International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 5, Sep-Oct 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Study of Cryptocurrency Crime Governance in the United States and China's Regulatory Path

Yang Yuqi, Wu Tianlong, Zhang Han, Xie Bowen

School of Law, School of Economics, and School of Information, Beijing Wuzi University, Beijing, China

ABSTRACT

This paper first outlines the background and research significance of Cryptocurrency Crime. It then proceeds to analyze various types of such crimes and illustrates their main forms and the Law Enforcement situation in the United States using specific case studies. The paper further examines the challenges confronting the United States across technology, law, Law Enforcement, and International Cooperation, subsequently outlining its primary response strategies. Finally, recommendations are proposed for China, focusing on four key areas: Regulatory Framework, Judicial Practice, Technical Means, and International Cooperation. The paper concludes by anticipating future directions for Cryptocurrency Crime Governance.

KEYWORDS: *Cryptocurrency Crime, Legal Regulation, United States, China.*

How to cite this paper: Yang Yuqi | Wu Tianlong | Zhang Han | Xie Bowen "A Study of Cryptocurrency Crime Governance in the United States and China's Regulatory Path" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-5, October 2025, pp.217-222, URL: www.ijtsrd.com/papers/ijtsrd97433.pdf

IJTSRD97433

I. INTRODUCTION

The rise of Blockchain and cryptocurrencies, while reshaping the global financial system, has simultaneously provided new tools and avenues for criminal activities. As the world's largest cryptocurrency market and financial center, the United States has emerged as the core of the global Cryptocurrency Ecosystem. This is due to its substantial number of holders, the largest Trading Platforms, the most active Startup Clusters, and the most influential Institutional Investors. Consequently, it functions as both the primary beneficiary of innovation and a significant victim and force in combating crime. Driven by technological evolution, Criminal Patterns have become increasingly professionalized, sophisticated, and globalized. Historically, examples included "Silk Road" Dark Web drug trading, whereas more recent years have seen the emergence of Flash Loan Attacks, Ransomware, and "Pump and Dump" schemes.

This paper systematically investigates the forms, characteristics, and Governance Challenges associated with Cryptocurrency Crime in the United States, utilizing it as a case study to derive applicable lessons for China. The core questions addressed include: What are the primary forms of Cryptocurrency Crime in the United States? What are their Operating Models and characteristics? What Structural Challenges do the existing laws and Regulatory System confront? What Law Enforcement Strategy and Technological Innovation have been adopted by the United States to address these issues? What are the effectiveness and limitations of these measures? How can China draw lessons from these findings and construct its own Regulatory Framework?

II. Theoretical Framework and Typology Development for Cryptocurrency Crime

Before an in-depth analysis of specific cases, a clear theoretical framework needs to be constructed to systematically classify the complex and diverse Cryptocurrency Crime activities. Drawing upon theories from criminology and financial law, and based on the core role cryptocurrency plays in criminal activities, these activities can be categorized into the following three types:

Table I: Cryptocurrency Crime Typology

Crime Type	Key Characteristic	Main Forms	Typical Cases Crime Object
Crime object	Targets cryptocurrencies themselves	Exchange hacks, fraud, private key theft	Coincheck hack incident, FTX collapse
Criminal Tools	Uses cryptocurrencies for payments and value transfers	Money laundering, Ransomware, Dark Web transactions, evasion of sanctions	Colonial Pipeline ransomware case, BitMEX money laundering case
Market Order Disruption	Undermines the fairness of the cryptocurrency market	Market manipulation, fraudulent issuance, DeFi vulnerability exploitation	Ripple securities violation case, Twitter hack incident

This typology offers a clear analytical framework for the subsequent analysis of specific U.S. cases and facilitates a comprehensive understanding of the multifaceted nature of Cryptocurrency Crime.

III. Typical Forms and Case Analysis of Cryptocurrency Crime in the United States

A substantial number of representative Cryptocurrency Crime cases have been addressed by the United States Law Enforcement and Regulatory Authorities, encompassing all the aforementioned categories. These cases illustrate not only the specific methods employed in these crimes but also the response strategies and their effectiveness within the United States Law Enforcement system.

A. Exchanges as Targets of Crime: Hacking and Massive Theft

Coincheck Hacking Incident (2018) and FTX Implosion (2022): Although Coincheck was a Japanese exchange, the incident sent shockwaves globally and prompted U.S. regulators to intensify scrutiny. More than $530 million worth of NEM tokens were stolen by hackers. This case exposed the substantial risks associated with exchanges storing large quantities of assets in hot wallets. More directly relevant to the U.S. context is the collapse of FTX. Although its direct causes included the misappropriation of client funds and failures in corporate governance, at its core, it represented an unprecedented act of fraud and theft targeting user assets. SBF, the founder, and his associates transferred billions of dollars in client assets held in custody to Alameda Research, an affiliated trading firm, for high-risk speculation, ultimately resulting in losses estimated at tens of billions of dollars. The enormous destructive power of insider misconduct within centralized exchanges was underscored by the conviction of SBF in a case jointly investigated by the US Department of Justice, the SEC, and the CFTC.

B. Case Study: Criminal Instrumentalities – Money Laundering in the BitMEX Case (2020)

As one of the world's largest cryptocurrency derivatives exchanges, BitMEX was jointly sued by the U.S. Commodity Futures Trading Commission (CFTC) and the Department of Justice for failing to implement anti-money laundering (AML) and "Know-Your-Customer" (KYC) procedures required by the Bank Secrecy Act (BSA). The platform's anonymous trading features were exploited as instruments for money laundering and sanctions evasion. As a result, BitMEX ultimately paid a USD 100 million fine to reach a settlement, and one of its co-founders pleaded guilty. This case established the principle of U.S. jurisdiction, applying the BSA to offshore cryptocurrency exchanges, and strengthened the regulatory red line for platform compliance obligations.

C. Disruption of Market Order: Fraudulent Issuance—SEC v. Ripple (2020 to present)

The U.S. Securities and Exchange Commission (SEC) sued Ripple Labs Inc. and its executives, alleging they conducted an unregistered securities offering worth US$1.3 billion through the sale of XRP tokens. The core legal dispute of this case centered on whether XRP should be classified as a "security." The SEC cited the "Howey Test," arguing that investors invested in a common enterprise with an expectation of profit derived from Ripple's efforts. The protracted legal battle, spanning four and a half years, ultimately concluded with a victory for Ripple. This victory was not only a milestone for Ripple but also a landmark event for the U.S. crypto industry in its challenge to the SEC's regulatory authority.

IV. Core Challenges of Governance Cryptocurrency Crime in the United States

Despite a series of Law Enforcement victories achieved by the United States, its Governance system continues to confront numerous Structural Challenges, which in turn offer crucial insights into the complexities of Cryptocurrency Crime.

A. Technical Challenges: The Paradox of Anonymity and Pseudo-Anonymity

Cryptocurrencies like Bitcoin are pseudo-anonymous. All transactions are publicly traceable on the Blockchain, but the identity of the owner behind the address remains concealed. This presents the initial obstacle for investigations. Criminals utilize mixers, privacy coins, cross-chain bridges, and rapid transfers between multiple exchanges to complicate tracing efforts. While on-chain analysis companies like Chainalysis and Elliptic are continually advancing their technological capabilities, this remains a technological arms race, and Law Enforcement agencies must therefore continually invest resources to maintain their lead. In its 2020 publication, 'Cryptocurrencies: Enforcement Framework', the United States Department of Justice specifically mentioned that the use of privacy coins such as Zcash, Monero, and DASH may indicate criminal activity.

B. Legal and Regulatory Challenges: Ambiguous Jurisdiction and Overlapping Responsibilities

1. Regulatory Authority Disputes

A major challenge for the United States is the absence of a unified federal cryptocurrency Regulatory Framework. While the SEC considers most cryptocurrencies to be "securities" and thus subject to its jurisdiction, the CFTC, conversely, views them as "commodities," with their futures and derivatives markets falling under its purview. Additionally, the Financial Crimes Law Enforcement Network, operating under the Department of the Treasury, regulates these assets from the perspective of payments and anti-money laundering. This fragmented regulatory model leads to overlapping responsibilities and inconsistent rules, which in turn imposes high compliance costs on businesses and creates loopholes that allow certain criminal activities to go unchecked within a regulatory vacuum.

2. Jurisdictional Conflicts

The cross-border nature of cryptocurrencies makes determining jurisdiction exceptionally complex. Does a US court possess jurisdiction over the fraudulent activities of an exchange that operates in the US, is registered in Seychelles, has servers in Lithuania, and targets European users? Differences in legal systems across countries provide criminals with room for "regulatory arbitrage." The US Department of Justice asserts jurisdiction in its framework over individuals who conduct cryptocurrency transactions involving US servers; however, the international recognition of this claim remains questionable.

C. Law enforcement capability challenges: shortage of professional talent and technical tools

Cryptocurrency investigations necessitate professionals with interdisciplinary expertise, including finance, law, Blockchain technology, cybersecurity, and data analysis. These professionals command extremely high compensation in the private sector, resulting in a severe talent drain within law enforcement agencies. Although the U.S. Department of Justice has established the National Cryptocurrency Enforcement Team and the FBI maintains a specialized cryptocurrency unit, their personnel numbers and budgets remain insufficient to counter the scale of criminal profits. U.S. Attorney General William Barr also acknowledged, "Ensuring that the use of this technology is secure, and does not jeopardize our public safety or national security, is critical to the United States and its allies."

D. International Cooperation Challenges

Cryptocurrency Crime is inherently global, and unilateral actions are often insufficient. Effective efforts to combat such crime rely on close international judicial cooperation, including intelligence sharing, joint investigations, evidence exchange, and the extradition of criminals. However, discrepancies among countries in cryptocurrency legislation, regulatory approaches, and Law Enforcement priorities pose significant obstacles to International Cooperation. For example, the strict regulatory stance of the United States towards privacy coins contrasts with the relatively lenient policies of some European countries, and this regulatory asymmetry can be exploited by criminals. critical to the United States and its allies."

V. The United States' Response Strategies

Facing these challenges, the United States has progressively formulated a set of technology-driven response strategies, distinguished by an all-of-government coordinated approach. These strategies largely represent the cutting edge of global Cryptocurrency Crime Governance.

A. All-of-Government Law Enforcement Strategy (All-of-Government Approach)

The United States has shifted from relying on individual agencies operating independently to emphasizing inter-agency coordination. This approach is exemplified by cases such as FTX and BitMEX, where the DOJ, SEC, and CFTC collaborated, simultaneously addressing issues at criminal, civil, and regulatory levels to generate a robust, unified enforcement impact. Furthermore, the Department of the Treasury, through FinCEN, develops anti-money laundering regulations. Concurrently, its Office of Foreign Assets Control (OFAC) designates mixer

addresses and criminal organization wallet addresses for inclusion on the SDN list, thereby prohibiting U.S. entities from engaging in transactions with them and imposing financial sanctions.Of the 32 cryptocurrency-related bills introduced by Congress in 2020, 12 were specifically aimed at curbing the use of digital currencies to facilitate illicit activities, including money laundering, terrorism, and human trafficking.

B. Technology Empowerment: Regulatory Technology (RegTech) and On-chain Analysis

US law enforcement agencies are actively acquiring and deploying on-chain analysis tools. For instance, the IRS and FBI have entered into significant contracts with Chainalysis to train their agents. The recovery of the Colonial Pipeline ransom serves as a prime example of technology-enabled law enforcement. In the future, artificial intelligence and machine learning will be more extensively applied to identify anomalous transaction patterns and for predictive policing, enabling early warnings before crimes take place. The 83-page document, "Cryptocurrencies: Enforcement Framework," released by the US Department of Justice, also provides a detailed overview of both the legitimate and illicit uses of cryptocurrencies, along with corresponding regulatory strategies.

C. Regulatory Clarification and Legislative Advancement

Despite the slow progress, the United States is actively working to clarify its regulatory landscape.Through enforcement actions, the SEC and CFTC have sought to delineate legal boundaries by setting precedents. Concurrently, bipartisan members of Congress have also proposed several comprehensive cryptocurrency regulatory bills, aiming to legislatively clarify asset classification, supervisory responsibilities, and consumer protection standards. Although these bills have not yet been passed, they signify positive legislative momentum.

D. Strengthening Public-Private Partnerships (PPP)

The U.S. government acknowledges that it cannot address these challenges in isolation. It actively establishes information-sharing mechanisms with centralized exchanges, on-chain analytics firms, and academic research institutions. Exchanges are required to submit suspicious activity reports, analytics firms provide technical support and training to Law Enforcement agencies, and academia offers cutting-edge research. This public-private collaboration is key to enhancing overall Governance effectiveness. The U.S. Department of Justice explicitly stated in its report: "To promote public safety and protect national security, all stakeholders—including private sector entities, regulators, elected officials, and individual cryptocurrency users—must take steps to ensure that cryptocurrencies are not used as illicit platforms."

Table II: Key U.S. Cryptocurrency Crime Governance Strategies and Effects

Response Strategy	Specific Measures	Representative Cases/Documents	Implementation Effect
Whole-of-Government Law Enforcement	Multi-agency joint investigation and prosecution	BitMEX case, FTX case	Coordinated Law Enforcement efforts are established, enhancing deterrence
Technology Empowerment	On-chain analysis tools, AI prediction	Colonial Pipeline Ransom Recovery	Investigative efficiency is improved, and fund tracing is achieved
Regulatory Clarity	Law Enforcement defining boundaries, legislative advancement	SEC v. Ripple case, multiple regulatory bills	Regulatory boundaries are progressively clarified, reducing grey areas
Public-Private Partnership	Information sharing, technical cooperation	FinCEN requiring exchanges to submit SARs	Societal resources are integrated, thereby enhancing overall Governance capabilities

VI. China's Lessons Learned and Legal Regulation Recommendations

As a major global digital economy power, China similarly faces severe challenges posed by Cryptocurrency Crime. Drawing upon U.S. experience and China's specific circumstances, targeted recommendations are presented across four key areas: Regulatory Framework, Judicial Practice, Technical Means, and International Cooperation.

A. Constructing a Classified Regulatory Framework and Clarifying Regulatory Responsibilities

China can draw lessons from the U.S. "classified regulation" approach, but must avoid the problem of ambiguous responsibilities stemming from its "multi-headed regulation." It is recommended that the Anti-Money Laundering Law of the People's Republic of China be amended to include regulatory provisions concerning money laundering involving digital cryptocurrencies. Furthermore, the central bank's role

as the primary regulatory body should be clarified, and a dedicated cryptocurrency regulatory coordination institution ought to be established. Drawing on the regulatory models of Singapore and Japan, China could establish a classification Regulatory System based on cryptocurrency functions, which would involve the categorization of cryptocurrencies into payment tokens, security tokens, and utility tokens, with corresponding regulatory rules then applied to each.

Specifically, payment tokens could be integrated into the Central Bank Digital Currency Regulatory Framework, necessitating trading platforms to implement stringent KYC and AML measures. Security tokens could be overseen by the CSRC, and would be subject to the relevant provisions of the Securities Law. Utility tokens, conversely, might be managed under a registration-based system, primarily to mitigate the risks of illegal fundraising. This differentiated regulatory model would not only prevent regulatory gaps but also avoid unduly stifling innovation.

B. Improve the criminal legal system to adapt to the characteristics of digital crime

The "Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Criminal Cases Involving Concealment or Disguise of Criminal Proceeds and Their Benefits" (Fa Shi [2025] No. 13), which came into effect in China on August 26, 2025, marks a significant stride. It specifically brings acts of concealing or disguising criminal proceeds carried out using virtual currency within the scope of regulation. Next steps to consider:

Firstly, the scope of predicate offenses for money laundering should be broadened. Currently, predicate offenses for money laundering in China are limited to seven specific categories of crimes. It is recommended that this scope be expanded to include all major criminal activities, thereby increasing the legal costs for those who use cryptocurrencies for money laundering.

Secondly, the criteria for establishing subjective knowledge should be refined. Drawing upon US experience, a comprehensive approach to determination could be adopted, focusing on the perpetrator's deliberate attempts to sever the link between funds and identity, actions that are clearly inconsistent with normal investment practices, and the intentional exploitation of the borderless nature of virtual currencies.

Thirdly, differentiated thresholds for criminalization should be established. Drawing inspiration from the two-tiered criminalization standards set forth in China's new judicial interpretation for the offense of concealing or disguising criminal proceeds, small-amount, high-frequency money laundering activities conducted using cryptocurrencies, even if they do not meet the threshold for criminal prosecution, could be subject to administrative penalties. This approach would create a dual Governance structure that integrates administrative and criminal enforcement.

C. Develop Regulatory Technology to Enhance Law Enforcement Capabilities

China should make substantial investments in regulatory technology development to enhance the on-chain analysis capabilities of its law enforcement authorities:

Firstly, independently controllable Blockchain analysis tools should be developed, and a nationwide cryptocurrency transaction monitoring platform should be established to facilitate real-time monitoring of key transaction venues and wallet addresses.

Secondly, artificial intelligence and machine learning technologies should be introduced to automatically identify abnormal transaction patterns and predict potential criminal activities. The on-chain tracing capabilities demonstrated by the United States in the Colonial Pipeline case serve as a valuable model for China.

Thirdly, talent development within law enforcement agencies should be strengthened, and specialized cryptocurrency investigation units should be established. This initiative aims to cultivate interdisciplinary professionals proficient in technology, law, and finance. The experience of the U.S. Department of Justice in establishing the National Cryptocurrency Enforcement Team can serve as a valuable reference.

The successful cracking of a USDT money laundering case by Hunan Yueyang police in 2025 demonstrates that Chinese law enforcement authorities have already developed the capability to investigate and address significant Cryptocurrency Crime. Moving forward, the investigative experience gained from such cases should be further disseminated, and the professional competence of grassroots law enforcement personnel should be enhanced.

D. Strengthen International Collaboration and Participate in Global Governance

The transnational nature of Cryptocurrency Crime underscores the imperative for China to enhance International Cooperation.

On the one hand, this entails actively participating in the formulation of international rules, promoting the establishment of unified cryptocurrency regulatory standards under the framework of international organizations such as FATF, and enhancing intelligence sharing and Law Enforcement collaboration.

On the other hand, bilateral cooperation mechanisms should be established with key countries, especially with cryptocurrency-active nations like the United States, Japan, and Singapore, to create 'green lanes' for joint investigations, evidence exchange, and the extradition of criminals.

Notably, China has already attained a global leadership position in the digital currency domain, with the research, development, and pilot programs of the digital RMB offering valuable experience for central bank digital currencies worldwide. In the future, the controllable anonymity features of the digital RMB could be explored to provide necessary interfaces for regulation while protecting user privacy. This approach could offer a Chinese solution for combating Cryptocurrency Crime.

VII. Conclusion

The analysis of cryptocurrency crime types, cases, and governance strategies in the United States reveals its multifaceted nature and the significant challenges in its governance. While the U.S. has, to a certain extent, curbed the spread of cryptocurrency crime through strategies such as "whole-of-government" Law Enforcement, technological empowerment, regulatory clarity, and public-private partnerships, the technological, legal, Law Enforcement, and International Cooperation challenges it faces remain severe.

For China, the lessons learned from the U.S. provide valuable insights: it must both avoid the issues of U.S.-style regulatory fragmentation and fully leverage its advanced experience in technology-driven Law Enforcement. China should develop a differentiated Regulatory Framework, improve its criminal legal system, advance regulatory technology, and strengthen international cooperation to establish a Cryptocurrency Crime Governance system tailored to China's national conditions.

Future research could focus on the following areas: First, the criminal risks and regulatory countermeasures in emerging areas like Decentralized Finance (DeFi); Second, the potential and limitations of Central Bank Digital Currency (CBDC) in preventing Cryptocurrency Crime; and Third, the challenges posed by AI-generated crime (e.g., leveraging AI to identify vulnerabilities in smart contracts) to existing legal frameworks. Only through continuous institutional innovation and technological empowerment can Cryptocurrency Crime be effectively curbed, while simultaneously fostering financial innovation and safeguarding national financial security and social stability.

References

[1] Mou Ruijun, "A Discussion on Virtual Currency Crimes – Centered on the 2024 CALIFORNIA CRYPTO CONFERENCE (Part 1)", *Legal Affairs Communication*, No. 3211, May 31, 2024.

[2] Li Lanying, "Risk Analysis of Virtual Currency Crimes and Governance Strategies", *Journal of Guizhou Provincial Party School*, 2021, No. 2.

[3] Lin Haizhen (Second Prosecutorial Department, Ruian City People's Procuratorate, Zhejiang Province), "Criminal Law Regulation of Illegal Cryptocurrency Transfers", *China Prosecutor*, 2021, No. 18.

[4] U. S. Department of Justice (DOJ), "Cryptocurrencies: Enforcement Framework", 2022.

[5] U. S. Financial Crimes Enforcement Network (FinCEN), Proposed Anti-Money Laundering Rule Changes for Virtual Asset Service Providers (VASP) (NPRM), 2020.

[6] Financial Action Task Force on Anti-Money Laundering (FATF), *Revised FATF Standards 12-Month Review for Virtual Assets and Virtual Asset Service Providers*, June 2020.

[7] Supreme People's Court, Supreme People's Procuratorate, *Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Concealing or Disguising Proceeds of Crime* (Fa Shi [2025] No. 13), effective on August 26, 2025.

[8] Cipher Trace, *2020 Cryptocurrency Crime and Anti-Money Laundering Report*, February 2021.

[9] Chainalysis, *2024 Cryptocurrency Crime Report*

[10] Hu Yunteng, Editor-in-Chief; Zhou Zhenjie, Lai Zaoxing, Associate Editors-in-Chief, *The Legal Regulation of Cryptocurrencies*, Law Press, March 2025.