Cryptocurrency Scams: A Multi-Pronged Approach to Mitigating Risks Through Regulation, Enforcement, and Consumer Education

Hasan, Amena and Nahar, Kamrun and Akhter, Suraiya

Atish Dipankar University of Science Technology, Bangladesh, Kustia Government College, Bangladesh, Notre Dame University College, Bangladesh

17 January 2024

Cryptocurrency Scams: A Multi-Pronged Approach to Mitigating Risks Through Regulation, Enforcement, and Consumer Education

Amena Hasan
Department of Business Administration
Atish Dipankar University of Science & Technology, Bangladesh

Kamrun Nahar
Faculty of Business, Kustia Government College, Bangladesh

Suraiya Akhter
Department of Business Studies, Notre Dame University College, Bangladesh

Abstract

This article explores the risks and impacts of cryptocurrency scams on investors, the market, and the global financial system. It emphasizes the need for government regulation, enforcement activities, and consumer education to address these scams. The article also discusses the relationship between the grey economy and the technosocial, highlighting the evolving nature of online and offline life and its implications for criminology. The study uses ethnographic research and participant observation to investigate the cultural context of cryptocurrency frauds. It examines various types of scams, including pump-and-dump schemes, advanced fee frauds, and rug pulls. The article concludes by emphasizing the importance of combating cryptocurrency frauds to protect investors, foster technological innovation, and maintain customer trust.

Keywords: Cryptocurrency; scams; risk; blockchain; regulatory; technosocial

JEL Codes: E21; D72; O33; C51

Introduction

Cryptocurrency scams pose significant risks to investors, particularly those with limited knowledge and experience in discerning legitimate offerings from fraudulent ones. These scams not only lead to financial losses for individuals but also tarnish the reputation of the cryptocurrency market and deter potential investors from supporting legitimate projects. By eroding investor trust and normalizing fraud and manipulation, cryptocurrency scams undermine the integrity of the

market, hindering the adoption of blockchain technology and impeding the growth and development of the cryptocurrency ecosystem (Agarwal, et al., 2023).

For governments and regulatory agencies tasked with protecting consumers and maintaining financial stability, addressing cryptocurrency schemes presents complex regulatory challenges. To combat fraud, regulators may need to enact new legislation, enhance enforcement activities, and improve consumer education and awareness (Chowdhury et al., 2023). It is crucial to address cryptocurrency frauds in order to foster technological innovation and facilitate growth in the blockchain and cryptocurrency space. Scams hinder the entry of honest businesses and initiatives into the market, obstructing the creation of novel solutions and applications that could benefit society (Ducas and Wilner, 2017).

According to Toufaily (2022), the impact of cryptocurrency scams extends beyond the cryptocurrency market itself and can have broader implications for the stability of the global financial system. Large-scale scams or systemic threats can undermine investor confidence and attract regulatory scrutiny. Moreover, scams can contribute to increased volatility in cryptocurrency values. Building and maintaining customer confidence are essential for the widespread acceptance and utilization of cryptocurrencies and blockchain technologies. When consumers lose trust in cryptocurrency due to scams, they are less likely to enter the market and embrace innovative technology. Rebuilding and preserving trust is crucial to encourage widespread adoption and unlock the potential benefits of cryptocurrencies (Chowdhury, 2018).

Effectively combating cryptocurrency frauds involves navigating complex legal and ethical considerations, including jurisdictional issues, enforcement challenges, and the protection of individuals' rights and interests (Campbell-Verduyn, 2018). Developing successful regulatory and enforcement strategies to combat scams while upholding principles of fairness and justice requires striking a delicate balance between these objectives.

This article investigates the interplay between two contemporary trends in criminology: the "grey" or shadow economy, and the "technosocial" (Brown 2006; Powell et al. 2018). The case analysis focuses on Bitcoin fraud as an example of the grey economy in the realm of unregulated financial investment speculation. Within this culture, traders engage in risky bets on volatile and uncertain

assets, celebrating their audacity and embracing the idea of taking "moonshots." Cryptocurrency represents a frontier of technological development, around which a distinct "degen" culture has emerged, characterized by high-stakes crypto bets with potentially significant rewards (Chowdhury et al., 2021).

The article argues that as society continues to embrace metaversal lifestyles that blend online and offline experiences, criminology must adapt its theories and methodologies to effectively recognize and analyze the novel "virtual/networked spaces" (Hayward, 2012) in which grey economies and associated crimes exist.

The discourse surrounding cybercrime spans two extremes: the "new threat" perspective (Yar 2005) and the "old wine in new bottles" perspective (O'Neill, 2000; Grabosky, 2001). The former considers internet crime as a new and distinct challenge that demands fresh approaches, while the latter argues that although criminal activities may shift to online platforms, the fundamental structure of crime remains unchanged. It is evident that neither extreme is sustainable due to the ongoing evolution and integration of technology into our everyday lives, which leads to the hybridization of online and offline existence (Brown, 2006; Chowdhury & Chowdhury, 2022)). This hybridization represents a significant marker of social change and necessitates the adaptation of criminological theory and methodologies to understand and analyze the emergent "virtual/networked spaces" in which grey economies and associated crimes thrive (Orton-Johnson and Prior 2013).

Methodology

The study employed ethnographic research methods to investigate financial crime in the crypto world and its implications for criminology. The primary methodological strategy was participant observation, which involved participating in crypto trading chatrooms to understand the market's language and collect personal anecdotes from traders about scams they have encountered. Additionally, the researcher engaged in bitcoin trading to gain firsthand experience and a better understanding of the financial instruments involved in the scams being investigated.

While the focus of this study is on scams in the crypto world, future research could explore other distinguishing features, such as demographic characteristics of crypto traders. It is worth noting

that the majority of crypto traders are young men, and the chatrooms often exhibit aggressive right-wing, individualist, hetero-normative, soft-pornographic, and racist language and attitudes. However, this study specifically focuses on the scams themselves rather than the perpetrators and targets of these frauds (Hooley et al. 2012).

The study's timeline was driven by data saturation regarding the primary research topics, namely how the primary scam types in the crypto world work and how they fit into or alter criminological theories regarding cyber or digital crimes' hybrid technosocial development.

An important ethical consideration in conducting an ethnography of online economic crime is the issue of anonymity. In crypto chatrooms, everyone uses online aliases, and only a small percentage of individuals have publicly revealed their true identities. Given that all data is collected from publicly accessible online forums where anonymity is fundamental, and the research is in the public interest without any hidden agenda, the secrecy of participant identities can be justified.

Findings

A Discussion on Technosocial Metaverses and the Shadow Economy

In Neal Stephenson's science fiction novel Snow Crash (1992), the term "metaverse" was introduced to describe a 3D virtual environment where individuals exist as avatars (Stephenson 1992; Laue 2011). The concept of metaverses has gained cultural significance with works like Ernest Cline's Ready Player One (2011) and the short story "Metaverses" (Cline, 2011). Companies like Facebook and Microsoft are actively working towards constructing the metaverse, with Facebook even changing its name to Meta in October 2021 to underscore its commitment (Banerjee, 2021).

Mark Zuckerberg's vision of an "embodied internet that you are inside of rather than just gazing at" is both intriguing and indicative of the direction the metaverse is heading (Wong and Duncan, 2021). Microsoft plans to develop an "enterprise metaverse" where corporate conferences and classroom instruction take place in a virtual world of avatars (Banerjee, 2021). The metaverse is often associated with computer-generated environments where people gather to play games, socialize, and work (Palmer, 2021). Although the metaverse is still a blend of aspiration, hype, and

reality, trends in augmented and virtual reality, gaming, socializing, and online infrastructure development are paving the way for its emergence (Palmer et al. 2000).

As the distinction between the real and the simulated blurs, the online/offline divide is starting to disappear and will likely continue to do so (Orton-Johnson and Prior 2013). The internet is evolving towards "Web 3.0," a decentralized realm powered by blockchain technology that promises a new political, social, and economic metaverse (Silver, 2020). Governance tokens, cryptocurrency transactions, and Non-Fungible Tokens (NFTs) have deep connections to the cryptocurrency market and are integral to the property ownership and economic exchanges within metaverses. Given the socio-cultural, political, and economic foundations on which metaverses are currently being formed, it is crucial to understand the criminology of cryptocurrency as a first step towards comprehending the criminology of the metaverse. The financial crimes in the metaverse are the focus of this study.

Scholarly discussions on cybercrime have evolved to encompass the social aspects of our technosocial existence (Stratton et al., 2017). The field of digital criminology has expanded its analyses beyond the novelty and illegality of technology-enabled crimes to understand online crime as inherently social (Powell et al., 2018). This study contributes to this research trajectory by exploring the cultural and sociological context of fraudulent activities within the evolving crypto market ecosystem. Crypto scams combine elements of innovation and tradition in their design and execution, reflecting the convergence of online and offline spaces in a hybrid human-technical world (Brown 2006, 227).

To understand the potential impact of these developments on criminology, it is useful to explore the literature on grey economies. Grey economic activity refers to unregulated or partially regulated marketplaces that often blur the line between legality and illegality (Ohnsorge and Yu, 2021). These activities are often characterized by a sense of ambiguity regarding their legality, as participants may regard them as "a bit lawful, a bit illegal" (Galemba, 2008). Cryptocurrency represents one such grey economy, a thriving online market with an uncertain legal status that challenges traditional notions of market regulation. Like Stanley Cohen's concept of the "public secret," cryptocurrency is widely known, tolerated, but not officially endorsed in most countries, presenting complex policy concerns (Cohen, 2001). Issues range from the viability of a globally

unregulated financial system (Dodd, 2018; Zook and Blankenship, 2018) to the prevalence of crime within the crypto space that often goes unaddressed by traditional law enforcement (Reddy and Minaar, 2018; Kethineni and Cao, 2019; Foley et al., 2019). As institutional actors in the crypto market operate primarily online to evade scrutiny, participants also engage online, often anonymously, with little physical presence (Ohnsorge and Yu, 2021).

Cryptocurrency has become a substantial economic force with a market cap of nearly $3 trillion, comparable to the value of Apple, the world's most valuable firm (Reid, 2021). As one of the largest players in global finance, cryptocurrency has become a technosocial playground for fraud. Despite ongoing discussions about its regulatory status, the crypto market exists with minimal official regulation or law enforcement oversight, making it a significant challenge for established financial systems (Reddy and Minaar, 2018; Kethineni and Cao, 2019; Foley et al., 2019).

Scams in the Present Era

Scams have a long history, as evidenced by books and articles from the late 19th and early 20th century that document the era of the "Big Con" (Maurer, 1940; Brannon, 1948). Unlike simpler scams, the Big Cons required the mark to empty their bank account in order to participate. The con artists would convince their target that they had advanced knowledge of race outcomes or other opportunities to cheat the system, leading the mark to believe they were gambling on a sure thing (Maurer, 1940).

To execute their cons, con artists often hire actors to pose as customers at their fake establishments. The mark would be given minor victories at the phony betting shop before being sent off to collect funds for a larger bet, only to be defeated in the end. The con artists would then cool the mark out and disappear while dismantling the fake establishment (Maurer, 1940).

While sports betting was a common theme in these cons, scams can take many forms, such as fraudulent stock market investments or quick money schemes. The key to their success lies in their diversity, as if all scams looked the same, they would be easier to avoid. However, despite the different variations, there are common characteristics shared by all scams (The Big Con).

One important factor is making the scam appear to be a legitimate business or opportunity. If it seems too good to be true, the scam will fail. Similarly, the con artist must fit in and give a plausible excuse for their involvement to avoid suspicion (Doocy et al., 2001; Levi, 2008: 394). For instance, Bernie Madoff's clients believed they were investing in a standard business and fund manager, not a con artist running a Ponzi scheme (Balleisen, 2017; Manning, 2018).

Another factor is targeting individuals who are willing to bend the rules or are enticed by the promise of illegal profits. Even if the mark doesn't have to be dishonest to benefit, they may be presented with a scheme that appears to be in their favor but is actually against them (Mackenzie 2010).

The lure of an offer that seems too good to be true is also a common element in scams. Temptation can override the mark's better judgment, causing them to dismiss indications that it may be a scam (Leff, 1976; Prus and Sharper, 1977).

The impropriety of the opportunity and the realization that it was too good to be true contribute to the time needed for the mark to cool off. They may feel complicit in illegal activities and be less likely to report them to authorities. Even if the scheme is legal, the mark may be led to believe they share some blame for falling for it (Titus and Gover, 2001; Holt and Graves, 2007).

The concept of a limited-time opportunity is another reason why marks are pressured to act quickly. They may believe that if they don't seize the chance, someone else will. This urgency can make them overlook their reservations and dive into the scam without conducting a thorough examination (Leff, 1976). The presence of gaming or elements that exploit gamblers' fallacies also plays a role in the Big Con and other scams. Taking advantage of the "near-win" effect, where individuals believe that close-but-no-win experiences increase their chances of winning, con artists keep their marks invested over time rather than taking a large sum all at once (Chowdhury and Abedin, 2020).

These six mechanisms are common in scam scripts and have been observed in both historical and modern scams. In the realm of cryptocurrency trading, scams continue to rely on these classic essential elements. It is important to note that while digital technology may facilitate scams in terms of speed, distance, and volume, the underlying scam routines have only required minor

adaptations and transformations. However, crypto frauds have also become a cultural form integral to their own spaces, highlighting the hybridization of online and offline culture, economy, and social life (Grabosky and Walkley, 2007; Wall, 2015; Levi et al., 2015).

Progress in Cryptocurrency Markets

Blockchains, known as online distributed ledgers, eliminate the need for human intervention in verifying transactions due to the use of algorithms (Zook and Blankenship, 2018). These distributed ledgers store virtual currencies in digital token form. By 2020, the rise of DeFi (decentralized finance) resulted in widespread use of decentralized exchanges ('dex'), enabling users to trade tokens through a web-based interface. The dex serves as a mechanical intermediary, rendering banks and other intermediaries unnecessary. To ensure the functionality of these decentralized token exchanges, dex liquidity is crucial. In essence, liquidity acts as a repository of tradable tokens from which buyers can draw to fulfil their token orders (Chowdhury and Humaira, 2023a). Token issuers and subsequent traders contribute to the pool of available liquid assets. Deposited liquidity takes the form of token loans, which the dex utilizes to settle the trades of other users in exchange for a share of the dex's trading fees (Chowdhury & Begum, 2012) .

DeFi has opened up new investment and profit opportunities. The concept of DeFi is to liberate financial product markets from the control of centralized institutions in the current economic system (Härdle et al., 2020). DeFi allows users to participate in activities like obtaining loans, investing for yield, speculating on future price fluctuations, and utilizing their money in various ways, without requiring credit checks, bank accounts, or character references. However, alongside the benefits of DeFi and decentralization, it is important to be aware of potential drawbacks.

In a decentralized market, individuals have full control over their finances without external support (Chowdhury, 2021). There are no confirmation processes for transfers, no customer service hotlines to call for assistance, no age restrictions, and no daily limits on transfer amounts or numbers. Furthermore, there are no restrictions on recipients, regardless of their age, gambling habits, mental stability, or financial standing. This market is open to anyone with internet access and a high tolerance for financial risk (compare Van Wyk and Benson, 1997 with Schoepfer and Piquero, 2009). If funds are mistakenly sent to the wrong person, attempts to retrieve the money will likely be futile. Poor investment decisions or selling during market downturns are solely the

individual's responsibility. Additionally, acting as a liquidity provider for a dex by lending tokens to the platform carries the risk of losing those tokens if the dex goes out of business or ceases to exist.

The Growth of Cryptocurrency Markets

Cryptocurrency trading has given rise to a subculture of crypto investors who congregate in online communities to discuss market trends, strategies, and technical analysis (Pathak, 2018). Platforms such as Telegram, Discord, and Reddit are popular forums for these discussions. Within these communities, a range of topics is covered, from rational market analysis to the promotion of risky investments known as "shitcoins." Shitcoins refer to tokens with low market capitalization and recent release dates, which offer the potential for high rewards but also carry significant risks (Chowdhury, 2024).

The fear of missing out (FOMO) and the desire to make quick profits drive some traders, referred to as "degens," to quickly invest in shitcoins in a practice known as "aping" or "yoloing" (Grauer and Updegrave, 2021). They hope to experience the excitement of witnessing the value of their investments skyrocketing in a short period. However, the volatile nature of these investments also means that losses can be equally shocking and devastating. To avoid the risks associated with FOMO, it is crucial for traders to conduct their own research (DYOR) and evaluate the fundamentals and pumpamentals of a token before investing (Chowdhury & Reza, 2013).

One notable characteristic of the crypto industry is the prevalence of vaporware, which refers to technical solutions that have not yet been implemented. Unlike the traditional stock market, where the term "fundamentals" is used to assess the value of an investment, the crypto industry emphasizes "pumpamentals" (Grauer and Updegrave, 2021). Pumpamentals refers to the likelihood that a shitcoin will generate FOMO and experience a significant price increase.

In the world of crypto trading, there is a running joke about buying a Lamborghini (Pathak, 2018). The idea is that investing in a shitcoin early on and seeing it experience a massive price surge could potentially generate enough profits to afford a luxury car like a Lamborghini. This playful aspiration is often shared through photos of flashy cars on crypto forums (Chowdhury, 2023).

The socioeconomic backdrop of the crypto market sets the stage for fraud to flourish (Warren, 2020). Firstly, market abuse is prevalent, with whales (individuals or entities holding a large number of tokens) manipulating prices to their advantage. This manipulation can lead to sudden price drops and panic selling among smaller traders. Secondly, rapid financial failures, such as project cancellations or exchange hacks, have become common in the crypto industry, causing investors to accept the possibility of losing their funds (Grauer and Updegrave, 2021). Finally, the decentralized nature of cryptocurrencies makes it challenging to seek legal recourse or obtain restitution in the event of fraud (Ross and Smith, 2011).

Although crypto scams account for a significant portion of crypto-related crime, law enforcement and regulators have shown limited interest in pursuing these cases (Warren, 2020). This lack of regulation adds to the perception that traders are responsible for their own actions and losses in the crypto market. As a result, self-help avoidance techniques and awareness-raising efforts play a vital role in preventing fraud (Shadel, 2012; Chowdhury et al., 2022).

The growth of crypto markets has fostered a subculture of investors driven by the fear of missing out and the allure of high-risk, high-reward investments. While these markets offer opportunities for profits, they are also rife with risks, including market abuse, rapid financial failures, and scams. As the crypto industry remains largely unregulated, traders must navigate this landscape with caution and skepticism.

We discovered a cluster of 'wild west' signals in the crypto space, shedding light on the uncharted cultural and economic territory known as the technosocial grey region (Grabosky et al., 2001; Wall 2007). Within this space, there exists a vulnerable population of individuals who are easy prey for con artists in the decentralized trading environment. These individuals include those who blindly enter highly speculative investments with a low risk threshold, those who anticipate market manipulation and do not expect fairness, those who accept financial loss as a cost of doing business, and those who do not report crimes (Grabosky et al., 2001; Wall, 2007).

The conditions in this environment are conducive to fraud, where fear of missing out (FOMO) thrives, and discussions of "pumfamentals" and quick investments dominate online forums. The anonymity and global availability of the internet allow fraudsters to converse simultaneously with

hundreds, or even thousands, of individuals located worldwide, facilitating instantaneous transfers and disappearing without a trace (Grabosky et al., 2001; Wall, 2007).

As a result, fraud, particularly pump-and-dump schemes (Kamps and Kleinberg, 2018) and Ponzi schemes, thrives in the cryptocurrency industry. Pump-and-dump schemes involve manipulating the price of a cryptocurrency through promotion and subsequent sale by insiders, leading to significant value increases followed by crashes (Stevenson, 2000; Shover et al., 2003). Ponzi schemes, similar to pump-and-dump in spirit, rely on attracting new investors whose funds are used to pay dividends to earlier investors (Balleisen, 2017; Chowdhury et al., 2021).

Both pump-and-dump and Ponzi schemes are characterized by their ability to exploit the fear of missing out (FOMO) and the psychological principle of coming close to success (Grabosky et al., 2001; Wall, 2007). It can be challenging to distinguish legitimate influencers from orchestrated pump-and-dump schemes, making it crucial for individual traders to remain vigilant and view any investment calls with suspicion (Smith, 2007). By adopting a proactive approach and refusing to succumb to FOMO, traders can play a significant role in preventing such fraud (Smith, 2007; Schulte, 1995; Shadel, 2012).

Advanced fee frauds, such as giveaway scams and cry for aid scams, are also prevalent in the cryptocurrency industry. Giveaway scams involve fraudsters posing as influential figures in the crypto industry, promising to multiply cryptocurrency sent to them as part of a giveaway. Victims who send cryptocurrency never receive any in return (Grabosky et al., 2001). Cry for aid scams exploit the cardinal sin of sharing seed phrases by pretending to need assistance with a broken wallet, leading victims to deposit gas into the wallet, which is then redirected to the con artist (Grabosky et al., 2001).

Rug pulls, another form of exit scam, are characterized by the developer gradually selling off tokens after the project's launch, causing the price to fall and eventually resulting in project failure (Levine, 2021). The slow rug pullers often engage with investors in Telegram channels, employing techniques such as "cooling out" to prevent victims from reporting the crime and keeping them on the hook until the scam is complete (Goffman, 1959).

In order to protect themselves from such fraudulent activities, traders must be aware of the risks associated with new ventures that lack reliable data. While some warning signs may be detectable, the temptation to invest in potential high-profit opportunities can be strong. Traders must exercise caution and only invest amounts they can afford to lose (Grabosky et al., 2001; Wall, 2007). By being vigilant and informed, traders can contribute to preventing fraud in the cryptocurrency market (Smith, 2007).

Revamping the Section: Metaverse and the Future of Technosocial Grey Crypto Economy

Scams have become alarmingly common in the unregulated world of crypto trading, leading to their acceptance as an expected part of the experience and diminishing their legitimacy as serious grievances. With the crypto industry still mostly devoid of legal regulations, responsible traders operate on the principle of "buyer beware," while fraudsters exploit countless variations on well-known scams. These ever-evolving fraudulent practices are the root cause of the widespread deception plaguing this sector (Chai et al., 2022; Chowdhury, 2016).

Traders who fall victim to scams like sending Bitcoin to unfamiliar addresses in the hope of receiving a larger amount in return, succumbing to manipulative cries for help, getting caught up in pump and dump schemes, falling prey to rug pulls, or investing too late in Ponzi tokens all share a common belief that they should have been more cautious, ultimately owning partial responsibility for their misfortunes (Hajek et al., 2023). Although these scams often present themselves as legitimate opportunities, they are inherently harmful and morally wrong. Many of these schemes exploit the adage, "You can't trick an honest man," creating the illusion that the odds are stacked in the victim's favor. In hindsight, the irresistibly enticing offers presented by these scams are evidently fraudulent.

These scams heavily rely on time pressure and swift responses, leaving little room for contemplation. In certain scenarios, such as giveaway scams, there may be a limited-time offer, while in others, participants are led to believe that being among the first to engage is crucial. These tactics borrow proven methods from the gaming industry, enticing individuals with promises of substantial payouts for small investments or leveraging the psychological phenomenon of the "near win" to encourage continued betting after a close call.

Policy Recommendations

Government and Regulatory Agencies

The government should enact new legislation specifically targeting cryptocurrency scams, providing legal frameworks for addressing fraud. Regulatory agencies should allocate resources to investigate and prosecute these scams, utilizing specialized cybercrime units and collaborations with international law enforcement agencies. Governments should also invest in public awareness campaigns to educate consumers about the risks associated with cryptocurrency scams and provide guidance on how to identify and avoid fraudulent schemes. Regulatory authorities should foster international cooperation to combat cross-border cryptocurrency scams, sharing information and best practices to effectively address fraud in the global market (Chowdhury and Humaira, 2023b).

Crypto Exchanges and Platforms

Crypto exchanges and platforms should enhance their Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures to verify and validate the identities of users, reducing the risk of fraudulent activities. They should prioritize security protocols, including multi-factor authentication, encryption, and cold storage of funds, to protect users from hacking and unauthorized access (Moula et al., 2017; Chowdhury, 2018). Exchanges and platforms should provide clear and comprehensive information about listed projects, including their team members, technology, and audited financial reports, to enable investors to make informed decisions and avoid scams. Additionally, crypto exchanges should collaborate to establish self-regulatory bodies that set industry standards, promote best practices, and enforce compliance to prevent fraudulent activities (Chowdhury and Khan, 2023).

Financial Institutions

Financial institutions should implement advanced monitoring systems to detect and report suspicious transactions related to cryptocurrency scams, enabling swift action by law enforcement agencies. They should develop risk assessment frameworks specific to cryptocurrency-related activities, enabling them to identify and mitigate potential risks associated with fraudulent schemes. Financial institutions can play a crucial role in educating their customers about the risks of cryptocurrency scams, providing guidance on how to protect their investments and report suspicious activities.

Education and Research Institutions

Educational institutions and research organizations should promote interdisciplinary research on cryptocurrency scams, combining expertise from fields such as criminology, law, economics, and technology to develop comprehensive strategies for combating fraud. Educational curricula should integrate cryptocurrency education to equip individuals with the knowledge and skills to navigate the crypto market safely, recognize scams, and protect themselves from fraudulent activities. Academic institutions should collaborate with industry stakeholders, such as exchanges, regulatory agencies, and cybersecurity firms, to exchange knowledge, share insights, and develop proactive measures against cryptocurrency scams.

Cryptocurrency Community

The cryptocurrency community should establish self-regulatory initiatives, such as codes of conduct and ethical guidelines, to foster a culture of transparency, integrity, and responsible trading. Community members should actively share information, experiences, and warnings about cryptocurrency scams to help protect each other from falling victim to fraudulent schemes. Crypto enthusiasts should advocate for responsible regulation of the industry, emphasizing the need for consumer protection, market integrity, and the prevention of fraudulent activities (Chowdhury, 2023).

Conclusion

Cryptocurrency scams pose significant risks to investors, undermine market integrity, and impede the growth and development of the cryptocurrency ecosystem. Addressing these scams requires a multi-faceted approach involving various stakeholders. For governments and regulatory agencies, enacting new legislation, enhancing enforcement activities, and improving consumer education are crucial steps. By providing clear regulations, allocating resources for investigations, and raising awareness about the risks associated with cryptocurrency scams, governments can protect consumers and maintain financial stability. Additionally, international collaboration is essential to combat cross-border fraud and promote global market integrity. Cryptocurrency exchanges and platforms also have a responsibility to address scams. By implementing stricter due diligence processes, enhancing security measures, and providing transparent information, exchanges can create a safer trading environment for users. Establishing self-regulatory mechanisms and

collaborating with industry peers can further promote best practices and compliance. Financial institutions play a pivotal role in combating scams by monitoring suspicious transactions and developing risk assessment frameworks specific to cryptocurrencies. They can also educate customers about the risks and provide guidance on protecting investments and reporting suspicious activities. Education and research institutions should foster interdisciplinary research on cryptocurrency scams and incorporate cryptocurrency education into curricula. By equipping individuals with knowledge and skills to navigate the market safely, these institutions can empower them to recognize scams and protect themselves. The cryptocurrency community itself can contribute to combating fraud by promoting self-regulation, advocating for responsible regulation, and advocating for peer-to-peer support. Building a culture of transparency, integrity, and responsible trading can help protect community members from falling victim to scams.

References

1. Abdullah, M.N., Chowdhury, E.K. & Tooheen, R.B. (2022). Determinants of capital structure in banking sector: a Bangladesh perspective. *SN Bus Econ.* 2, (190). https://doi.org/10.1007/s43546-022-00370-8
2. Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2023). Blockchain and crypto forensics: Investigating crypto frauds. International Journal of Network Management, e2255. https://doi.org/10.1002/nem.2255
3. Baldwin, J. (2018), 'In Digital We Trust: Bitcoin Discourse, Digital Currencies, and Decentralised Network Fetishism', *Palgrave Communications,* 4(14): 1–10. DOI: https://doi.org/10.1057/s41599-018-0065-0
4. Balleisen, E. (2017), *Fraud: An American history from Barnum to Madoff*. Princeton University Press. Banerjee, P. (2021), *Microsoft details plans for building a metaverse for enterprises*, Mint [Online]. Available at: https://www.livemint.com/industry/infotech/microsoft-reveals-metaverse-plans-for-the-enterprise-11635897733673.html [accessed 15 November 2021].
5. Chowdhury E.K, & Khan I.I. (2023). Reactions of Global Stock Markets to the Russia–Ukraine War: An Empirical Evidence, *Asia-Pacific Financial Markets*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1007/s10690-023-09429-4
6. Chowdhury E.K, Khan I.I, Dhar B.K. (2021). Catastrophic impact of Covid-19 on the global stock markets and economic activities. *Business & Society Review*, 127 (2), 437-460. https://doi.org/10.1111/basr.12219
7. Chowdhury E.K, Khan I.I, Dhar B.K. (2023). Strategy for implementing blockchain technology in accounting: Perspectives of stakeholders in a developing nation. *Business Strategy & Development,* 6 (3), 477-490. https://doi.org/10.1002/bsd2.256

8. Chowdhury, E, K., & Islam, A. (2017). Role of Foreign Direct Investment in the Stock Market Development of Bangladesh- A Cointegration and VAR Approach. *The Bangladesh Accountant*, April-June, 2017, 63-74. The Institute of Chartered Accountants of Bangladesh. https://tinyurl.com/y8hs2paf
9. Chowdhury, E. K (2021). Does Internal Control Influence Financial Performance of Commercial Banks? Evidence from Bangladesh. *South Asian Journal of Management*, 28(1), 59-77. https://tinyurl.com/59nr5axm
10. Schoepfer, A. and Piquero, N.L. (2009), 'Studying the Correlates of Fraud Victimization and Reporting', *Journal of Criminal Justice*, 37(2): 209–15. Doi: https://doi.org/10.1016/j.jcrimjus.2009.02.003
11. Schulte, F. (1995), *Fleeced!: Telemarketing Rip-offs and How to Avoid Them*. Prometheus Books.
12. Shadel, D. (2012), *Outsmarting the Scam Artists: How to Protect Yourself From the Most Clever Cons*. John Wiley & Sons.
13. Chowdhury, E. K. (2012). Impact of inflation on bank lending rates in Bangladesh. Journal of Politics and Governance, 1(1), 5-14. https://tinyurl.com/26y2pw6y
14. Chowdhury, E. K. (2012). The Impact of Merger on Shareholders' Wealth. *International Journal of Applied Research in Business Administration and Economics*, 1(2), 27-32. https://tinyurl.com/ycxt59vz
15. Chowdhury, E. K. (2016). Investment Behavior: A Study on Working Women in Chittagong. *Premier Critical Perspective*, 2 (1). 95-109. http://digitalarchives.puc.ac.bd:8080/xmlui/handle/123456789/67
16. Chowdhury, E. K. (2017). Functioning of Fama-French Three- Factor Model in Emerging Stock Markets: An Empirical Study on Chittagong Stock Exchange, Bangladesh. Journal of Financial Risk Management, 6(4), 352-363. https://doi.org/10.4236/jfrm.2017.64025
17. Chowdhury, E. K. (2017). Measuring the Effect of Macroeconomic Variables on the Stock Market Return: Evidence from Chittagong Stock Exchange. AU -International e-Journal of Interdisciplinary Research, 2(2), 1-10. http://www.assumptionjournal.au.edu/index.php/eJIR/article/view/4227
18. Chowdhury, E. K. (2021). Financial accounting in the era of blockchain-a paradigm shift from double entry to triple entry system. Available at SSRN 3827591. http://dx.doi.org/10.2139/ssrn.3827591
19. Chowdhury, E. K. (2021). Prospects and challenges of using artificial intelligence in the audit process. In Abedin, M.Z., Hassan, M.K., Hajek, P. (eds.) The Essentials of Machine Learning in Finance and Accounting (pp. 139-155). Routledge. https://tinyurl.com/4stz7ycj
20. Chowdhury, E. K. (2022). Disastrous consequence of coronavirus pandemic on the earning capacity of individuals: an emerging economy perspective. SN Bus Econ. 2(153). https://doi.org/10.1007/s43546- 022-00333-z
21. Chowdhury, E. K. (2023). Is the Application of Blockchain Technology in Accounting Feasible? A Developing Nation Perspective. In Abedin, M.K., Hajek, P. (eds.) Cyber

Security and Business Intelligence Innovations and Machine Learning for Cyber Risk Management (pp. 46-64). Routledge. https://doi.org/10.4324/9781003285854
22. Chowdhury, E. K. (2024). Cultural Norms and Their Effect on Entrepreneurial Endeavors: Perspectives from Bangladesh. Journal of Developmental Entrepreneurship, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1142/S1084946724500079
23. Chowdhury, E. K. (2024). Do weather patterns effect investment decisions in the stock market? A South Asian perspective. Journal of Asset Management, 25(2), 162-171. https://doi.org/10.1057/s41260-023-00334-z
24. Chowdhury, E. K. (2024). Examining the benefits and drawbacks of social media usage on academic performance: a study among university students in Bangladesh. Journal of Research in Innovative Teaching & Learning, 1-17, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JRIT-07-2023-0097
25. Yar, M. (2005), 'The Novely of Cybercrime', *European Journal of Criminology,* 2(4): 407–27. Doi: https://doi.org/10.1177/147737080556056
26. Zook, M.A. and Blankenship, J. (2018), 'New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance', *Geoforum,* 96: 248–55. Doi: https://doi.org/10.1016/j.geoforum.2018.08.023
27. Chowdhury, E. K., & Abdullah, M. N. (2023). Gauging Demand for Cryptocurrency over the Economic Policy Uncertainty and Stock Market Volatility. *Computational Economics*, 1-19. https://doi.org/10.1007/s10614-023-10423-1
28. Chowdhury, E. K., & Abedin, M. Z. (2020). COVID-19 effects on the US stock index returns: an event study approach. Available at SSRN 3611683. http://dx.doi.org/10.2139/ssrn.3611683
29. Chowdhury, E. K., & Begum. R. (2012). Reward Management as Motivational Tool in Various Industries in Bangladesh: An empirical study. *International Journal of Contemporary Business Studies*, 3(11), 22-34. https://tinyurl.com/3vzu9cu8
30. Chowdhury, E. K., & Chowdhury, G. M. (2014). Applicability of Prediction Techniques in the Stock Market-A Chittagong Stock Exchange Perspective. *International Journal of Advanced Information Science and Technology*, 32(32), 126-136, DOI:10.15693/ijaist/2014.v3i12.124-134
31. Chowdhury, E. K., & Chowdhury, R. (2017). Online Shopping in Bangladesh: A Study on the Motivational Factors for Ecommerce that Influence Shopper's Affirmative Tendency towards Online Shopping. *South Asian Journal of Marketing & Management Research*, 7(4). 20-35. DOI:10.5958/2249-877X.2017.00019.4
32. Chowdhury, E. K., & Chowdhury, R. (2022). Empirical research on the relationship between renewable energy consumption, foreign direct investment and economic growth in South Asia. *Journal of Energy Markets*, *15*(2). 1-21, https://DOI:10.21314/JEM.2022.012
33. Chowdhury, E. K., & Chowdhury, R. (2023). Role of financial inclusion in human development: Evidence from Bangladesh, India and Pakistan. *Journal of the Knowledge Economy*, 1-26. https://doi.org/10.1007/s13132-023-01366-x

34. Chowdhury, E. K., & Humaira, U. (2023). The Russia–Ukraine conflict and investor psychology in financial markets. *Economic Affairs*, *43*(3), 388-405. https://doi.org/10.1111/ecaf.12596
35. Chowdhury, E. K., & Humaira, U. (2023). Transformation of investor attitude towards financial markets: A perspective on the Russia–Ukraine conflict. *International Social Science Journal*. 74(252), 561-583. https://doi.org/10.1111/issj.12470
36. Chowdhury, E. K., & Nahar, S. (2017). Perceptions of Accountants toward Sustainability Development Practices in Bangladesh. *Journal of Management and Sustainability*,7(3), 112-119. doi:10.5539/jms.v7n3p112
37. Chowdhury, E. K., & Reza, T. (2013). Diagnostic Study on Interactive Ads and Its Response towards the FM Radio. *International Journal of Research in Commerce, IT & Management*, 3(2), 36-41. https://tinyurl.com/5n8huanv
38. Chowdhury, E. K., Abdullah, M. N., & Tooheen, R. B. (2021). Role of information and communication technology in economic progress and increasing demand for renewable energy: evidence from China and India. *Asian Journal of Technology Innovation*, 30(3), 651-671. https://doi.org/10.1080/19761597.2021.1961090
39. Silver, C. (2020), *What is Web 3.0?*, Forbes [Online]. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/01/06/what-is-web-3-0/?sh=6164d5ad58df [accessed 15 November 2021].
40. Smith, R.G. (2007), 'Consumer Scams in Australia: An Overview', *Trends & Issues in Crime and Criminal Justice No. 331*. Australian Institute of Criminology.
41. Smith, R.G., Holmes, M.N. and Kauffman, P. (1999), 'Nigerian Advance Fee Fraud', *Trends & Issues in Crime and Criminal Justice No. 121*. Australian Institute of Criminology.
42. Chowdhury, E. K., Dhar, B. K., & Stasi, A. (2022). Volatility of the US stock market and business strategy during COVID-19. *Business Strategy & Development*, 1–11. https://doi.org/10.1002/bsd2.203
43. Chowdhury, E. K., Dhar, B. K., Gazi, M., & Issa, A. (2022). Impact of Remittance on Economic Progress: Evidence from Low-Income Asian Frontier Countries. *Journal of the Knowledge Economy*, 1-26. https://doi.org/10.1007/s13132-022-00898-y
44. Chowdhury, E. K., Dhar, B. K., Thanakijsombat, T., & Stasi, A. (2022). Strategies to determine the determinants of financial performance of conventional and Islamic commercial banks: Evidence from Bangladesh. *Business Strategy & Development*, 1–19. https://doi.org/10.1002/bsd2.207
45. Chowdhury, E. K., Stasi. A. & Pellegrino. A. (2023). Blockchain Technology in Financial Accounting: Emerging Regulatory Issues. *Review of Economics and Finance*. 21 (1), 862-868. https://refpress.org/ref-vol21-a94/
46. Chowdhury, E.K. (2018). An Assessment of Return Spillover Among Selected Stock Markets in SAARC Countries. *South Asian Journal of Management*, 25 (1), 51-63. Association of Management Development Institutions in South Asia. https://tinyurl.com/y2bd39tk

47. Wall, D.S. (2015), 'The Internet as a Conduit for Criminal Activity', in A. Pattavina, eds, *Information Technology and the Criminal Justice System*. 77–98. Sage.
48. Warren, J.M. (2020), 'A Too Convenient Transaction: Bitcoin and Its Further Regulation', *Journal of Law & Cyber Warfare,* 8(1): 5–29.
49. Chowdhury, E.K. (2018). Does Foreign Direct Investment Stimulate Economic Progress of a Developing Country? Empirical Evidence from Bangladesh. *CIU Journal*, 1 (1), 71-86. Chittagong Independent University. https://tinyurl.com/3scz3jzh
50. Chowdhury, E.K. (2019). An Empirical Study of Volatility in Chittagong Stock Exchange. *CIU Journal*, 2 (1), 19-38. Chittagong Independent University. https://tinyurl.com/3w6k89k8
51. Chowdhury, E.K. (2019). Transformation of Business Model through Blockchain Technology. *The Cost and Management*, 47(5), 4-9. The Institute of Cost and Management Accountants of Bangladesh. https://tinyurl.com/bdz4ns7t
52. Chowdhury, E.K. (2020). Catastrophic Impact of Covid-19 on Tourism Sector in Bangladesh: An Event Study Approach. *The Cost and Management*, 48(4), 43-52. The Institute of Cost and Management Accountants of Bangladesh. https://tinyurl.com/ccu6mkbx
53. Chowdhury, E.K. (2020). Is Capital Market Integration among the SAARC Countries Feasible? An Empirical Study. *Eurasian Journal of Business and Economics*, 13(25), 21-36. https://doi.org/10.17015/ejbe.2020.025.02
54. Chowdhury, E.K. (2020). Non-Performing Loans in Bangladesh: Bank Specific and Macroeconomic Effects. *Journal of Business Administration*, 41(2), 108-125. University of Dhaka. https://tinyurl.com/54f5pexw
55. Chowdhury, E.K. (2020). Volatility in Cryptocurrency Market–Before and During Covid-19 Pandemic. *CIU Journal*, 3(1), 69-86. Chittagong Independent University. https://tinyurl.com/mr3djzcn
56. Chowdhury, E.K. (2022). Strategic approach to analyze the effect of Covid-19 on the stock market volatility and uncertainty: a first and second wave perspective, *Journal of Capital Markets Studies*, 6(3), 225-241. https://doi.org/10.1108/JCMS-05-2022-0015
57. Chowdhury, E.K. (2023). Integration of Artificial Intelligence Technology in Management Accounting Information System: An Empirical Study. In: Abedin, M.Z., Hajek, P. (eds) Novel Financial Applications of Machine Learning and Deep Learning. International Series in Operations Research & Management Science, vol 336. Springer, Cham. https://doi.org/10.1007/978-3-031-18552-6_3
58. Chowdhury, E.K., & Rozario, S. O. (2018). Impact of Attitude and Awareness of Investors on their Investment Behavior- A Study on Bangladesh Stock Market. *The Bangladesh Accountant*, July- September, 81-89. The Institute of Chartered Accountants of Bangladesh. https://tinyurl.com/4av6swas
59. Chowdhury, EK (2020). India's NRC, CAA may take Bangladesh closer to China. *Asian Regional Review*, Diverse Asia, Seoul National University Asia Center, 3(2). https://diverseasia.snu.ac.kr/?p=4525

60. Chowdhury, M.R.A., & Chowdhury, E. K. (2010). Estimation of Stock Market Risk-A Value at Risk Approach. *The Cost & Management*, 38(4), 22-27. https://tinyurl.com/4ax978ud
61. Chowdhury, M.R.A., Chowdhury, E. K., & Chowdhury, T. U. (2015). Application of Capital Asset Pricing Model: Empirical Evidences from Chittagong Stock Exchange. *The Cost & Management,* 43(03), 38-44. https://tinyurl.com/bddv24cy
62. Wong, W.H. and Duncan, J. (2021), *Facebook's metaverse won't be bound by physical borders—neither are human rights*, The Globe and Mail [Online]. Available at: https://www.theglobeandmail.com/opinion/ article-facebooks-metaverse-wont-be-bound-by-physical-borders-neither-are/ [accessed 15 November 2023].