

ON A MULTIDIMENSIONAL FRAMEWORK FOR CROSS-BORDER CYBERCRIME ASSET RECOVERY IN THE DIGITAL ERA

*Sun Pengqing**

I. INTRODUCTION

In the digital era, the state-centric legal frameworks, which were designed to recover illicit assets through physical borders and centralized banking, now face a challenge of enforcement efficacy. The weak territorial character of cyberspace, while facilitating the globalization of crime, has also profoundly challenged the system of extraterritorial jurisdiction in criminal justice based on territorial boundaries. This is most evident in the overall capacity of authorities to combat crime, the lack of legitimacy in extraterritorial criminal justice activities leading to defects in evidentiary admissibility, and the differentiated application of laws resulting from jurisdictional constraints. In the context of cybercrime, cryptocurrencies play a key role in contemporary cybercrime. Due to their rapid transaction speed, strong anonymity, and ease of cross-border transfer, they can be the subject matter of crime and widely utilized tools to facilitate illicit activities.¹ However, given their decentralized nature, anonymity, and cross-border characteristics, traditional asset recovery mechanisms, which rely on geographic jurisdictions and banking systems, now face significant challenges.² Consequently, the recovery of criminal assets remains at a low rate and has poor effectiveness all over the world. China also confronts escalating cybercrime threats,³ arising from barriers in international judicial cooperation and the inherent characteristics of digital assets, especially in terms of cross-border digital asset recovery. It is crucial to propose a feasible

* Researcher at the China Institute for Judicial Studies of Tsinghua University and the Judicial Case Research Base of the Supreme People's Procuratorate, and Ph.D. Candidate at Tsinghua University. This paper is supported by the Major Project of the National Social Science Fund of China entitled *Theoretical Foundations and Implementation Plan for Building the Socialist Rule of Law System with Chinese Characteristics* (23ZDA073) and the National Social Science Fund of China entitled *Research on the Theory and Practice of International Criminal Judicial Assistance in Combating Cybercrime* (19BFX073).

1 INTERPOL, MORE THAN 300 ARRESTS AS AFRICAN COUNTRIES CLAMP DOWN ON CYBER THREATS, at <https://www.interpol.int/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats> (Last visited on October 27, 2025).

2 See Hu Ming, *On the Disposal of Virtual Currency Involved in Criminal Cases*, 6 *Modern Law Science* 102 (2024).

3 SUPREME PEOPLE'S PROCURATORATE OF THE PEOPLE'S REPUBLIC OF CHINA, CYBERSPACE GOVERNANCE, at <https://en.spp.gov.cn/cyberspacegovernance.html> (Last visited on October 24, 2025).

asset recovery framework for China in the digital era.⁴

Asset recovery involves tracking, seizing, and mandatorily surrendering assets, etc. In criminal law, recovery refers to the detection, tracing, and seizure measures taken to deprive offenders of proceeds obtained from the commission of any crime. According to article 64 of *China's Criminal Law*, there are three main situations regarding criminal proceeds: recovery or restitution, return, and confiscation.⁵ Currently, there are two principal methods for asset recovery: direct recovery of assets and international cooperation mechanisms for confiscation and recovery. These methods differ in initiation mechanisms: direct recovery of assets occurs upon request by victims, whereas international confiscation and recovery rely on cooperative international mechanisms. Various international treaties and Chinese domestic laws have stipulated asset recovery for cross-border cybercrime to varying extents. These regulations collectively establish the normative framework and main institutional elements for asset recovery in the digital era. China actively engages in multilateral and bilateral international cooperation against transnational crimes, including cybercrime and associated asset recovery. Relevant international legal framework primarily includes the *United Nations Convention Against Transnational Organized Crime*, the *United Nations Convention Against Corruption*, a series of bilateral judicial assistance treaties, and the recently adopted *United Nations Convention Against Cybercrime* (UNCC). On October 25-26, 2025, China, together with 70 other countries and regions, signed the UNCC, the first international convention in the cyber domain negotiated under the auspices of the United Nations. It includes detailed provisions on asset recovery. The domestic legal framework for cybercrime asset recovery mainly comprises the *Criminal Law*, the *Criminal Procedure Law*, the *Law on International Criminal Judicial Assistance*, and relevant judicial interpretations and departmental regulations. These laws and regulations govern procedural measures and substantive dispositions regarding seizure, freezing, confiscation, and return of the involved assets.

Asset recovery is crucial for depriving offenders of unlawful profits,

4 Notably, assets discussed herein refer to any property obtained through criminal conduct (directly or indirectly). Cyber assets include any physical or software defined components, such as devices, networks, data, applications, and user accounts. Additionally, in this paper, the object of asset recovery refers to virtual digital assets.

5 Article 64 of the *Criminal Law of the People's Republic of China*: 'All property illegally obtained by an offender shall be recovered, or the offender shall be ordered to return it or pay compensation for it. The lawful property of victims shall be returned without delay. Contraband and the offender's personal property which has been used for the commission of a crime shall be confiscated. All confiscated property and fines shall be turned over to the State Treasury and shall not be misappropriated or be dealt with without authorization.'

detering crime, compensating victims, and preventing criminal proceeds from being used for illegal activities. Thus, more comprehensive crime governance can be achieved by targeting asset recovery of both direct and indirect proceeds. The international community is collaboratively enhancing asset recovery capabilities and increasingly addressing key issues related to digital assets, including cryptocurrencies. The UNCC acknowledges the role of ‘virtual currencies’ in asset recovery. In the process of confiscation and restitution, if the value of intercepted virtual currency substantially exceeds the amount of illicit proceeds, the UNCC requires that only the equivalent portion be confiscated and returned, rather than the entirety. Given that cybercrime and related money laundering offenses frequently involve virtual currencies, determining their legal characterization and establishing clear rules for their disposition remain pressing challenges for the future.⁶ In fact, specialized research on digital asset recovery specific to China’s cross-border cybercrime remains relatively scarce.⁷ Internationally, although global research has been conducted on cybercrime, there are limited studies specifically targeting China, despite its significant role in the global economy and notable presence of cybercrime.

Domestic studies tend to focus on three aspects. The first concerns specific institutional arrangements, such as studies on asset-sharing mechanisms.⁸ The second focuses on international cooperation in asset recovery, for instance the interaction between China’s criminal confiscation system and asset recovery efforts.⁹ The third examines concrete rules of asset recovery, including methods for calculating the amount to be recovered.¹⁰ However, researchers have observed that a particular policy trend lies in improving the handling of criminal assets as a means to strengthen crime control. This discussion primarily encompasses three key dimensions:

6 See Shao Cong, *The United Nations Convention Against Cybercrime and Coordinated Advancement of Cross-Border Investigation*, 2 China Criminal Law Magazine 143, 153 (2025).

7 As of July 2025, a keyword search on the China National Knowledge Infrastructure (CNKI) for ‘cross-border cybercrime asset recovery’ reveals no literature directly on point. Broadening the search to simply ‘asset recovery’ yields fewer than ten representative journal articles, with the majority of results being graduate theses and dissertations. See Luo Qiaoyu, *Cybercrime as an Industry: Examining the Organizational Structure of Chinese Cybercrime*, 11(1) Humanities and Social Sciences Communications 1 (2024).

8 See Li Haiying, *A Practical Choice for Asset Recovery in Corruption Crimes: The Construction of an Asset Sharing Mechanism*, 7 Social Science Front 229 (2017); Mei Chuanqiang & Shi Xin, *On the Construction of the International Sharing Mechanism of Drug Crimes Forfeited Assets in China*, 4 Jilin University Journal of Humanities and Social Sciences 15 (2020); Jiang Xinmiao & Xie Zhizhao, *Research on Building a Legal Mechanism for Intercountry Recovery of Stolen Assets Sharing in China: Based on a Functional Perspective*, 3 Huxiang Law Review 132 (2023).

9 See Zhang Shijin, *Practical Considerations on International Legal Cooperation in Asset Recovery*, 28 Tribune of Political Science and Law 145 (2010).

10 See Huang Feng, *An Analysis of Value-Based Confiscation and Rules for Assessing Recoverable Assets*, 5 Journal of Comparative Law 1 (2015).

unilateral cross-border criminal proceedings, mutual legal assistance (MLA), and international conventions.¹¹ Accordingly, this paper discusses challenges and risks, systematically presents normative frameworks and institutional formations, and proposes strategies for the digital asset recovery pathway in China, aiming to establish an ideal comprehensive resolution framework for China and the global community.

II. MULTIDIMENSIONAL CHALLENGES IN ASSET RECOVERY OF CROSS-BORDER CYBERCRIME IN THE DIGITAL ERA

A. Ambiguous Legal Status and Difficulties in Handling Digital Assets

Various international documents, treaties, and conventions have defined assets, including the *United Nations Convention Against Transnational Organized Crime*, the *United Nations Convention Against Corruption*, and the UNCC. These conventions reveal that property refers to assets of any kind — tangible or intangible, movable or immovable, physical or non-physical, including virtual assets and legal documents evidencing ownership or interests in these assets. These conventions consistently define criminal proceeds as any property directly or indirectly derived or obtained through criminal activity. Criminal proceeds primarily arise from unlawful means, and such proceeds should be recovered to prevent anyone from benefiting from criminal activities and related conduct.¹² However, the evolution of laws and regulations often lags behind technological advances.¹³ As a result, existing legal concepts are inadequate to define the legitimacy of digital assets and transactions within existing legal and regulatory frameworks, creating exploitable grey areas. Traditional network assets are typically defined within organizations, while new digital assets are often outside conventional financial systems. The legislative classification of digital assets is subject to ambiguity regarding their designation as property, currency, securities, or otherwise. This ambiguity directly affects tracing, seizure, valuation, and return of such assets, as current laws were not designed for them. The value of digital assets is multidimensional and

11 See Huang Yong, *Diversified Approaches to Improving Procedures for the Disposal for Criminal Case-Related Property*, 7 *Journal of Law Application* 22, 34 (2025).

12 See Shi Yanan & Liu Wei, *Definition of Proceeds of Crime and Criminal Gains*, 2 *The Chinese Procurators* 36 (2007).

13 See Sun Chengcheng, *Construction of a New Legal Regulatory System in the Context of Digital Economy*, 1 *Administration Reform* 80 (2024).

intangible, creating distinct challenges to traditional valuation and recovery. The extreme volatility of cryptocurrencies further complicates reliable assessment. Effective asset recovery in the digital era, therefore, requires attention not only to the tokens themselves but also to their market context and associated legal rights.

Digital cryptocurrencies remain in a legal and regulatory grey zone and continue to face challenges to their legitimization.¹⁴ China has officially prohibited the circulation of virtual currencies and related financial activities, denying their legal tender status. Since 2013, regulations on virtual currencies have been progressively tightened. In 2021, 10 departments, including the People's Bank of China (PBOC), jointly issued the *Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation*, which comprehensively prohibits activities such as exchanges between legal tender and virtual currencies, inter-virtual currency transactions, central counterparties in trading, information intermediaries, pricing services, Initial Coin Offerings, and derivatives trading, classifying them as illegal financial activities. Services provided by offshore exchanges to domestic residents via the Internet are also deemed illegal. This regulatory approach significantly affects the handling of virtual currencies involved in criminal cases. Documents from the PBOC and other departments have previously classified Bitcoin as a specific virtual commodity. At the same time, some argue that the PBOC's classification of digital currency as a type of virtual commodity does not adequately capture its actual nature. They suggest that digital currency should be defined as a means of payment or transfer, and that virtual currencies should be classified as instruments of payment.¹⁵ Furthermore, article 127 of the *Civil Code of the People's Republic of China* provides that legal protection applies to data and online virtual property where specified by law. Judicial practice and academic research generally regard virtual currencies that possess value, scarcity, and controllability as legally protected virtual property or objects,¹⁶ thereby qualifying as subjects of crime or criminal proceeds and falling into the scope of criminal asset disposition.¹⁷ Many jurisdictions lack a clear definition or consistent handling for digital items as 'assets', posing fundamental obstacles

14 See Xie Ping & Shi Wuguang, *Research on Digital Cryptocurrencies: A Literature Review*, 1 *Journal of Financial Research* 1, 11 (2015).

15 See Fan Yunhui & Li Yaoxin, *Discussing the Legal Regulation of Digital Currencies with Bitcoin as an Example*, 7 *Journal of Law Application* 48 (2014).

16 See Qi Aimin & Zhang Zhe, *On the Concept and Legal Nature of Digital Currency*, 2 *Science of Law (Journal of Northwest University of Political Science and Law)* 80 (2021).

17 See Tian Linan, *On the Compulsory Disposal of Virtual Property Involved in Criminal Cases*, 5 *China Legal Science* 114 (2023).

to the application of traditional asset recovery mechanisms.¹⁸ A report from the Cambridge Centre for Alternative Finance emphasizes the need to situate ‘new’ digital assets within established legal concepts, noting that private law considerations lag behind practical developments.¹⁹ The nature of crypto-assets further complicates asset recovery. Suppose a cryptocurrency wallet is not explicitly recognized as legally ownable and transferable ‘property’ or ‘asset’ within a given jurisdiction, legal orders for its seizure or confiscation may become unenforceable. However, it is difficult for legislative measures and international cooperation to keep pace with the rapidly evolving cybercrime landscape, or to address the complexity and dynamism of modern cyber threats, which results in a persistent gap between regulatory action and criminal practice. Thus, it is crucial to develop a legal framework that takes into account social, technological, and environmental factors.

B. Technical Dilemmas and Widening Gap in Law Enforcement Capability

The anonymity, decentralization, and ease of cross-border transfer of digital assets pose significant challenges to asset recovery. Typical cryptocurrencies are associated with anonymity, making it difficult to link them to real-world identities. Through the use of mixing services, criminals tend to combine lawful and illicit cryptocurrency transactions, thereby creating considerable barriers to traditional law enforcement methods in identifying individuals through financial tracing.²⁰ The decentralized nature of blockchain technology enables criminals to operate effortlessly across borders, further complicating tracking and prosecution. Traditional seizure methods that rely on physical media for storing private keys are inadequate to fully control virtual currencies, as suspects may access and transfer private keys in various ways. Effective seizure requires obtaining and managing private keys to transfer involved virtual currencies to judicially designated wallet addresses, presenting technical difficulties and risks of non-cooperation from suspects. Additionally, virtual currencies on offshore platforms require reliance on international judicial assistance or technical investigative measures, significantly increasing the difficulty of asset recovery. Against

18 See Hu Ming, *supra* note 2.

19 See JASON G. ALLEN, MICHEL RAUCHS & APOLLINE BLANDIN ET AL., LEGAL AND REGULATORY CONSIDERATIONS FOR DIGITAL ASSETS, at <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf> (Last visited on October 19, 2025).

20 See Stephen Kingah, *Measures on Asset Recovery: Utility of a Multi-Actor Global Fund for Recovered Stolen Assets*, 6 World Bank Legal Review 457 (2015).

this backdrop, Decentralized Finance (DeFi) presents a notable example of the unique obstacles facing asset recovery in the digital era. The advent of Bitcoin and the subsequent development of blockchain technology inspired widespread enthusiasm for the application of decentralized systems to broader domains. In 2015, the launch of Ethereum, an open-source public blockchain platform equipped with smart contract functionality, gave rise to the concept of DeFi. DeFi refers to financial applications and services built on open blockchain networks (primarily Ethereum) that utilize smart contracts, operating independently of traditional intermediaries.²¹ Designed to be more open, transparent, efficient, and accessible, DeFi challenges traditional regulatory models that rely on intermediary institutions.²² In genuinely decentralized protocols, pinpointing accountability is difficult. Without intermediaries, traditional anti-money laundering/combating financing of terrorism methods become difficult to apply.²³ DeFi protocols eliminate centralized control points that are crucial for traditional financial regulations and asset recovery mechanisms, such as court orders to freeze accounts. This necessitates a paradigm shift in regulatory thinking, potentially redirecting towards regulatory oversight of code, developers, or access points. DeFi platforms operate without intermediaries, making it hard to monitor or regulate transactions. Transactions on DeFi platforms are generally irreversible. The absence of central authorities complicates the process of obtaining information, freezing assets, and enforcing legal order, as there is no single point of contact or control. The instant and low-cost international transfer of digital assets facilitates illegal fund flows. Criminals take advantage of regulatory gaps by utilizing exchanges and platforms that do not require verification. The speed and convenience of cross-border transfers constrain the capacity of law enforcement and asset recovery. Traditional asset recovery methods rely on locating and freezing bank accounts or other financial instruments in the possession of individuals or entities. The anonymity of digital assets severely complicates initial identification. Traditional jurisdictional frameworks are insufficient when decentralized assets exist globally without specific jurisdictional locations or intermediaries. In purely decentralized systems, the institutional cooperation typically provided by central financial

21 The concept of 'independent control' was proposed to identify non-DeFi protocols, categorizing true DeFi as 'critical infrastructure'. See Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, 2 *Journal of Financial Regulation* 215 (2025).

22 See Zhao Lei, *Legal Regulation on NFT: Starting with the Case of Fat Tiger Getting Vaccinated*, 11 *Journal of Law Application* 138, 149 (2023).

23 See RASIM OZCAN, *DECENTRALIZED FINANCE*, in *FINANCIAL ECOSYSTEM AND STRATEGY IN THE DIGITAL ERA: GLOBAL APPROACHES AND NEW OPPORTUNITIES*, at 57 (Springer International Publishing, 2021).

entities in traditional asset recovery is absent.²⁴ The irreversibility of many cryptocurrency transactions means that traditional banking mechanisms cannot easily reverse the transferred funds. The fundamental difference between digital asset ecosystems and conventional financial systems necessitates legal strategies, advanced technological tools, and international cooperative mechanisms that address their distinctive features.

Technically, several issues are worth considering. First, cryptocurrency price volatility complicates accurate valuation of crime quantification, restitution, or confiscation. Second, judicial authorities lack uniform and secure standards for virtual currency custody and the supporting technical infrastructure, thereby risking asset loss, theft, or depreciation. The challenges of disposal and return represent the most significant obstacles to asset management. Third, cybercriminals quickly adapt to new trends and technologies, employing increasingly innovative and sophisticated methods. The discussion around applying artificial intelligence (AI) and machine learning (ML) to darknet and cryptocurrency forensics highlights the need for law enforcement to advance its technological capability promptly.²⁵

C. Barriers to International Cooperation on Contested Digital Assets

1. National Legal Divergences and Procedural Barriers to Application. — Cross-border asset recovery efforts necessarily encounter the laws of other states, which often diverge from or even conflict with one another across jurisdictions. China's approach to handling involved assets and responding to international cooperation requests is strictly governed by the *Criminal Law*, the *Criminal Procedure Law*, and the *Law on International Criminal Judicial Assistance*, which emphasizes procedural standardization and national sovereignty. However, significant variations exist among national laws regarding asset ownership, fraud, foreign judgment enforcement, and data privacy. Legal discrepancies in cybercrime definition, evidence collection procedures, and asset confiscation procedures complicate global law enforcement operations. Regarding asset recovery, differences emerge in the freezing, seizure, and confiscation processes, notably in non-conviction-based

24 See UNITED NATIONS OFFICE ON DRUGS AND CRIME, INFLECTION POINT: GLOBAL IMPLICATIONS OF SCAM CENTRES, UNDERGROUND BANKING AND ILLICIT ONLINE MARKETPLACES IN SOUTHEAST ASIA, at https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf (Last visited on October 31, 2025).

25 See Ramy El-Kady, *Decoding the Dark: AI and ML in the Dark Web, Cybercrime, and Cryptocurrency Forensics*, International Cybersecurity Law Review 1 (2025).

asset forfeiture procedures and evidentiary standards.²⁶ Cross-border electronic evidence collection also encounters disparities in preservation, verification, and admissibility standards across jurisdictions. In cross-border cybercrime cases, significant differences exist among jurisdictions regarding how to ensure the legality of evidence obtained abroad and the integrity of electronic evidence.²⁷ This discrepancy can lead to electronic evidence legally obtained in one country facing challenges regarding evidentiary qualification or probative value in courts of another jurisdiction. Additionally, data protection regulations further complicate evidence collection. Laws such as *EU's General Data Protection Regulation* and *China's Cybersecurity Law*, *Data Security Law*, and *Personal Information Protection Law* set stringent conditions for the cross-border transfer of personal information and critical data. For instance, laws in China mandate security assessments by the Cyberspace Administration of China for transferring essential data abroad (data processed by critical information infrastructure operators or data exceeding certain thresholds). The transfer of personal data requires individual notification, explicit consent, personal information protection impact assessments, and compliance with security assessments, certifications, or standard contracts. Crucially, article 36 of the *Data Security Law* and article 41 of the *Personal Information Protection Law* explicitly prohibit domestic organizations or individuals from providing data/personal information stored within China to foreign judicial or law enforcement agencies without approval from Chinese authorities. These regulations have effectively safeguarded China's digital sovereignty, but they may also, at a normative level, constrain cross-border cooperation in asset recovery and reduce its efficiency. This tension necessitates regulatory adjustments to mitigate potential normative conflicts. Furthermore, current rules on criminal electronic evidence in China differ from those of the UNCC in areas including in data classification, investigative measures, and the scope of jurisdiction. These divergences may pose institutional obstacles to China's international cooperation in electronic evidence collection and criminal prosecution in cyberspace once the UNCC comes into force.

2. Institutional Inefficiency of Traditional MLA and the Gap in Rapid Information Exchange. — The main barrier to timely information sharing is not a lack of platforms, but insufficient legal channels, as well as the absence of mutual trust required to utilize existing platforms for sharing sensitive intelligence. Overreliance on MLA channels is inefficient. Existing reports

26 See Ari Wibowo, *Barriers and Solutions to Cross-Border Asset Recovery*, 26(4) *Journal of Money Laundering Control* 739 (2023).

27 See Feng Junwei, *The Adoption of Criminal Evidences Obtained Abroad*, 4 *China Legal Science* 247 (2015).

indicate that asset recovery through MLA faces practical and procedural hurdles, leading to prolonged delays.²⁸ Moreover, the bilateral treaties on MLA in criminal matters concluded by China are limited in number and uneven in quality.²⁹ Formal MLA procedures often take excessive time and are incompatible with the rapid transfer characteristics of cybercrime assets. Such crimes involve thousands of electronic data points requiring rapid analysis capabilities. The immense volume of data in cross-border cybercrime poses significant challenges to law enforcement. Seizing digital assets usually requires controlling private keys or compelling virtual asset service providers (VASPs) to freeze accounts with relevant digital assets.³⁰ VASPs collect Know Your Customer (KYC) information to comply with anti-money laundering and counter-terrorism financing regulations.³¹ If multiple jurisdictions' VASPs are involved, each requires separate legal procedures, typically following different timelines and standards. Assets frequently move repeatedly before all necessary legal orders are finalized, necessitating pre-established rapid-response protocols and potentially pre-authorized multi-jurisdictional seizure mechanisms for urgent cybercrime cases.

3. Limited Use and Effectiveness of China's Asset Confiscation Procedures. — Since the introduction of the special criminal confiscation procedures in the *Criminal Procedure Law* in 2012, the practical application remains limited. Accordingly, scholars have explored pathways to activate the special confiscation procedure, with a particular focus on its role in overseas asset recovery within anti-corruption efforts.³² Therefore, in the context of cross-border cybercrime, asset recovery across jurisdictions has remained far from satisfactory,³³ and it is necessary to explore diverse pathways for recovering digital virtual assets. Moreover, China should further ground its efforts in the realities of domestic asset recovery practice and proactively harmonize its legal framework with the UNCC, thereby fostering institutional

28 See JEAN-PIERRE BRUN, LARISSA GRAY & CLIVE STCOTT ET AL., *ASSET RECOVERY HANDBOOK: A GUIDE FOR PRACTITIONERS*, at 128 (The World Bank, 2011).

29 Hou Rouqian, *The Digital Progression of International Criminal Mutual Legal Assistance: Cross-Border E-Discovery as an Object of Analysis*, 1 *The South China Sea Law Journal* 42 (2025).

30 Know Your Customer (KYC) refers to the due diligence process that entities with anti-money laundering obligations must perform on transactions suspected of involving money laundering. See Yang Meng, *Criminal Risks and Regulation of Anti-Money Laundering KYC on Online Financial Platforms*, 11 *Law Science* 107, 108 (2019).

31 See Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin, *Cryptocurrency Compliance and Risks: A European KYC/AML Perspective*, *Blockchain & Cryptocurrency Regulation* 472-474 (2020).

32 Dai Xiaoqiang, *Activation Paths for the Confiscation Procedure of Illicit Proceeds: From the Perspective of Overseas Anti-Corruption Asset Recovery*, 3 *Journal of the People's Public Security University of China (Social Sciences Edition)* 74 (2025).

33 See Jiang Wei & Cao Wuqing, *Several Issues of International Cooperation on Anti-Corruption Fugitive Repatriation and Asset Recovery*, 2 *China Journal of Applied Jurisprudence* 15, 21 (2023).

innovation and achieving more effective governance in cross-border cybercrime asset recovery.

III. A MULTIDIMENSIONAL FRAMEWORK FOR CROSS-BORDER CYBERCRIME ASSET RECOVERY: FORGING SYSTEMATIC PATHWAYS IN THE DIGITAL ERA

A. Defining the Property Status of Digital Virtual Assets and Including Them Within the Scope of Asset Recovery

Criminal MLA aimed at asset recovery carries a certain punitive dimension and requires strict review criteria, as it involves the deprivation or alteration of property rights. It is thus necessary to provide clear provisions and interpretations regarding which assets qualify as ‘property’ for the purpose of recovery. In this context, the status of digital virtual assets as property has already been recognized globally. The Financial Action Task Force defines virtual assets as digital representations of value that can be traded, transferred, or used for payment in a digital environment.³⁴ In order to combat cross-border cybercrime and strengthen the recovery of digital virtual assets across jurisdictions, it is necessary to clarify the following issues at the legislative level.

Firstly, it is necessary to establish, within the framework of criminal law, the status of digital virtual assets as ‘property’, which a number of scholars advocate. Some have argued that under *China’s Criminal Law*, the concept of property is defined broadly to encompass tangible objects, intangible assets, and property interests, and therefore is fully capable of covering digital virtual assets. Accordingly, virtual assets with economic value should be afforded the same criminal protection as physical property.³⁵ Others maintain that it is reasonable to treat the unlawful acquisition of another’s virtual assets as a property crime. Since the public has long been familiar with and frequently uses the concepts, interpreting virtual assets as property under criminal law would not undermine citizens’ ability to foresee the legal consequences of their conduct, nor would it conflict with the principle of legality.³⁶

Secondly, with respect to emerging forms of virtual currency, the mainstream view holds that they may be interpreted as ‘property’ under *China’s Criminal*

34 See Georgios Pavlidis, *International Regulation of Virtual Assets Under Financial Action Task Force’s New Standards*, 1 *Journal of Investment Compliance* 1 (2020).

35 See Chen Xingliang, *The Criminal Attribute of Virtual Property and Its Protection Method*, 2 *China Legal Science* 146 (2017).

36 See Zhang Mingkai, *The Nature of Illegally Acquiring Virtual Property*, 3 *Law Science* 12 (2015).

Law,³⁷ although some scholars disagree.³⁸ Given their property status, together with their technological foundation, transactional value, and the possibility of regulatory oversight, digital virtual currencies can and should be regarded as legitimate objects of confiscation.³⁹ Thus, the legal status and disposal rules of digital assets should be further clarified. It is vital that the *Criminal Law* and related judicial interpretations expressly define virtual currency and other digital assets as either criminal proceeds or the instruments of a crime.

Thirdly, on the premise that digital virtual assets are recognized as property and may serve as objects of criminal confiscation, a framework of special and operational criminal procedure rules must be formulated. These rules need to cover asset seizure by standardizing the technical methods and legal processes for controlling private keys.⁴⁰ Under judicial supervision, specific legal exceptions or channels could be created for the disposal of seized virtual currency, for example, by authorizing designated institutions under strict regulation, or by exploring cooperation with compliant foreign financial institutions to convert it and channel the funds back in an orderly manner. This approach is also consistent with the requirements of international cooperation, as the UNCC, to which China is a member, recognizes virtual property.⁴¹

Finally, a substantive interpretive approach to digital assets shall be adopted. When a digital asset has no real-world counterpart or its ‘substance’ consists solely of code or decentralized-network rights, its application becomes complex. Faced with the problem of legal uncertainty in classifying digital assets, a substantive interpretive approach should be adopted to achieve the proper disposition of digital assets within the existing legal framework. Courts and legislators must therefore expand the scope of legal provisions in the digital sphere, for example, by treating tokenized securities as traditional securities. This interpretive direction should focus on the substantive content of the asset and the rights associated with it, rather than its digital form. In essence, digital assets are a form of financial

37 See Ren Yanju, *Qualitative Analysis of Criminal Law on Illegal Acquisition of Virtual Currency*, 5 *Studies in Law and Business* 160 (2022).

38 See Zhang Chunli, *Criminal Law Attributes and Protection Path of Virtual Currency*, 11 *Zhejiang Social Sciences* 52 (2022).

39 See Zhao Guannan, *On the Criminal Confiscation of Bitcoin*, 4 *Journal of the People's Public Security University of China (Social Sciences Edition)* 96 (2022).

40 See Lan Lihong, *On the Seizure Strategy of Using Virtual Currency to Launder Criminal Assets*, 7 *Policing Studies* 29 (2017).

41 Article 2 of the UNCC explicitly provides that ‘property’ shall mean assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, including virtual assets, and legal documents or instruments evidencing title to, or interest in, such assets.

assets, and their full designation should be ‘digital financial assets’.⁴² Thus, treating digital assets legally as book-entry or registered assets, rather than as bearer instruments, to facilitate freezing and seizure is worth considering. Legislation needs to define pure digital objects as subjects of property rights. At the same time, to address the reality that private law provisions lag behind practice, a *bona fide* acquisition regime for digital assets should be established. Since traditional possession lacks explanatory power and practical vitality in the digital realm, regulations on real-right actions should be formulated with an emphasis on control rather than possession.⁴³

B. Leveraging Asset Recovery Technologies for Digital Virtual Assets

In cross-border cybercrime, the collection of digital evidence is indispensable to asset recovery. This process requires the establishment of both technical and regulatory pathways. On the technical side, advanced scientific tools must be developed and applied to facilitate evidence gathering. Taking DeFi-related criminal cases as examples, their features, including the interplay of on-chain and off-chain transactions, the absence of KYC verification, and deliberate address obfuscation, make detecting abnormal fund flows and tracing transaction chains particularly complex. By shifting investigative approaches, broadening analytical perspectives, and relying on both historical and real-time blockchain data to identify critical investigative leads, investigators can move from passive tracing to proactive detection, thereby responding more effectively to the evolving techniques and tools in virtual currency crimes.⁴⁴ Next-generation forensic tools capable of countering obfuscation technologies, privacy coins, and cross-chain transactions should be encouraged, and strategies should be devised to defeat the anonymity of privacy-enhancing cryptocurrencies and mixing services.⁴⁵ Specialized privacy-enhancing tools and services can be used to analyze transaction flows, identify addresses associated with criminal activity, and detect potential mixing behavior. Despite the capacities of advanced blockchain analysis tools, their effectiveness often depends on the off-chain data that can be integrated,

42 Tan Mingjun, *On the Conceptual Development and Theoretical Framework of Data Assets*, 10 Finance and Accounting Monthly 87, 90 (2021).

43 JASON G. ALLEN, MICHEL RAUCHS & APOLLINE BLANDIN ET AL., *supra* note 19.

44 See Xie Ling & Sun Meicheng, *Fund Flow Investigation Strategies Based on DeFi Crime Typological Analysis*, 2 Journal of the People's Public Security University of China (Science and Technology) 92 (2023).

45 See USMAN HANI & MUSTAFA KHAN, *DIGITAL ASSET SCAMS AND CROSS-BORDER FRAUD: HOW CYBERCRIMINALS EXPLOIT LOOPHOLES*, at <https://doi.org/10.13140/RG.2.2.33807.29608> (Last visited on October 31, 2025).

primarily the KYC information held by VASPs.

Regarding DeFi, scholars have argued that the concept of independent control should be adopted in the DeFi field. There has been a proposal to define independent control to identify centralized actors and classify genuine DeFi protocols as regulated critical infrastructure.⁴⁶ However, classifying specific decentralized systems as critical infrastructure may open up new regulatory and supervisory mechanisms, but it also raises significant questions about state intervention in permissionless systems. If a DeFi protocol is viewed as critical infrastructure, it implies a certain level of public interest that may justify the imposition of security standards, transparency requirements, or even, where technically feasible and in the absence of a central operator, taking emergency measures such as freezing illegally obtained assets. This approach goes beyond regulating through VASPs and regulates the system itself. The fundamental challenge lies in narrowly defining critical regulations and designing proportionate regulations that do not stifle legitimate uses and benefits, which requires regulators to have a high level of technical understanding. Therefore, technical strategies to improve tracing are closely tied to legal and regulatory strategies, ensuring that VASPs collect and share such data.⁴⁷ At the same time, AI and ML technologies can also be applied to recover digital assets. Literature shows that statistical methods, data mining, and ML techniques can be used for detecting money laundering, and multiple studies have examined ML and explainable AI techniques in anti-money laundering.⁴⁸ The International Criminal Police Organization (INTERPOL) has called for automation to keep pace with criminals. The current AI typically identifies known patterns. The future demand is for AI to spot emerging laundering or obfuscation patterns that human analysts have not yet identified, which requires large-scale unsupervised learning or anomaly detection. Moreover, a comprehensive approach to evidence collection should be encouraged. Digital forensics involves identifying and interpreting electronic data stored on devices such as computers and smartphones. Techniques include wallet extraction, device forensics imaging, and the analysis of cryptocurrency applications and wallets. Blockchain forensics focuses on tracing and analyzing transactions

46 Rebecca Rettig, Michael Mosier & Katja Gilman, *supra* note 21.

47 See MA YUYUN, WHO CONSTITUTES THE VASPS IN DEFI? A CASE STUDY ON MONEY LAUNDERING VIA CROSS-CHAIN BRIDGE FROM THE 2022 HARMONY HACK, at <https://doi.org/10.1016/j.jeconc.2025.100131> (Last visited on October 31, 2025).

48 DATTATRAY VISHNU KUTE, BISWAJEET PRADHAN & NAGESH SHUKLA ET AL., DEEP LEARNING AND EXPLAINABLE ARTIFICIAL INTELLIGENCE TECHNIQUES APPLIED FOR DETECTING MONEY LAUNDERING: A CRITICAL REVIEW, at <https://doi.org/10.1109/ACCESS.2021.3086230> (Last visited on October 31, 2025).

within a blockchain, whereas cryptocurrency forensics traces digital assets and their movement on the chain. Combining transaction monitoring with digital forensics enables investigators to collect evidence from the blockchain and devices used by criminals, thereby gaining a more comprehensive understanding of illegal activities and facilitating asset recovery.

C. Enhancing the Cross-Border Asset Recovery Regime for Digital Virtual Assets

1. Strengthening the Normative Basis for Cross-Border Digital Asset Recovery. — To address the inherent issues in traditional international cooperation, a redesign of MLA is required. While reinforcing existing treaties is necessary, a more agile solution is essential to bridge the gap between the rapid evolution of cybercrime and the slower development of novel policy. Given these difficulties, countries should actively promote the universal ratification and effective implementation of international treaties such as the UNCC. Future international legal instruments should focus more on operational aspects, including freezing and seizing digital assets, and consider adopting unified regulatory standards for VASPs as well as provisions for cross-border law enforcement cooperation. Future mutual assistance instruments shall incorporate near-real-time cooperation mechanisms and direct inter-agency collaboration, especially for scenarios requiring the freezing of highly volatile digital assets.

At the same time, one of the defining features of the digitalization of criminal justice in cyberspace is the differentiated application of laws across jurisdictions. To address these divergences, legislators in China should, while remaining grounded in its own national conditions, align with relevant international treaties and adjust its domestic legislation, thereby reducing legal conflicts in cross-border asset recovery. Data-law requirements must be coordinated with international cooperation obligations. Regarding the approval requirements under the *Data Security Law* and the *Personal Information Protection Law* for providing data to foreign judicial or law enforcement bodies, implementing rules should be issued as soon as possible to specify the scope of competent authorities, approval procedures, and timelines, and explore the establishment of a fast-track or simplified procedure for data requests made pursuant to international treaties (such as MLAs), thereby reducing potential impediments to normal judicial cooperation. A balance should be struck between safeguarding data security and the necessary information exchange required by international obligations.

In the field of criminal evidence gathering, a sovereignty-based framework has been established domestically, which adopts a tiered and classified model for digital evidence collection, thereby distinguishing between legislative and law enforcement powers and integrating multiple collection methods. First, the principle of procedural data sovereignty should be affirmed, strengthening equal consultation and cooperation with other states and establishing a reciprocal jurisdictional model for electronic data collection in criminal cases.⁴⁹ Second, evidentiary rules should be examined through the lens of the rule of law in foreign-related affairs, ensuring proportionality between evidentiary measures and the categories of targeted data, while incorporating digital rights into the evidentiary framework.⁵⁰ Finally, it is necessary to clearly distinguish between legislative jurisdiction and law enforcement jurisdiction, and within the latter, explore new cross-border evidence-gathering approaches beyond traditional MLA. In particular, both direct cross-border collection and indirect collection through third-party assistance must be based on the logic of overcoming the territorial limits of law enforcement jurisdiction.

2. Establishing Expedited Judicial Assistance Mechanisms and Secure Information-Sharing Platforms. — Cross-sectoral and cross-border cooperation, reinforced by technological support and resource integration, and the deep optimization of international judicial cooperation models are essential measures for recovering cross-border digital virtual assets.⁵¹ Within existing treaty frameworks, efforts should be made, where possible, to establish more direct and efficient counterpart channels with major partner countries to supplement formal channels and expedite information flow. Informal cooperation mechanisms are crucial for intelligence acquisition, establishing cross-border contacts, and supplementing formal MLA. They afford the flexibility and trust that formal structures often lack. Practice has shown that almost all successful cryptocurrency seizure cases involve robust public-private cooperation and rapid informal cooperation networks. VASPs typically take the lead in identifying illicit transactions, while cybersecurity firms may detect compromised wallets or illegal infrastructure. Many successful crypto seizures involve assets held by or transiting through centralized VASPs, which usually maintain KYC data and can swiftly execute freeze orders. Recovery from non-custodial wallets or DeFi protocols is far rarer and much more complex,

49 See Liang Kun, *Data Sovereignty-Based Mode of National Jurisdiction over the Collection of Criminal Evidence*, 2 Chinese Journal of Law 188 (2019).

50 See Pei Wei & Tong Yiyao, *Alignment of China's Electronic Evidence Collection Rules with the UN Convention on Combating Cybercrime*, 2 Journal of Public Security Science 21 (2025).

51 See Chen Guangzhong, *Discussion on Several Issues Concerning the Improvement of Criminal Procedure Involving Foreign Factors*, 2 Law Science 98 (2025).

typically relying on operational security mistakes by criminals. An actual on-chain seizure in a decentralized environment without VASPs involvement is exceptional.⁵² Future recovery of virtual assets should contemplate cooperative arrangements with compliant VASPs, requesting their assistance in identifying users, freezing accounts, and providing transaction records. Under legal authority, technical investigation measures may include using specific techniques to obtain private key information or trace transactions. Direct cooperation channels should be established with foreign law enforcement units or financial intelligence bodies specialized in digital asset crime to share intelligence and technical methods. Meanwhile, smart-contract applications should be explored. Theoretically, employing smart-contract technology to automatically freeze or return assets could be considered. The UNCC places particular emphasis on the multiple obligations of service providers in criminal justice processes, including data preservation, real-time collection, data disclosure, technical assistance, and confidentiality. China could actively leverage the UNCC's dynamic adjustment mechanisms to define obligations of service providers in a reasonable manner.⁵³ In this process, the balance between safeguarding individual privacy and facilitating cybercrime investigations must be maintained. When legislating disclosure obligations for Internet service providers during investigations, the principle of proportionality should guide the assessment of necessity, appropriateness, and minimization of intrusions into privacy rights.

Intelligence sharing and joint investigation coordination with foreign law enforcement agencies should be strengthened within legal boundaries, while building long-term trust that underpins formal collaboration. In practice, this is often facilitated through mechanisms such as the INTERPOL or directly established liaison channels. Through these arrangements, law enforcement bodies exchange intelligence, notify leads, and coordinate investigations, providing rapid and flexible responses that help secure preliminary information, locate suspects, or trace assets, thereby laying the groundwork for subsequent formal MLA requests. In one respect, a proactive threat-intelligence assessment and emerging technology monitoring mechanism should be established. Specifically, law enforcement agencies should establish intelligence-sharing and collaborative research mechanisms with research institutes and private enterprises, actively monitor and assess new criminal

52 See Nicholas Ryder et al., *The Rise of De-Fi and the Difficulties Associated with the Seizure of Cryptoassets*, 33 *Journal of Financial Crime* 104, 112-115 (2025).

53 See Pei Wei, *Procedural Obligations of Service Providers Under the United Nations Convention Against Cybercrime*, 3 *Journal of Shanghai University of Political Science and Law (The Rule of Law Forum)* 92 (2025).

risks and asset concealment methods driven by emerging technologies, and develop counter-strategies in advance. Transaction monitoring involves observing and analyzing cryptocurrency transactions to identify suspicious patterns and potential illegal activity. Effective monitoring of emerging technology risks in asset recovery requires robust public-private partnerships, including cybersecurity companies as well as the developers, academics, and innovators in these new fields. Law enforcement alone cannot keep pace with the rapid innovation in permissionless environments. The INTERPOL has emphasized cooperation with blockchain intelligence companies and broader discussion on public-private partnerships.⁵⁴ For truly emerging technologies, law enforcement agencies need insights from the technology's builders. For example, developers of new DeFi protocols or metaverse platforms often understand potential avenues for abuse better than anyone else. Establishing non-adversarial dialogue and research partnerships with these communities can provide early warnings and support the design of systems that are more conducive to asset seizure. This signifies a shift from law enforcement's suspicion of new technologies toward proactive engagement with innovators to understand and mitigate risks.⁵⁵

In another respect, efficient intelligence-sharing platforms and protocols must also be established. A truly efficient system will facilitate the rapid, secure, and lawful sharing of specific indicators of threat or illicit activity between the public and private sectors, enabling assets to be swiftly traced or frozen. Given data privacy and liability concerns, this is crucial for combating fast-moving cybercrime finance. According to article 55(2) of the UNCC, establishing cooperative networks for information sharing constitutes an important component of preventing and combating cross-border cybercrime, with an emphasis on integrating resources and enhancing law enforcement efficiency through multi-stakeholder collaboration.⁵⁶ In addition, relevant organizations have established regularized mechanisms for intelligence sharing to address cross-border cybercrime. Such mechanisms could include dedicated funding from states or international bodies, the provision of secure communication platforms, and protocols that specify how intelligence acquired through these networks can be formalized into admissible MLA

54 INTERPOL, INTERPOL GLOBAL CRIME TREND REPORT 2022, at https://www.interpol.int/content/download/18409/file/INTERPOL_Global_Crime_Trend_Report_2022.pdf. (Last visited on October 27, 2025).

55 WORLD ECONOMIC FORUM, CYBERCRIME PREVENTION: PRINCIPLES FOR PUBLIC-PRIVATE ALLIANCES ON CYBERCRIME, at https://www3.weforum.org/docs/WEF_Cybercrime_Prevention_Principles_Public_Private_Alliances_2016_report.pdf. (Last visited on October 27, 2025).

56 See Pei Wei, *Public-Private Cooperation and China's Response Under the Framework of the United Nations Convention Against Cybercrime*, 2 Criminal Science 125 (2025).

evidence, thus bridging the gap between informal and formal evidence.

3. *Adopting Diverse Pathways for Cross-Border Recovery of Digital Virtual Assets in Cybercrime.* — In practice, China's efforts to recover cross-border digital assets still have room for improvement. Nevertheless, adopting multiple recovery approaches represents an important direction for future work.⁵⁷ In the area of cross-border digital asset recovery, articles 49 and 50 of the UNCC explicitly require states to cooperate in enforcing confiscation orders issued by foreign courts and to permit non-conviction-based forfeiture in situations such as the offender's death, flight, or absence. The provisions further mandate measures to freeze, seize, and ultimately confiscate digital assets located abroad, while safeguarding the rights of *bona fide* third parties. These mechanisms establish the institutional basis for pursuing on-chain assets across jurisdictions. As China advances its digital asset recovery efforts, domestic procedures should be aligned with the UNCC framework to build a coherent system that connects domestic processes with international cooperation mechanisms.

The primary pathway involves achieving direct recovery of digital assets.⁵⁸ One possible approach is civil litigation aimed at directly recovering property, which mainly takes two forms. The first is civil actions initiated by the victim. This method applies when offenders, after illegally acquiring property, neither invest nor consume it lawfully, but instead store it in DeFi protocols or other digital environments. In such cases, victims may file a civil lawsuit, use blockchain tracing and forensic analysis to identify relevant wallet addresses, and seek a court order for the recovery of digital assets held at these addresses. The second is non-conviction-based forfeiture (NCBF) proceedings initiated by the state. This procedure is especially suited to digital assets, as the anonymity and technical complexity of cybercrime often make it difficult to identify and convict specific perpetrators. Unlike traditional confiscation, which serves as a form of criminal punishment, NCBF is civil or *in rem* in nature: its subject is the asset itself rather than a particular defendant. This feature allows the legitimate owner of the assets to participate as a claimant and defend the legitimate source of the assets.⁵⁹ The *in rem* character of NCBF aligns closely with blockchain technology, enabling courts to bring actions directly

57 See Jin Zegang, *Dilemma Approach Protest of Solution of Extraterritorial Application of Chinese Criminal Law*, 4 Law Science 58 (2025).

58 This article adopts a broad understanding of 'direct recovery', encompassing civil claims and non-conviction-based forfeiture, as mechanisms that permit the identification and return of stolen assets without requiring a criminal conviction.

59 See THEODORE S. GREENBERG, WINGATE GRANT & LINDA M. SAMUEL ET AL., *STOLEN ASSET RECOVERY: A GOOD PRACTICES GUIDE FOR NON-CONVICTION BASED ASSET FORFEITURE*, at 8-9 (Wang Xiaoxin trans., China University of Political Science and Law Press, 2013).

against tainted wallet addresses or smart contracts and thus to demonstrate their connection to illicit activity through on-chain analysis — even without identifying the ultimate controllers. The advantages of this approach include a lower burden of proof compared to criminal proceedings and the availability of relief where conviction is difficult or impossible to obtain.⁶⁰ It is further recommended that China should refine the implementation rules of both criminal confiscation and NCBF, and strengthen their procedural linkages. Third, when illicit proceeds are recovered from offenders, whether voluntarily or involuntarily, judicial authorities may employ summary procedures for the direct return of assets to victims. This measure streamlines judicial processes and enhances the efficiency of restitution.⁶¹ For example, this procedure may be applied when hackers return stolen cryptocurrencies to a project wallet, or when a centralized exchange identifies and freezes funds related to fraud, thereby ensuring swift relief for victims. Importantly, summary return requires either the offender's admission to criminal facts or sufficient evidence to establish the illicit nature of the assets. Another available remedy is the use of compensation or restitution orders. Where illicit proceeds have been converted through decentralized exchanges into other digital assets or used for on-chain investment and consumption, victims may seek compensation or restitution orders to recover their property through civil remedies. This approach requires the victim to demonstrate a direct causal link between the offender's unlawful gains and the victim's losses.⁶² The amount of restitution or compensation must correspond to the victim's losses. Moreover, particular attention must be given to the extreme volatility of digital asset prices when determining valuation points and amounts, in order to effectively safeguard victims' rights.

Furthermore, asset-sharing mechanisms should be advanced to encourage suspects to voluntarily return illicit assets during criminal proceedings.⁶³ In 2018, the *Law on International Criminal Judicial Assistance* officially established an overseas asset-sharing mechanism at the legislative level. Its core purpose is to encourage states to actively participate in international

60 See Jiang Xinmiao & Xu Luting, *The Evolution of International Legal Rules on Cross-Border Recovery of Corrupt and Non-Conviction-Based Assets Confiscation*, 6 *Presentday Law Science* 97 (2022).

61 See HUANG FENG, *RULES AND PRACTICES OF INTERNATIONAL JUDICIAL COOPERATION IN CRIMINAL MATTERS*, at 157-159 (Peking University Press, 2008).

62 See Xia Wei, *A Study on the United Nations Convention Against Corruption and the Asset Recovery System*, 1 *Southeast Law* 110-118 (2016).

63 The United States calls it equitable sharing, the United Kingdom the Asset Recovery Incentive Scheme, Canada the forfeiture property sharing, and Australia the Equitable Sharing Program — all denote a system whereby the state holding the criminal assets and the state of origin share confiscated assets, after deducting reasonable expenses incurred in law enforcement and judicial cooperation, in proportion to each state's contribution. See XIE BIN, *STUDIES ON CRIMINAL LEGAL ISSUES OF OVERSEAS RECOVERY OF STOLEN ASSETS*, at 139 (China University of Political Science and Law Press, 2016).

cooperation, supplement the finances of cooperating parties, and serve as a shared economic incentive for the recovery of illicit assets. The asset-sharing system serves to balance and reconcile economic interests of all parties, motivate joint efforts to trace illicit assets, improve recovery efficiency, help resolve dilemmas in the disposal of confiscated property, and maximize mutual benefits.⁶⁴ On a reciprocal basis, a more proactive stance should be adopted in negotiating bilateral agreements or *ad hoc* arrangements with cooperating states on asset sharing and return. Clear rules on distribution can effectively incentivize requested states to devote resources to asset recovery, particularly in digital asset cases that demand substantial technical investigation and legal expertise. For instance, if a state provides key on-chain transaction analysis, assists in freezing accounts at centralized exchanges, or uses technical means to access offline private keys, confiscated assets could be shared proportionally after deducting law enforcement and judicial expenses. Asset sharing could take the form of long-term agreements or arrangements tailored to individual cases. In terms of distribution, confiscated assets should first be returned to victims or lawful owners. This principle is crucial for upholding justice and protecting victims in cases involving multiple victims such as phishing attacks or exchange theft. After reasonable expenses are deducted, the remaining assets could then be distributed among cooperating states. The primary basis for allocation should be the contribution of each party, supplemented by factors such as the nature of the crime and the degree of harm to the requesting state.⁶⁵ Drawing on successful *ad hoc* cooperation, China could gradually stabilize bilateral asset-sharing practices and establish reasonable distribution standards based on the nature of individual cases.

Finally, establishing a dedicated mechanism for valuing and proportionately returning digital assets is imperative. The UNCC has recognized virtual assets as ‘property’.⁶⁶ Given the extreme volatility and technical complexity of digital assets, the traditional model of complete confiscation is no longer suitable. To address this challenge and align with international standards, there is an urgent need to pioneer a new pathway for digital asset recovery. First, a dynamic valuation standard should be established. International cooperation should be directed toward developing a shared methodology for valuing digital assets, using key judicial principles as benchmarks. Prices should be referenced against

64 See HUANG FENG, *COMPARATIVE STUDIES ON ASSET RECOVERY*, at 145 (Beijing Normal University Press, 2010).

65 See Shang Haowen, *Research on the Asset Sharing System in Overseas Stolen Goods Recovery*, 5 *China Legal Science* 286, 304 (2022).

66 *Supra* note 41.

major exchanges or calculated using time-weighted averages to ensure fair valuation. Confiscation should be limited to the portion equivalent to the illicit proceeds, with appreciation or amounts exceeding the illicit proceeds returned to the rightful owners. This approach not only complies with the UNCC but also protects legitimate property rights. Second, blockchain technology should be leveraged for precise restitution. Tools such as smart contracts could facilitate a transparent and efficient mechanism for asset disposal and return. Once a judgment takes effect, smart contracts could automatically transfer the adjudicated amount to the victim's or the treasury's designated wallet, with the remaining balance automatically returned. This technology-driven pathway not only mitigates valuation challenges stemming from price volatility but also guarantees precision, transparency, and efficiency in law enforcement, adhering to the principle of 'code is law'.⁶⁷ This can also reduce trust costs in cross-border law enforcement. Third, an international consensus should be pursued on the treatment of assets seized in excess of illicit proceeds. Given the divergent national approaches to the legal characterization of virtual property, China should actively participate in multilateral dialogues to reach a consensus on the legal status of digital assets, standardized valuation methods, and the principles governing the return of excess assets. It should be clarified that in the context of international cooperation, requested states should respect proportional confiscation judgments rendered by requesting states under the UNCC and provide procedural support for executing such partial return orders, thereby removing the legal barriers in digital asset recovery.

IV. CONCLUSION

The practical challenges posed by cross-border cybercrime in the digital age cannot be overlooked. From the threefold perspectives of norms, technology, and procedure, this paper aims to provide a preliminary response to the complex subject of crime governance. Nonetheless, it must be further emphasized that several critical issues require in-depth research, for instance, jurisdictional conflicts, evidentiary difficulties, procedural remedies, and the protection of human rights in asset recovery. The adoption of the UNCC presents both new opportunities and challenges. China should seize this opportunity to better align its domestic legal framework with its obligations under international treaties.

⁶⁷ 'Code is law' means that with the emergence of digital technology, code has gradually become the primary means of regulating the behavior of internet users. See Zhao Lei & Cao Jianfeng, *From 'Code Is Law' to 'Law Is Code': Taking Blockchain as an Internet Regulatory Technology as the Entry Point*, 5 Science Technology and Law 7 (2018).

Against the backdrop of the fourth amendment to the *Criminal Procedure Law*, China should recognize the trajectory of digitalization in foreign-related criminal proceedings. Guided by a comprehensive legislative model,⁶⁸ it must pay close attention to the differences, reciprocity, equality, and fragmentation that arise from balancing domestic and international regimes. Specifically, the legislative process for digital asset recovery should be further advanced. Correspondingly, the role of China's judicial authorities in recovering assets from cross-border cybercrime must be strengthened, with the establishment of a clear and accountable recovery framework, so as to establish a scientific, effective, convenient, reciprocal, and regularized system for cross-border asset recovery in cybercrime.

(Edited by Gong Li)

68 See Chen Weidong, *Research on Several Issues Concerning the Legislation on Foreign-Related Criminal Procedure*, 5 Law Science Magazine 1, 13 (2025).