Dean&Francis
ISSN 2959-6130

Analysis of Financial Fraud Crimes Involving Non-Legal Digital Currency: An Empirical Study Based on Multiple Cases

Yanchun Li

Affiliation: Chongqing Technology and Business University
Email: 1793248557@qq.com

Abstract:

With the proliferation of blockchain technology, financial fraud involving non-legal digital currency has become a prevalent type of crime in the digital economy. The 2020 "PlusToken scam" involved approximately 14.8 billion RMB, and the 2023 "Stellar Coin false ICO case" affected over 100,000 investors. Such crimes use "high returns" and "blockchain technology packaging" as bait, employing models like fake trading platforms, illegal ICOs, and pyramid-scheme-style referrals, severely infringing upon public property rights and disrupting financial order. Currently, ambiguities remain in the qualitative assessment and evidence identification of digital currency financial fraud under China's Criminal Law. This study aims to conduct an in-depth analysis of typical financial fraud cases to summarize fraud typologies and propose potential methods to reduce the probability of such crimes.

Keywords: Non-Legal Digital Currency, Refinement of Criminal Charges, Blockchain Technology, Empirical Research Method

1. Introduction

With the proliferation of blockchain technology, digital currency financial fraud has become a prevalent type of crime in the digital economy. The 2020 "PlusToken scam" involved approximately 14.8 billion RMB, and the 2023 "Stellar Coin false ICO case" affected over 100,000 investors. Such crimes use "high returns" and "blockchain technology packaging" as bait, employing models like fake trading platforms, illegal ICOs, and pyramid-scheme-style referrals, severely infringing upon public property rights and disrupting financial order.

Currently, ambiguities persist in the qualitative assessment and evidence identification of digital currency financial fraud under China's Criminal Law, necessitating improved institutional design based on empirical cases. Focusing on digital currency financial fraud as the core empirical subject, this study collects multiple typical cases such as "PlusToken" and "Stellar Coin". Using the empirical research method, it summarizes the behavioral pattern of "technical disguise - profit temptation - hierarchical diffusion". Combining normative analysis, it examines controversies in the application of charges and evidence identification within the current Criminal Law. By drawing on regulatory experiences from the United States and the European Union [4], it seeks to

fill theoretical gaps in the specific field of digital currency financial fraud and contribute to maintaining financial market stability.

2. Analysis of Behavioral Types and Characteristics of Digital Currency Financial Fraud

2.1 General Forms of Digital Currency Fraud

Referring to [1] Shi Xiuxia's "Research on Money Laundering Crimes Using Virtual Currency", the general forms of digital currency fraud include:

- Utilizing the anonymity, irreversibility, and speed of virtual currency for money laundering.
- Laundering money using virtual currency administrators or traders located in different countries with varying levels of regulation, or conspiring with them to launder money, or using virtual currency traders to perform multiple conversions between different types of virtual currency for money laundering.
- Utilizing third-party funding for money laundering, i.e., using peer-to-peer transfers to top up accounts, making uninformed or willing third parties act as "money mules".
- Laundering money using the non-face-to-face nature of virtual currency, including controlling legitimate user accounts for laundering and laundering directly using the anonymity of virtual currency.
- Combining with other payment methods for money laundering, integratively using fund transfer services, cash deposits/withdrawals, prepaid cards, money mules, and other means to acquire virtual currency and transfer funds.

2.2 Common Typical Fraud Case Types

Based on recent financial fraud cases, three core fraud types can be summarized:

- False ICO Fraud: As seen in the "Stellar Coin case", funds are raised by forging blockchain project whitepapers, fabricating technical teams, and using "low-price initial offering, future high-multiple appreciation" as bait.
- Fake Trading Platform Fraud: Some platforms create illusions of profit through "fake orders, price manipulation", inducing users to deposit funds before absconding with the money.
- Pyramid-Scheme-Style Referral Fraud: As seen in the "PlusToken case", incentives like "referral commissions, hierarchical dividends" are used to form a multi-level diffusion network involving over 2 million people.

2.3 Refine of Behavioral Characteristics

The core behavioral logic of this type of fraud is "technical term disguise - excessive profit temptation - target population propagation", possessing three core characteristics:

- High-Tech Nature: Relying on blockchain technology packaging, using professional terminology to conceal the fraudulent essence.
- Concealment: Utilizing the anonymity and decentralization characteristics of blockchain to evade tracking, making traces difficult to detect.
- Scale: Rapid diffusion through hierarchical referrals and online propagation, involving a large number of people and substantial amounts of money [5].

3. Analysis of the Causes of Digital Currency Financial Fraud (Focusing on Fraud-Specific Incentives)

3.1 Technical Level

The "decentralization, anonymity" characteristics of blockchain provide inherent convenience for fraud: criminal actors can transfer funds through anonymous wallets to avoid identity tracking; they can use the "immutable" characteristic of blockchain to forge transaction records, enhancing the credibility of the scam and lowering victims' vigilance.

3.2 Economic Level

The dual attributes of the digital currency market - "high speculation + regulatory gaps" - induce crime: some members of the public, driven by a "get-rich-quick" mentality, overlook investment risks, providing a large target group for high-yield fraud; the lack of clear regulatory rules allows illegal trading platforms and false ICOs to persist, resulting in low crime costs and high benefits. According to a 2023 Report by cryptocurrency tracking company [2] Chainalysis, global digital currency fraud revenue reached $5.9 billion that year.

3.3 Legal Level

The current Criminal Law's regulation of financial fraud contains ambiguities: the distinction criteria between the "crime of fraud" and the "crime of fund-raising fraud" are unclear, leading to difficulties in qualitative assessment by judicial organs; the lack of uniform legal basis for calculating the value of virtual currency and tracing transaction records makes it difficult to establish a solid evidence chain, posing obstacles to case handling.

3.4 Social Level

Referring to related research in [1] Shi Xiuxia's "Research on Money Laundering Crimes Using Virtual Currency", the public holds cognitive biases regarding "blockchain + digital currency": most investors confuse "legal digital

ISSN 2959-6130

currency (e.g., central bank digital currency) with illegal virtual currency", and lack sufficient understanding that "blockchain technology ≠ guaranteed principal and returns", making them easily misled by false propaganda. Meanwhile, the characteristics of decentralized virtual currency make it a 持续 favored tool for crimes like fraud and illegal fundraising, and compared to traditional payment methods, pose greater regulatory challenges.

4. Problems and Deficiencies in China's Current Criminal Law's Response to Digital Currency Financial Fraud

4.1 Confused Application of Charges

Comparative case analysis reveals the phenomenon of "different charges for similar cases":

• Case 1: In the case of Xiong et al. involved in fund-raising fraud, Xiong and others developed trading software, created their own virtual currency "CGC Coin", attracted investment through false propaganda and price manipulation, then suppressed the coin price to zero, illegally obtaining over 15 million Tether coins (worth approximately 100-108 million RMB). The Guangdong Provincial High People's Court finally determined their actions constituted the crime of fund-raising fraud.

• Case 2: In the cross-border fraud case of Yu et al., Yu, under the guise of a "London Gold" trading broker, established operations overseas, channeling victims to virtual futures investment platforms to commit fraud, involving 280 million RMB. In September 2024, the Yantai Intermediate Court sentenced the principal offender Yu to life imprisonment in the first instance for the crime of fraud.

Similar digital currency fraud cases suffer from unclear qualitative standards, leading to discrepancies in charge application and affecting judicial credibility [6].

4.2 Difficulties in Evidence Identification

The dilemma in evidence identification is mainly reflected in two aspects:

• Lack of Uniform Standard for Virtual Currency Value Calculation: In judicial practice, calculations are based either on the "average exchange price at the time of the crime" or the "victims' actual deposit amount", leading to significant differences in the determination of the amount of crime.

• Obstacles in Tracing Blockchain Transaction Records: Some overseas exchanges (e.g., Binance) do not cooperate with domestic judicial authorities in providing user data, resulting in an inability to fully track fund flows and a broken evidence chain.

5. Foreign Criminal Law Systems and Experience in Responding to Digital Currency Financial Fraud

5.1 Legal Regulation in the United States

The New York State Department of Financial Services took the lead in June 2015 by passing regulations specifically governing virtual currency, implementing a licensing system for virtual currency business activity: those without a license cannot engage in virtual currency business activity (with specific exemptions). So-called "virtual currency business activity" includes: receiving currency for transmitting virtual currency (with specific exemptions), storing/holding/custodialing/controlling virtual currency on behalf of others, buying/selling virtual currency, providing virtual currency exchange services, controlling/administering/issuing virtual currency, etc. (developing and disseminating software itself does not constitute such activity).

Licensed entities must undertake anti-money laundering obligations: establish anti-money laundering mechanisms, maintain transaction records, report large and suspicious transactions, prohibit transfers that hide customer identity, identify customers, block illegal transactions, comply with supervision, etc.

Furthermore, the U.S. SEC (Securities and Exchange Commission) identifies "false ICOs" as illegal securities offerings. For actions involving "raising funds from the public + promising returns", it prioritizes the application of the Anti-Securities Fraud Law to pursue criminal responsibility (similar to China's crime of fund-raising fraud). It also requires overseas exchanges to provide user data to U.S. judicial authorities, solving the problem of evidence tracing.

5.2 Experience Refinement

The core insight from foreign responses to digital currency financial fraud is "clarifying charge application standards + improving evidence rules + linking regulation and criminal law", rather than simply increasing punishment severity. By refining the scenarios for charge application, establishing uniform evidence identification standards, and strengthening regulatory pre-conditions and judicial cooperation, a whole-chain governance system is formed to effectively curb the spread of crime.

6. Conclusion

As a new type of crime in the digital economy era, non-legal digital currency financial fraud, with its characteristics of "high-tech nature" relying on blockchain technology, "concealment" utilizing anonymity, and "scale" formed

through hierarchical diffusion, poses a serious threat to public property security and challenges the traditional criminal law regulatory system and financial supervision models.

Through empirical analysis of typical cases like "Plus-Token" and "Stellar Coin", this paper has clarified the three core types of such fraud: "false ICO", "fake trading platform", and "pyramid-scheme-style referral". It has analyzed the incentives for crime across four dimensions: technology, economy, law, and society, and pointed out the practical difficulties in charge application and evidence identification under China's current Criminal Law. By drawing lessons from the U.S. experience of "charge refinement + regulatory pre-conditions", it provides theoretical and practical references for responding to this type of crime.

However, the governance of non-legal digital currency financial fraud is not solely a legal issue; its essence lies in the dynamic balance between technological innovation and institutional regulation, market speculation and risk prevention/control. Only through the continuous deepening of theoretical research, the constant improvement of the legal system, and the coordinated efforts of social governance can the spread of non-legal digital currency financial fraud be effectively contained, building a solid security barrier for the healthy development of the digital economy.

References

[1] Shi Xiuxia. Research on Money Laundering Crimes Using Virtual Currency.

[2] Chainalysis. (2023). 2023 Global Crypto Fraud Report.

[3] Xie Yizhang. (2021). Financial Risks and Criminal Law Regulation of Digital Currency. China Legal Science, (4), 185-203.

[4] Wang Ying. (2022). Transnational Governance of Blockchain Financial Crime. Beijing: Law Press.

[5] Li Xin, & Zhang Weidong. (2020). Research on the Dissemination Models and Governance Paths of Online Financial Crime. Chinese Journal of Law, 42(2), 167-185.

[6] Zhang Mingkai. (2019). The Boundary and Concurrence Between Illegal Fundraising and Financial Fraud. Peking University Law Journal, 31(5), 1145-1163.