paradigm and philosophy influence how knowledge is perceived and interpreted, with ontology, epistemology and axiology exploring the extremes of objectivism and subjectivism (Mark et al., 2012). The selection of a research approach depends upon the context of research with qualitative research being appropriate for in-depth understanding (Sim et al., 2018; Creswell and Creswell, 2017). Research outcomes fall into theory building and testing, and this research uses grounded theory (Khan et al., 2022). An inductive approach to theory building that subscribes to interpretivism, relativism ontology and subjectivism epistemology for knowledge discovery (Goulart, 2019). The goal of this exploratory research is to provide new insights for prospective investors, the corporate world and the government.

**Sample size and technique**

Qualitative research can begin with a sample size of 1, which can still provide valuable insights (Kaur and Kumar, 2021; Boddy, 2016). This implies that the study recognises the wealth of information that a single person may provide. Qualitative research does not require huge sample numbers, and even a single participant’s insights might deepen knowledge in a given study environment (Moser and Korstjens, 2018). Qualitative research methods are flexible enough to draw insights from individual experiences and views (Mason et al., 2010).

When justifying the sample size, researchers should consider factors such as data saturation and population homogeneity (Trotter, 2012). Homogeneous populations can be adequately represented with a small sample size (Sandelowski, 1995), and data saturation can be achieved with as few as 12 in-depth interviews (Guest et al., 2006). In the present study, the term “homogeneous population” pertains to a group of persons who possess shared attributes or experiences about their knowledge and experience in cryptocurrency investments (Robinson, 2014). The rationale behind the consideration of a homogenous population is in the objective of ensuring that the participants have comparable levels of competence and comprehension within the particular topic of interest (Hennink and Kaiser, 2022). Further, it seeks to enhance the depth and quality of the qualitative data acquired by specifically selecting respondents who possess a common background in cryptocurrency (Boddy, 2016; Dworkin, 2012; Mason et al., 2010). For this research, 12 in-depth interviews were conducted with respondents who have knowledge and investment experience in cryptocurrency. The interview questions are provided in Appendix 1. This sample size aligns with previous studies in the field of marketing and finance and is adequate to yield meaningful findings (Genc and Oksuz, 2015; Hallock et al., 2019; Lagrosen and Grundén, 2014). Participants were invited to participate in the research through LinkedIn with a written request, and all participants provided voluntary assent for the interviews.

**Data collection**

This study uses in-depth interviews, and a qualitative method (Khan et al., 2022; Whiting and Williams, 2013; Chapman et al., 2015), to investigate the negative aspects of cryptocurrency
and its impact on investors’ decision-making. Some interviews were conducted online while others were face-to-face, with each interview lasting approximately 20–25 min. The participants were carefully selected based on their high level of education, knowledge of cryptocurrency and having two to five years of investing experience in cryptocurrency. To protect anonymity, all participants were assured that their identities would be kept secret. The interviews were taped and transcribed to collect information on the participants’ age, gender and level of education. The questions were reframed and rephrased as required. The details of the participants were presented in tabular form in the study (see Table 1).

Data analysis

The final transcript was examined using NVivo 14. NVivo 14 is widely used as a software tool for the analysis of qualitative data (Bonello and Meehan, 2019). The NVivo 14 software was used to streamline the coding process and provide an audit trail, resulting in trustworthy and predictable outcomes (Richards and Hemphill, 2018; Wang et al., 2022). Moreover, the interview results were automatically compiled and coded using the NVivo 14 software and text analysis method based on word similarity. NVivo 14 includes a feature that automatically detects emotions in text, reducing the subjectivity of human interpretation. Text can be categorised into codes such as technical barriers, security barriers, trust issues, market-related barriers and regulatory barriers. Additionally, illicit activities are further classified into codes such as terrorism financing, money laundering, fraudulent activities and ransom payments. The use of these distinct codes allows a nuanced understanding of different aspects covered in the interviews. The auto-coding tool in NVivo does not classify an entire statement as positive or negative but rather assesses words individually. This approach adds a layer of granularity to the analysis, capturing the subtleties of language and expression in the data. Each interview is first coded into these categories and then visually displayed through sentiment auto-coding (Dhakal, 2022; Pudaruth et al., 2018), as shown in Figures 1 and 2. These visualisations likely provide a concise overview of the distribution of sentiments and themes across the interviews, aiding in the interpretation of the qualitative data.

Findings

The dark aspects of cryptocurrency can be categorised into different dimensions, as revealed by the analysis. These dimensions include technical and security challenges, trust issues, lack of government support and the promotion of illicit activities such as money laundering, funding of terrorism, ransom payments and fraudulent transactions. These factors collectively shed light on the challenges faced by cryptocurrency (Q1). Figure 3 provides a

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Information of the participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Age</td>
</tr>
<tr>
<td>R1</td>
<td>37</td>
</tr>
<tr>
<td>R2</td>
<td>33</td>
</tr>
<tr>
<td>R3</td>
<td>26</td>
</tr>
<tr>
<td>R4</td>
<td>27</td>
</tr>
<tr>
<td>R5</td>
<td>26</td>
</tr>
<tr>
<td>R6</td>
<td>28</td>
</tr>
<tr>
<td>R7</td>
<td>27</td>
</tr>
<tr>
<td>R8</td>
<td>60</td>
</tr>
<tr>
<td>R9</td>
<td>32</td>
</tr>
<tr>
<td>R10</td>
<td>35</td>
</tr>
<tr>
<td>R11</td>
<td>28</td>
</tr>
<tr>
<td>R12</td>
<td>30</td>
</tr>
</tbody>
</table>

Source: Authors’ own creation
visualisation of these challenges. The analysis is based on empirical evidence gathered from interview quotes, which reveal the presence of several significant themes that are well-supported by data. Given below are the explanations of these issues along with some supported transcripts.

**Dark side of cryptocurrency**

The findings obtained from the analysis conducted using NVivo 14 demonstrate that the dark sides of cryptocurrency can be classified into two distinct categories, namely, its act as a barrier and its involvement in illicit activities. This addresses the research (Q2).

**Cryptocurrency and its barrier**

*Technical barrier.* According to Chowdhury et al. (2019), a key obstacle to the adoption of cryptocurrency is a lack of technical knowledge among experts. Additionally, Bu Qammaz and Almaian (2020) emphasised that investors may lack sufficient technical expertise, which may result in inadequate risk management practices. The findings in this study support the assertion, demonstrating that the biggest obstacle in the technical barriers
category is a lack of technical expertise regarding cryptocurrencies. Some statements were provided by respondents to express this perspective, which include:

A lack of technical understanding about cryptocurrencies may hamper their intentions and general adoption. (R2)

Another respondent expressed:

A lack of technical knowledge about cryptocurrencies can have several potential consequences it can lead to financial losses due to a lack of understanding of how to safely store and manage their cryptocurrency assets. It can also make them vulnerable to scams and fraudulent activities in the cryptocurrency market. (R7)

The technical complexity of cryptocurrencies and their underlying blockchain technology can pose a challenge for traditional financial institutions that are not familiar with these technologies. This can make it difficult to integrate cryptocurrencies into existing financial infrastructure and systems. (R5)

Market-related issues. The prevalence of speculative activities within the cryptocurrency market results in a significant level of volatility and uncertainty, ultimately diminishing the efficacy of crypto assets (Antonakakis et al., 2019). This phenomenon is a key factor that can lead investors to exhibit hesitancy towards using cryptocurrencies in their portfolio-building
activities. Furthermore, it is worth noting that frequent fluctuations in cryptocurrency valuations are not an uncommon occurrence (Fang et al., 2022). The significant variations in the token value would make cryptocurrency adoption more challenging, the major obstacle in transactions and restricted usage of cryptocurrencies (Liu et al., 2018; Liu and Tsyvinski, 2021). Some statements were provided by respondents to express this perspective, including:

1. Cryptocurrencies are highly volatile, with significant price fluctuations occurring over short periods. This can make it difficult to accurately assess the value of a cryptocurrency and determine the appropriate exchange rate when converting it to a traditional currency. (R7)

2. The high volatility and lack of stability in cryptocurrency prices can make it difficult for traditional financial institutions to assess and manage the risks associated with integrating cryptocurrencies into their services. (R9)
Trust-related issues. Despite the perceived strength of cryptocurrency security, concerns about trust persist among users due to the fully digital nature of these currencies without any physical presence (Vyas and Lunagaria, 2014). The security and privacy of cryptocurrency, for instance, were evaluated by Bushager et al. (2018), who identified self-induced events, malicious events, hardware failure and software failure as the most common causes of cryptocurrency key loss. The security, speed and lack of intermediaries offered by cryptocurrencies can ease international transactions, but their broad adoption is constrained by the scope of fraud and crime (Sanz-Bas et al., 2021). According to Cypher Trace’s research, Bitcoin fraud and theft cost $1.9bn in the first 10 months of 2020. This included financial losses caused by Ponzi schemes, exit scams and deceptive initial coin offerings (ICOs). As some respondents commented:

If a cryptocurrency wallet password is weak, an attacker can steal the funds stored in the wallet. This can result in significant financial losses for the wallet owner. (R1)

Cryptocurrency can have a negative impact on the level of trust. Cryptocurrencies are decentralised and operate outside of traditional financial systems, making them more susceptible to fraud and scams. (R2)

Regulatory issues. Cryptocurrency raises certain regulatory concerns (Ojih et al., 2023). It is more difficult to rely on it since it is decentralised and operates independently on a private blockchain-based cryptography system (Erevelles et al., 2022). Several governments have implemented legislation prohibiting the usage of cryptocurrency (Jane et al., 2014). Strict national and international regulations are necessary for the decentralised technology of cryptocurrency, which can improve market confidence and diversify a company’s portfolio (Ramassa and Leoni, 2022). During the interviews, the issue of barriers to using cryptocurrency was raised, and it was emphasised that one of the most significant obstacles is a regulatory barrier:

One respondent says “The lack of regulatory clarity and oversight in the cryptocurrency market can make it difficult for an investor to embrace cryptocurrencies fully”. (R2)

Others remark that “Regulatory frameworks for cryptocurrencies and their conversion to traditional currencies can be unclear or non-existent in some jurisdictions, which can create legal and compliance challenges for cryptocurrency users and service providers”. (R6)

Cryptocurrency is generally considered to be a riskier currency compared to traditional currencies, such as the US dollar or the euro. This is primarily because cryptocurrencies are not backed by any government or central authority, and their value is determined by market demand and supply. (R10)

Security issues. According to Quamara and Singh (2022), even though Bitcoin is one of the latest cryptocurrencies, it is still accompanied by a wide range of security concerns, and finding solutions to them has become an important topic of research. In this context, Vyas and Lunagaria (2014) provided research on Bitcoin security difficulties and concerns, with a focus on characteristics connected to the mining and transaction processes. According to a Coinbase poll, 56% of respondents have personal experience or knowledge of someone being a victim of a cryptocurrency scam, with a median loss of $2,000 among those impacted (Biswa, 2023). These responses to inquiries regarding security concerns associated with cryptocurrency are documented below:

Phishing attacks can be used to trick cryptocurrency users into revealing their wallet passwords or private keys. This can give an attacker access to the wallet and the funds stored within it. (R8)

Once a cryptocurrency transaction has been processed, it cannot be reversed. This means that if an attacker gains access to a wallet and initiates unauthorised transactions, the funds cannot be easily recovered. (R3)
Cryptocurrency's role in illicit activities

**Ransomware attacks.** Ransomware refers to malicious software that encrypts a victim’s computer system or data, rendering it inaccessible until a ransom is paid. Due to its anonymity and difficulty in being tracked, cryptocurrencies like Bitcoin have become more and more in demand by ransomware attackers in recent years (Alqahtani and Sheldon, 2022). Receiving payments in Bitcoins is quite simple for the attackers since they simply need to supply a Bitcoin wallet address (Zimba et al., 2019). A recent example of a ransomware attack on All India Institute of Medical Sciences computer systems demanded Rs 200 crore in cryptocurrency to restore data. The hacked data contains many high-profile individuals’ personal information, including past prime ministers, ministers, administrators and justices (Times of India.com, 2022). During the question about illicit activities involving cryptocurrency, some respondents provided answers related to ransomware attacks. These answers are listed below:

- Cryptocurrencies have been used in ransomware attacks, where hackers demand payment in cryptocurrency in exchange for returning control of a victim’s computer or data. (R12)

- One way in which cryptocurrency is used in illegal activities is through ransom payments. Ransomware attacks happen when attackers take control of someone’s computer or data and then ask for money in return for giving back the control. These attacks have become more frequent in recent times. (R10)

**Money laundering.** Money laundering is a well-known and long-standing practice that involves moving money across borders and using different financial instruments to hide its origin (Wronka, 2022). Each year, between $500bn and $1tn is estimated to be laundered globally. Money laundering is a prevalent problem in many countries, with the Basel anti-money laundering (AML) Index identifying around 64% of countries as having a high risk of money laundering. Since its inception in 2009, cryptocurrency has emerged as a possible instrument for those seeking to launder money, since it offers an alternative means of transporting illicit money across international boundaries (Wronka, 2022; Albrecht et al., 2019). A sum of $540m was effectively laundered by criminals involved in cryptocurrency operations through the utilisation of a platform referred to as Ren Bridge (Sigalos, 2022). Some of the interviewees’ comments on the topic of money laundering are as follows:

- Due to its pseudonymous nature, cryptocurrency has become a popular instrument for money laundering. (R5)

- The anonymity and decentralised nature of many cryptocurrencies make it difficult to trace transactions and identify the parties involved, making them attractive to criminals engaged in money laundering, tax evasion, or illicit trade. (R1)

- The absence of governmental control in the case of cryptocurrencies might enhance the likelihood of fraud, money laundering, and other illegal acts. (R4)

**Terrorist financing.** Because of their significant volatility, cryptocurrencies are not yet extensively used for terrorist financing. Cryptocurrencies have limited acceptability, making them less appealing for terrorist funding (Dyntu and Dykyj, 2021). However, terrorist groups still find cryptocurrencies useful for facilitating quick international transactions and raising money all over the world (Wang and Zhu, 2021). For example, cryptocurrency is suggested as a secure and anonymous means of payment by organisations such as the Islamic State of Iraq and Syria (Higgins (2014)) and Al-Sadaqah (Keatinge (2018)). A recent Hamas attack in Israel involved the financing of terrorist activities with cryptocurrency, which prompted the FATF to issue a warning regarding the potential use of crypto assets for illicit and terrorist financial operations (Reuters, 2023). Respondents shared their perspectives through statements such as:
Terrorist organisations have been known to use cryptocurrencies to receive donations and transfer funds across borders without detection. (R5)

Cryptocurrencies have also been identified as a potential means of funding terrorism due to their anonymity and lack of regulation. (R8)

**Fraudulent activities.** Dark market users are increasingly using cryptocurrencies. This is due to their secrecy or partial anonymity, inability to undo transactions, quick transaction processing, and lack of regulatory oversight. Cryptocurrencies have become a commonly used form of payment on dark market platforms, with their importance often being likened to that of PayPal in the development of eBay (Foley et al., 2019). Many studies such as Leuprecht et al. (2022), and Foley et al. (2019) have shown that using cryptocurrencies to finance illegal activities, particularly the purchase of illicit products is a popular way of using them. Some real-world examples of cryptocurrency fraud and scams such as from October 2020 to March 2021, the USA Federal Trade Commission reported that customers lost more than $80m in cryptocurrency-related frauds, with a median loss of $1,900 per individual. Furthermore, according to research done by the University of Technology Sydney, around 10% of all ICOs issued in 2017 were fraudulent. By the beginning of 2018, over 80% of ICOs had been discovered as frauds or had previously failed (Biswas, 2023). Here are some responses related to cryptocurrency that can be used for fraudulent activities:

- Cryptocurrencies are decentralised and operate outside of traditional financial systems, making them more susceptible to fraud and scams. (R3)
- The lack of regulatory oversight in some jurisdictions could create opportunities for fraud or scams targeting unsuspecting investors. (R2)
- Cryptocurrency has gained notoriety for being a popular tool used in fraudulent activities due to its anonymity, irreversibility of transactions, and process efficiency. (R8)

**Word cloud.** The research (Q3) uses a word cloud analysis to probe the primary reasons for investors not including cryptocurrency in investment portfolios. Word clouds visually depict word frequency, making complex data more transparent and straightforward (Lohmann et al., 2015; Atenstaedt and Singh, 2012; Kashive et al., 2020). According to the researchers, despite the complexity of data analysis, a word cloud remains a simple and transparent tool (Jayashankar and Sridaran, 2017; Simsar, 2021). According to DePaolo and Wilkinson (2014), the most frequently mentioned words during analysis are depicted in the word cloud. Analysis of the most frequently used words in respondents’ answers using word cloud. The result is shown in Figure 4, where the most frequently used words include “cryptocurrency”, “illegal”, “scams” and “dark sides”. These words indicate that the interviewees are mainly concerned about the illegal nature of cryptocurrency and its negative aspects. The most prominent word among these is “illegal”, suggesting that it is a significant reason for not incorporating cryptocurrency into investment portfolios. Sample responses from interviewees include:

**Discussion and conclusion**

Emerging as a novel financial instrument, cryptocurrencies present a myriad of prospects and obstacles. While they offer an innovative and simple means to conduct digital currency transactions, they are also linked to incidents of fraud, theft, tax evasion and terrorist funding. The rising interest in cryptocurrencies has prompted governments throughout the world to call for a united strategy to address the accompanying concerns. Because of their intricacy, cryptocurrencies need to be examined in more detail to fully grasp their potential and risks. It is of the utmost importance to possess this knowledge
to formulate policies that can efficiently address corruption and advance sustainable development (Rabbani et al., 2021).

This emerging field of study opted for a qualitative approach due to the lack of a standardised scale. The current study conducted a qualitative inquiry into this burgeoning area. The survey featured 12 respondents with knowledge and experience in cryptocurrency investing, who took part in in-depth interviews. NVivo 14 is used for the analysis. The findings provide answers to the research questions and disclose that the negative aspects of cryptocurrencies fall into two categories: their use as a barrier and their involvement in illegal activities. These categories are subdivided further into subthemes. Regarding its illicit use, the financing of terrorism is identified as the greatest concern. Cryptocurrency-related trust issues are the most significant barrier. The word cloud analysis reveals that “illegal” was a frequently used term among the interviewees. The illegitimate connotation of cryptocurrencies may discourage investors from including them in their investment portfolios. Investors exhibit reluctance to incorporate cryptocurrency into their portfolios due to a myriad of concerns identified through the analysis. Technical barriers, such as a lack of expertise and understanding, hinder adoption, with respondents citing the intricate nature of cryptocurrency and its blockchain technology. Market-related issues, including high volatility and frequent fluctuations, make accurately assessing cryptocurrency values challenging. Trust-related problems arise from the fully digital and decentralised nature of cryptocurrencies, leading to concerns about weak wallet security and susceptibility to fraud. Regulatory challenges, such as unclear frameworks, hinder full embracement. Security concerns, like phishing attacks and irreversible transactions, contribute to apprehensions. Additionally, the association of cryptocurrency with illicit activities, including ransomware attacks, money laundering, terrorist financing and fraudulent transactions, further deters investors. A word cloud analysis emphasises respondents’ predominant worry about the illegal nature and negative aspects of cryptocurrency, encapsulating the key reasons for hesitancy in its portfolio inclusion.

The study’s results will benefit the general public by raising awareness about the possible hazards associated with cryptocurrencies, such as their use in unlawful activities such as
money laundering and terrorism funding. This can assist people in making better choices when it comes to using or investing in cryptocurrency. The research can give politicians and regulators insights into how to manage the difficulties posed by cryptocurrencies, such as the need for more stringent regulations. Likewise, in the USA, the Securities and Exchange Commission has issued guidance on the treatment of cryptocurrencies and has acted against companies that violate securities laws. In Europe, the European Union has established regulations for cryptocurrency exchanges and wallet providers under the fifth anti-money laundering directive (Beebeejaun and Dulloo, 2023). By establishing a cooperative environment in which the cryptocurrency sector, governments and law enforcement organisations can collaborate to build and implement impenetrable AML/know your customer protocols and cutting-edge technologies to identify and detect any suspicious activity in cryptocurrency transactions. Educating users and the general public about the possible threats of terrorist funding using cryptocurrencies, can increase the security of the sector and make them more cautious and knowledgeable when dealing with digital assets. We can enable the cryptocurrency sector to stay ahead of unlawful actions by working together to create a safer and more trustworthy environment. The study also serves as a foundation for future cryptocurrency research and analysis, assisting in the development of a thorough and nuanced knowledge of this emergent technology and its influence on society.

Future research agenda

Our research yields qualitative insights into the detrimental aspects of cryptocurrency in an emerging economy. We acknowledge that the sluggish adoption of technology, coupled with institutional and infrastructural challenges, along with the economic landscape of the country, establishes a distinctive context for exploring these negative dimensions. Despite the careful execution of the study, we recognise the presence of limitations which offer opportunities for future research. Primarily, the qualitative nature of our methodology poses constraints on the generalisability of findings. Consequently, to cover the gap, the study advocates for future studies to contemplate the adoption of a quantitative approach and the formulation of a scale to systematically gauge the dark side of cryptocurrency, enhancing the rigour and comparability of analyses. Secondly, this qualitative study faces an issue of social desirability bias, as cryptocurrency investors may exhibit socially desired behaviours to counter any methodological biases. Hence, future research should include experiments and longitudinal studies to address this gap. Thirdly, this study focuses on the negative features of cryptocurrencies, pushing future research to investigate both favourable and undesirable aspects and comprehend different user opinions. Fourthly, a significant focus is on variables affecting investors’ decisions in a turbulent market, prompting more research into the long-term consequences of cryptocurrency investments and the influence of market manipulation. Although the study focuses on cryptocurrency barriers and illegal usage, future research should focus on crypto-ransomware detection and a broader analysis of security challenges. Fifthly, research on cryptocurrency mining’s impact on the environment is needed to offer eco-friendly alternatives and evaluate different cryptocurrencies. Finally, for a comprehensive knowledge of cryptocurrencies, a multidisciplinary study integrating economics, finance, psychology, law and technology is advised.

Theoretical contributions

Despite the development of a substantial body of research focusing on specific aspects of cryptocurrency’s dark side (Wronka, 2022; Leuprecht et al., 2022; Mackenzie, 2022), there is a limited understanding of how new technologies, such as blockchain-based cryptocurrency, are used for illicit purposes and how the broader spectrum of its dark sides is illuminated. Concerns have also been expressed concerning the under-theorisation of this study stream, with a concentration on manifestations of the dark side rather than the
broad term linked with cryptocurrency’s negative sides (Gurgun et al., 2022; Fonseca et al., 2020). Our research serves as a first step towards filling these gaps. Firstly, similar to other technological innovations with identified challenges (Baccarella et al., 2018; Faccia et al., 2020; Talwar et al., 2019; Sampat et al., 2023), this study significantly advances our theoretical understanding of the dark side of cryptocurrency by emphasising the country’s unique context. Working in a developing country like India, the existence of a cash-based economy and little technological penetration exacerbates the issues connected with the dark side. Secondly, our study illuminates the possible adverse consequences that may arise from the adoption of novel technologies, including blockchain-based cryptocurrency. Thirdly, using the grounded theory methodology in a qualitative exploration contributes novel conceptual frameworks that elucidate cryptocurrency crime, security and regulation. Grounded theory aids in contextualising the drawbacks associated with cryptocurrency by establishing categories and themes related to fraud, money laundering, scams and other adverse factors. This approach offers a more comprehensive understanding compared to conventional categories.

**Practical implications**

The practical implications of the study are as follows. Firstly, the study implies that cryptocurrencies open the door to new types of financial crimes and illegal activity, such as money laundering, ransomware attacks, terrorist financing and tax evasion. Secondly, the study brings attention to regulatory shortcomings in addressing the particular problems presented by cryptocurrency. This can result in suggestions for policy modifications or the creation of new regulatory frameworks. Finally, it reveals ethical dilemmas associated with the use of cryptocurrencies, such as issues about anonymity, trust, volatility and uncertainty, as well as technical issues associated with cryptocurrencies. The research can lead to improved cybersecurity and law enforcement strategies for countering cybercrime involving cryptocurrency. These novel insights have the potential to inform policy development and guide practical strategies in addressing the challenges posed by cryptocurrency.

**Managerial implications**

Managers and organisations need to be acutely aware of the managerial implications stemming from studies on the dark sides of cryptocurrency. First and foremost, a strong commitment to regulatory compliance is paramount to mitigate the legal risks in an ever-evolving regulatory environment. Robust risk management strategies and cybersecurity measures are crucial to protect assets and sensitive data from fraud, theft and market volatility. Secondly, educating customers about the inherent risks of cryptocurrencies and ensuring due diligence in partnerships and investments is essential. Implementing comprehensive compliance programs, crisis management plans and ethical practices within the organisation is vital. Thirdly, continuous market analysis, transparent reporting, and a long-term strategic approach are also necessary to navigate the complex cryptocurrency landscape effectively. Collaboration with industry peers and law enforcement agencies, along with an association with a legal counsel specialising in cryptocurrency regulations, can provide valuable support in this endeavour. Finally, the findings of this research offer valuable contributions to the broader discourse on cryptocurrency. By illuminating the dark sides of this digital asset class, policymakers and practitioners can gain a comprehensive understanding of the potential risks and pitfalls associated with its use. This, in turn, may lead to the development of more informed and effective policies and practices for navigating the cryptocurrency landscape.

**Limitations of the study**

While this study offers valuable insights into the dark sides of cryptocurrency, it is essential to acknowledge that there are certain limitations to this research. The exploratory nature of
the study, which was based on a sample size of 12 respondents, restricts the generalisability of the results. Future research should consider using quantitative or hybrid approaches in different geographic locations to verify the research questions posed in this study.

A holistic understanding of cryptocurrency requires exploration beyond its dark sides. Future research could delve into potential strategies to address the identified issues and focus on examining the long-term viability and sustainability of cryptocurrencies, considering their possible environmental effect, technical scalability, and legislative advancements which enhance the adoption of cryptocurrency, thereby contributing to a more comprehensive understanding of this emerging digital asset.

Furthermore, given that the present study solely concentrates on the negative aspects of cryptocurrency, it would be worthwhile to explore the factors driving the continuous rise in the popularity of cryptocurrency worldwide. These areas warrant further investigation in the near future. Finally, exploring the potential benefits and drawbacks of cryptocurrency in comparison to the stock market could pique the curiosity of future researchers, leading to a better understanding of the two investment options.

References


Appendix. Questionnaire

1. What are the potential consequences of a lack of technical knowledge about cryptocurrencies for individuals and society as a whole? (Priyadarshani, 2018)

2. What are the major challenges faced in integrating cryptocurrencies with other financial services such as banking, trading and investment platforms? (Nawari and Ravindran, 2019)

3. According to you, what are the difficulties associated with converting cryptocurrencies to traditional currencies? (Bentov et al., 2019)

4. What are the potential security gaps associated with cryptocurrency that can arise due to vulnerable wallet passwords and malicious software? (Zeiringer and Thalmann, 2020)

5. How does the ease of committing fraud with cryptocurrency affect the level of trust in this form of digital asset? (Perera et al., 2020)

6. What are the major challenges caused by the low maturity of current cryptocurrency technologies? (Novak, 2019)

7. Is cryptocurrency considered a riskier currency compared to traditional currencies? (Koblitz and Menezes, 2016)

8. What are the doubts surrounding the long-term viability of cryptocurrency systems, and how might these doubts impact the future of cryptocurrencies as a form of currency and investment? (Conrad et al., 2018)

9. What are the reasons for the low adoption rate of cryptocurrencies by Small and Medium Enterprises (SMEs)? (Zhou et al., 2016)

10. Will cryptocurrencies be used permanently in the long run, or is there a possibility that they will not be used in the future? (Herbert and Litchfield, 2015)

11. How does the incompatibility of cryptocurrency systems with the current legal system affect the regulation and adoption of cryptocurrencies? (Perera et al., 2020)

12. In what ways could cryptocurrencies potentially be used in illegal activities? (Perera et al., 2020)

13. How do criminals use cryptocurrencies to launder money and evade law enforcement?

Source: Authors’ own creation

About the authors

Kriti Mehta is a Research Scholar in the Department of Humanities and Management at Dr B R Ambedkar National Institute of Technology, Jalandhar. She has completed her BCom (Prof) from B. D. Arya Girls College, Jalandhar Cantt, (GNDU, Amritsar). She has completed her MCom from B. D. Arya Girls College, Jalandhar Cantt, (GNDU, Amritsar). She has also qualified UGC NET examination with JRF. She is working in the area of Cryptocurrencies, investment intentions and sentiments.

Dr Sonia Chawla is presently working as an Associate Professor at the Department of Humanities and Management, Dr BR Ambedkar National Institute of Technology, Jalandhar. She received her PhD from Guru Nanak Dev University, Amritsar in 2008. Her primary research interests are in the areas of Service Quality Measurement, Financial Economics, Portfolio Management, Cost Accounting, Blockchain and Cryptocurrency. Specifically, she works on issues related to Financial Intermediation, Portfolio Management and Corporate Governance. She published 02 books and more than 30 Research Papers in different International Journals of repute. She has supervised 06 PhD students and 07 are still pursuing their PhD. Sonia Chawla is the corresponding author and can be contacted at: chawlas@nitj.ac.in

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com