Multivariate Analysis in Forensic Approaches to Tackling Fake Cryptocurrencies and Valuation Fraud

Mohammed Suhail A[1], Sreeram K Y[2]
[1]*RR Institute of Management Studies, Bengaluru, INDIA*
[2]*Assistant Professor, Department of Forensic science, RR Institute of Management Studies, Bengaluru*

***Abstract*— Cryptocurrencies are digital assets that run over a blockchain network and are secured by cryptography that guarantees transaction anonymity and integrity. They are decentralized financial tools that broke away from the supervision of traditional institutions like banks or governments. Users have autonomy but also face new challenges.**

This study offers a forensic perspective for identifying the valuation fraud and counterfeit cryptocurrencies, emphasizing the need to comprehend and control associated risks. Examining both conventional and so-called cryptocurrencies, it reveals the causes of illegal activities such supply manipulation, speculative trading, and fraudulent schemes. The study also emphasizes the risks associated with utilizing third-party applications, which typically lack strong cyber security safeguards, for digital currency transactions. In the case of digital currency, these disadvantages put users at risk of financial exploitation, theft, and data breaches. Thus, they facilitate ransomware attacks, identity theft, and other illicit financial operations.

This research shows how investigators can follow the trail of digital money to break up fraud networks and make online security better. It suggests that we need stricter rules, continuous improvement in investigation techniques, and better education for users to keep the digital world safe. By combining forensic science with advanced analysis, we aim to keep the market fair, protect investors, and build trust in cryptocurrency markets.

***Index Terms*—cryptocurrency, blockchain, cyber, online frauds, valuation fraud.**

I. INTRODUCTION

Cryptocurrencies have evolved over the years, offering a decentralized digital monetary system unlike traditional financial systems. These digital assets operate on blockchain technology and are secured by cryptographic techniques, ensuring transaction integrity and user anonymity (Nakamoto, 2008). This emerging currency also brought several new concerning risks, which includes valuation fraud, counterfeit digital currencies, and illegal financial activities (Brenig, 2015).

The lack of centralized regulatory supervision has made cryptocurrencies appealing to both genuine investors and crooks. Fraudsters take use of the anonymity and decentralized nature of these digital assets to influence supply, engage in speculative trading, and plan fraudulent schemes (Gandal, 2018). Furthermore, the use of third-party applications for digital transactions, many of which lack effective cybersecurity protections, has raised the danger of financial exploitation, data breaches, and identity theft (Conti, 2018).

Forensic science contributes significantly to tackling these difficulties by offering systematic investigation procedures for tracing fraudulent activity, analyzing financial transactions, and uncovering criminal networks (Kethineni, 2020). This study investigates multivariate forensic analytic techniques for detecting and preventing bitcoin fraud, hence assuring market transparency and investor safety. By merging forensic science with cutting-edge digital analytics, the study seeks regulatory frameworks, improve investigative methods, and foster trust within the cryptocurrency ecosystem. (Trozze, 2022) identify various fraudulent schemes, including Ponzi schemes, pump-and-dump tactics, and ransomware attacks, which exploit market volatility and investor naivety. Regulatory frameworks play a crucial role in mitigating these risks, as discussed by (Trautman, 2024), who emphasize the SEC's role in enforcing compliance and investor protection.

(Trozze, 2022) and (Garba, 2024) claim that the cryptocurrency market is defined by sudden price fluctuations, fraud susceptibility, and links to financial crimes including Ponzi schemes and money

laundering. This article should highlight the main research results on the financial implications, regulatory responses, risks, and acceptability of cryptocurrencies. By examining market trends, security concerns, and impending challenges, it seeks to provide a comprehensive understanding of how cryptocurrencies are evolving within the global financial ecosystem.

II. CONVENTIONAL VS. SO-CALLED CRYPTOCURRENCIES

The cryptocurrency environment may be largely divided into two types: traditional cryptocurrencies and so-called cryptocurrencies, which are frequently false or deceptive digital assets aimed to defraud investors.

Traditional cryptocurrencies, such as Bitcoin (BTC), Ethereum (ETH), and Litecoin (LTC), are well-established, run on well recognized blockchain networks, and adhere to open protocols. They are backed by strong cryptographic techniques, decentralized networks, and vibrant development communities that assure security and functioning (Conti, 2018). These digital assets are utilized in transactions, smart contracts, and Decentralized finance applications.

On the other side, so-called cryptocurrencies are false digital assets that have the appearance of authentic cryptocurrencies but lack transparency, security, or true blockchain capability. These include scam tokens, Ponzi schemes, and fraudulent Initial Coin Offerings (ICOs), which frequently entice investors with promises of great returns but eventually lead to financial losses (Gandal, 2018). Fraudsters behind these scams control supply, engage in wash trading, and employ aggressive marketing efforts to build fakes demand before performing "rug pulls" in which developers quit the project and flee with investors' funds.

The growing prevalence of such fraudulent schemes emphasizes the necessity for a forensic approach to detecting and reducing bitcoin fraud. This research looks on forensic approaches for distinguishing between authentic and fraudulent cryptocurrencies, detecting valuation fraud, and building regulatory frameworks to improve security in the digital financial ecosystem.

III. AIM OF THE STUDY

This research aims to find out what causes valuation fraud and the rise of fake cryptocurrencies. It looks closely at both real and fake cryptocurrencies, examining factors like price changes, market actions, and ways to spot fraud. The study also includes a Multivariate analysis to evaluate how market manipulation and security flaws impact the cryptocurrency market. The goal is to promote better market transparency, protect investors, and create regulatory guidelines. Additionally, the research discusses data breaches related to third-party apps that request access to features like the microphone, files, contacts, and location

IV. OBJECTIVES OF THE STUDY

- To study and compare the price trends and fluctuations of real and fake cryptocurrencies.
- To look into how speculative trading, supply manipulation, and scams affect cryptocurrency prices.
- To evaluate the cybersecurity threats and weaknesses of third-party apps used for cryptocurrency transactions.
- To find out if the factors that cause price changes in regular cryptocurrencies also apply to fraudulent ones.
- To suggest ways to enhance regulation in the cryptocurrency market, improve investigation methods, and educate users.

V. METHODOLOGY

This study used a multivariate analysis technique to determine fraud trends in cryptocurrency marketplaces, combining quantitative financial modeling, blockchain forensic investigation, and cybersecurity risk assessment. Samples were selected from both conventional and so-called cryptocurrencies and the size for analysis was 5, then Real-time data was collected on leading cryptocurrencies and So-called Cryptocurrencies (meme) coins from sources like Coin Gecko, CoinMarketCap, and application known as Coin DCX.

- Time-Series Analysis: This study was used to analyze the past data with respect to

cryptocurrency prices for identifying patterns and trends. It also helped spot unusual price changes that could indicate fraudulent activities, like people trying to manipulate the prices. The research also looked at how certain events could affect cryptocurrency prices, and how groups of people might work together to artificially raise or lower the price of these digital assets.

- Principal Component Analysis (PCA): This was used to identify the fundamental characteristics that separate fraudulent from real cryptocurrency. It found to be the most prevalent indicators of fraud, such as Ponzi schemes or scams, by analyzing transaction volume, market value, and price fluctuations.
- Regression Model: A regression analysis was conducted to examine the impact of various activities on bitcoin pricing. This study aimed to determine whether fluctuations in price were attributable to speculative trading characterized by purchases driven by assumptions regarding insider information or recommendations wash trading, which involves artificially inflating demand for cryptocurrencies, or price manipulation tactics such as pump-and-dump schemes.
- Fake promotions and social media: These kind of fake promotions and social media has not only influenced but also played a major effect on cryptocurrency prices by spreading misleading information and creating fake demand in the market. Scammers used these deceptive techniques, advertisements and celebrity endorsements to lure in investors, and social media played a crucial role in boosting these strategies, relating to market sentiment and causing artificial price surges. This led to pump-and-dump schemes, leaving many investors with significant losses once the prices declined.

VI. RESULT AND DISCUSSIONS

1. Sample Size: The sample size selected for the analysis was 5.

Table 01: Conventional and so – called cryptocurrencies were taken.

Conventional Cryptocurrencies	So-called Cryptocurrencies
1. Bitcoin (BTC) – The first and most valuable cryptocurrency.	1. Dogecoin (DOGE) – The original meme coin.
2. Ethereum (ETH) – The leading smart contract platform.	2. Shiba Inu (SHIB) – A "Dogecoin killer" with no major use case.
3. Binance Coin (BNB) – Native token of Binance, the world's largest crypto exchange.	3. Floki Inu (FLOKI) – Dog-themed meme coin.
4. Ripple (XRP) – Fast, low-cost cross-border payments.	4. Pepe (PEPE) – Inspired by the internet meme.
5. Cardano (ADA) – Blockchain focused on scalability and sustainability.	5. Bonk (BONK) – A Solana-based meme coin.

2. Data Collection:

Real-time data was collected on leading cryptocurrencies and So-called Cryptocurrencies (meme) coins from sources like Coin Gecko, CoinMarketCap, and application known as Coin DCX.

Table 02: Primary data of Conventional Cryptocurrencies.

Cryptocurrency	Current Price (USD)	Market Capitalization (USD)	Price Change (30d)	Circulating Supply	Total Supply	All-Time High (ATH)	All-Time Low (ATL)
Bitcoin (BTC)	84,747.00	$1.68 trillion	-17.67%	19.83 million BTC	21 million BTC	$109,026.02 USD	$2.00 USD
Ethereum (ETH)	1,797.00	$220.7 billion	-11.24%	120.1 million ETH	Unlimited	$4,878.26 USD	$0.43 USD
Binance Coin (BNB)	335.25	$57.7 billion	-8.22%	155.9 million BNB	200 million BNB	$690.93 USD	$0.09 USD
Ripple (XRP)	1.06	$53.5 billion	-6.15%	50.3 billion XRP	100 billion XRP	$3.84 USD	$0.0028 USD

Table 03: Primary data of So-called Cryptocurrencies.

Cryptocurrency	Current Price (USD)	Market Capitalization (USD)	Circulating Supply	Total Supply	All-Time High (ATH)	All-Time Low (ATL)
Dogecoin (DOGE)	0.078	$10.4 billion	133.2 billion DOGES	Unlimited	$0.7376 USD	$0.000085 USD
Shiba Inu (SHIB)	0.000010	$5.6 billion	589.7 trillion SHIB	Unlimited	$0.000088 USD	$0.000000000056 USD
Floki Inu (FLOKI)	0.000009	$200 million	9.1 trillion FLOKI	Unlimited	$0.000236 USD	$0.000009 USD
Pepe (PEPE)	0.000003	$150 million	3.5 trillion PEPE	Unlimited	$0.00065 USD	$0.000002 USD
Bonk (BONK)	0.000002	$40 million	90.6 trillion BONKS	Unlimited	$0.000004 USD	$0.000002 USD

VII. DISCUSSION

1. Market Manipulation & Fraud Trends

An analysis of how prices move in both regular as well as different cryptocurrencies shows clear differences when it comes to how shaky or steady they are. Bitcoin (BTC) and Ethereum (ETH), which exist as cryptocurrencies, often have price shifts that are pretty stable; these shifts are affected by the financial state and new technology (Gandal et al., 2018). However, other cryptocurrencies vary a lot, usually moved by social media trends and schemes to pump and dump (Trozze et al., 2022).

Pump-and-Dump Patterns

The data present indicates that other cryptocurrencies often go through unexpectedly quick price rises and then especially steep drops. This case agrees with prior research about unsafe exchange, in which shared actions strangely increase worths of things before a major transaction occurs (Gandal et al., 2018). The wide-ranging three-year probe of pump-and-dump actions found over 900 dishonest events, implying that these plans are frequently made simpler by way of places such as Telegram and Conflict (Kamps & Kleinberg, 2021).

Wash Trading Indicators

Market capitalization versus transaction volume showed certain differences in meme coins, suggesting possible wash trading methods to make liquidity appear higher than it actually is. Wash trading has emerged as an important concern on unregulated exchanges (Cong et al., 2020). This trading involves traders executing simultaneous buy and sell orders to mislead many investors regarding demand. These specific actions closely match what detailed forensic finance studies have definitively found, showing that particularly dishonest deals can seriously skew market info (Brenig et al., 2015).

Fake Promotions & Social Media Influence

The impact of social media advertising was evident in the examined meme coins, as endorsements from celebrities and prevailing online trends led to considerable fluctuations in prices, often causing financial setbacks for average investors (Trozze et al., 2022). Research on market sentiment indicates that activity on platforms such as Twitter and Reddit directly influence cryptocurrency price movements, frequently surpassing the effects of fundamental economic factors (Lazer et al., 2021).

2. Security Risks in Third-Party Applications

Research demonstrates that third-party applications used for cryptocurrency trading and wallet management are significantly vulnerable to cyber threats. The study revealed multiple risks, including phishing attacks, in which malicious individuals utilize deceptive mobile applications to acquire private keys (Conti et al., 2018). Moreover, vulnerabilities in smart contracts present a notable danger, as numerous cryptocurrencies lack adequate security assessments, heightening the risk of rug pulls (Garba et al., 2024). Concerns regarding data privacy are also prevalent, with many applications demanding excessive permissions, which may lead to potential data breaches (Trautman et al., 2024). Additionally, the rise in cryptocurrency-related crimes, such as ransomware incidents, identity theft, and transactions on the dark web, can be attributed to security weaknesses in digital wallets and exchanges (Kethineni & Cao, 2020). A forensic analysis of crypto-theft and exchange vulnerabilities revealed that hot wallets and

centralized platforms are particularly attractive targets for cybercriminals, resulting in substantial financial losses (Conti et al., 2018).

3. Regression Model Results

Statistical analysis has revealed that fluctuations in the prices of fraudulent cryptocurrencies are more strongly associated with social media activity than with authentic market forces. Additionally, regression analysis has demonstrated that speculative trading significantly impacts valuations, often overshadowing fundamental economic indicators (Brenig et al., 2015). Moreover, Principal Component Analysis (PCA) has uncovered Ponzi-like traits in certain meme coins, suggesting that market demand is artificially maintained (Garba et al., 2024). In response to these challenges, machine learning models have been suggested to forecast fraudulent cryptocurrency activities by analyzing transaction patterns and market irregularities (Kamps & Kleinberg, 2021). These findings corroborate previous research in forensic finance and financial fraud detection, which emphasizes that the prices of digital assets are often subject to manipulation by both internal and external entities (Cong et al., 2020).

VIII. CONCLUSION

This study performs an extensive forensic examination of fraudulent activities in the cryptocurrency industry, focusing on valuation fraud, market manipulation, and related security risks. The findings indicate that cryptocurrencies are especially susceptible to fraudulent schemes, leading to significant financial losses for investors. The study highlights the critical role of forensic financial methodologies in detecting patterns of manipulation and stresses the necessity for regulatory measures to alleviate these risks. Enhancing security protocols, improving market transparency, and fostering user education are vital actions required to diminish fraudulent occurrences in the cryptocurrency landscape.

Future research should concentrate on using AI for fraud detection, exploring blockchain forensics, and understanding how cryptocurrencies relate to cybercrime. Investigating regulatory issues can lead to better fraud prevention strategies, and auditing smart contracts can boost security in decentralized finance (DeFi)

REFERENCES

[1] Brenig, C., Accorsi, R., & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. Proceedings of the 1st Workshop on Bitcoin Research.

[2] Cong, L. W., He, Z., & Li, W. (2020). Decentralized Finance: Blockchain Technology and the Future of Financial Intermediation. National Bureau of Economic Research (NBER).

[3] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452.

[4] Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price Manipulation in the Bitcoin Ecosystem. Journal of Monetary Economics, 95, 86-96.

[5] Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 325-344.

[6] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.

[7] Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price Manipulation in the Bitcoin Ecosystem. Journal of Monetary Economics, 95, 86-96.

[8] Garba, K. H., Lazarus, S., & Button, M. (2024). An assessment of convicted cryptocurrency fraudsters. Current Issues in Criminal Justice. https://doi.org/10.1080/10345329.2024.2403294

[9] Kamps, J., & Kleinberg, B. (2021). Pump-and-Dump Schemes in Cryptocurrency Markets: Detection and Analysis. arXiv Preprint.

[10] Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 325-344.

[11] Patsakis, C., Politou, E., Alepis, E., & Hernandez-Castro, J. (2024). Cashing out crypto: State of practice in ransom payments. International Journal of Information Security, 23, 699–712. https://doi.org/10.1007/s10207-023-00766-z

[12] Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting

anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33, 37. https://doi.org/10.1007/s12525-023-00654-3

[13] Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., & Davies, T. (2022). Cryptocurrencies and future financial crime: A systematic review. Crime Science, 11(1), 1-16. https://doi.org/10.1186/s40163-022-00172-7

[14] Trautman, L. J., Elzweig, B., & Newman, N. F. (2024). The SEC, fraud, and cryptocurrencies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4965035