Proceedings of the 4th International Conference on Social Psychology and Humanity Studies
DOI: 10.54254/2753-7048/2026.ZJU31824

# *Governance of Virtual Currency Money Laundering under Criminal Law*

**Yongji Wu**

*Graduate School of Arts and Science, New York University, New York, USA*
*ileonardowui@gmail.com*

***Abstract.*** Money laundering using virtual currencies, due to its anonymity, nature of cross-border, and technical complexity, has already posed a severe threat to the traditional criminal law system. There are some controversies in the Chinese legal system regarding the legal attributes of virtual currencies and the proper interpretation of "knowing" in the crime of money laundering. These controversies have made efforts in combating money laundering crimes involving virtual currencies ineffective. In this regard, it is urgent to establish a sound legal framework and clarify the subject of responsibility and sentencing of this technology abuse; Improve the active defense capability of technology and build a comprehensive real-time monitoring technology through multi-party cooperation; Promote social collaborative governance and enhance public awareness of prevention. While curbing the abuse of technology, people should also reserve space for its beneficial application and promote the development of deep counterfeiting technology within the legal and compliant boundaries, so as to maintain social stability and safeguard public interests.

***Keywords:*** Virtual currency money, criminal law, Chinese legal system

## 1. Introduction

"Virtual currency" refers to encrypted digital assets issued based on blockchain technology and do not have the status of legal tender. It includes mainstream cryptocurrencies such as Bitcoin and Ethereum as well as stablecoins and normal excludes non-fungible tokens (NFTs) and similar assets. Due to the widespread application of blockchain technology, virtual currency, as a new type of digital asset, has become an important component of the global financial system. However, while virtual currencies provide enormous investment opportunities for the financial market, they also offer some covert channels for illegal activities. According to the Chainalysis 2025 Crypto Crime Report, the worldwide scale of illicit and virtual currencies-related funds in 2024 was approximately $40.9 billion, with estimates suggesting it could ultimately exceed $51 billion by the end of 2025 [1]. Virtual currencies are consequently considered as an "accelerator" for money laundering crimes [2]. In China, the Notice on Further Preventing and Addressing Risks from Virtual Currency Trading and Speculation was issued on September 24, 2021. It imposed a comprehensive ban on virtual currencies and prohibited financial institutions, payment institutions, as well as trading platforms from engaging in related businesses. Nevertheless, criminal activities involving virtual currencies have not been effectively curbed. Criminal cases, such as the money laundering case by Chen and

DOI: 10.54254/2753-7048/2026.ZJU31824

the robbery of virtual currency by Zhang, emerge one after another. Therefore, how to govern crimes which utilize virtual currencies should be regarded as a noteworthy topic. This article aims to discuss the governance of the most prevalent category among virtual currencies crimes, namely money laundering. By combining the technological characteristics of virtual currencies themselves with money laundering networks, and through analyzing the multiple dilemmas faced in governing money laundering crimes using virtual currencies under current criminal law system, this paper proposes some corresponding countermeasures.

## 2. The characteristics of virtual currencies and money laundering

### 2.1. Features of virtual currencies

The significant technological characteristic of the virtual currency makes it highly vulnerable for money laundering [3]. First and foremost, one of the key aspects of virtual currencies is decentralisation. It is made possible by blockchain. The issuance, verification, management and transaction of virtual currency operate independently of any central authority outside the traditional banking system. This decentralized nature offers the virtual currency and network a high level of resistance against attacks, great transaction convenience, as well as being free from conventional financial or banking regulations. One such attribute is used by many criminals in order to effect transactions using illicit proceeds, that of virtual currency. However, while anonymity is essential to ensure privacy of bodies performing legal virtual currency transactions, it can be misused by criminal groups for identification avoidance. Anonymity is made possible mainly through blockchain's encryption technology that masks the real identity of individuals. Although this creates a privacy barrier for the users to a certain extent, it causes serious difficulties for regulators. Some virtual currencies might also strengthen this protection of anonymity by the adoption of sophisticated privacy-protecting technologies, which would further complicate attempts to attribute criminals' identities to actions. Coin-mixer functions also may be used to pool multiple transactions together and stir these funds, complicating the money trail and making it almost impossible to track down the source of the funds. The powerful internationalization of the virtual currency was also one of its main characteristics. In the traditional cross border payment system, people need to transfer money through some intermediary institution and it is much more complicated with high fees and long transaction time. By comparison, the virtual currency transactions are conducted through a globally decentralized network that enables users to make direct money transfer to any country at any time and withdraw without approval from traditional financial institutions or foreign exchange regulations. This cuts dramatically the cost of trading and improves liquidity of funds. Nonetheless, this great convenience is a challenge for financial regulation. Financial crimes such as capital flight and illicit fund transfers cannot be promptly intercepted within a single country due to this feature. Subsequent asset recovery requires international cooperation and consequently increases the complexity of judicial procedures.

### 2.2. The ecosystem of money laundering involving virtual currencies

The money laundering network using virtual currencies has a sophisticated and well-established ecosystem. Typically, the network can be divided into three main segments: upstream, midstream, and downstream. The upstream segment primarily consists of criminal gangs and "card ants" recruited by the gangs. These "card ants" normally join through social networks and part-time job platforms; some are fully aware of the true purpose behind their actions, while others are simply

DOI: 10.54254/2753-7048/2026.ZJU31824

lured by this lucrative opportunity. In general, the upstream of a money laundering network provides a vast pool of bank accounts and lays the foundation for further laundering operations. The midstream segment is the core of an entire money laundering chain. Its primary responsibility is to convert illicit funds into virtual currencies and thereby achieving the purpose of "cleaning". Midstream groups are composed of "crypto merchants", "score runners", and "fourth-party payment platforms". As the name suggests, "crypto merchants" are traders who supply virtual currencies; they typically accept orders via social platforms such as Wechat groups and Telegram. Then, "score runners" use the large number of accounts provided by upstream to purchase virtual currencies in batches, dispersing the funds across multiple digital wallets addresses to sever tracing paths. In this process, virtual currencies are predominantly used for "placement" and "layering", and rarely for "integration". Simply speaking, money laundering networks prefer to use virtual currencies to pocket the funds and then obfuscate them, seldom employing them for actual payment or spending [4]. The role of "forth-party payment platforms" is to provide channels for converting virtual currencies back into fiat currencies. Finally, the downstream segment mainly involves cashing out virtual currencies into legitimate fiat money and facilitating cross-border transfers. Offshore exchanges, over the counter (OTC) merchants, and underground money houses are primary participants in the downstream money laundering network. The money laundering network involves a wide range of individuals, and the relationship between personnel across different segments are often lost and disconnected. This structure frequently poses significant obstacles to efforts aiming at fighting against money laundering crimes.

## 3. The dilemmas of governing money laundering using virtual currencies

### 3.1. Ambiguity in legal attributes

The legal attributes of virtual currencies remain ambiguous. The Chinese legal system has yet to provide a clear definition of the legal attributes of virtual currencies. In the adjudication of certain criminal cases, virtual currencies have been treated as "property". For example, in the theft case of Zhang, the court explicitly stated in the criminal judgement that virtual currencies are objects subject to protection of criminal law. Although they do not possess the attributes of currency, they are still considered as a specific type of virtual commodity, acquired through mutual transfers in exchange for money and thus possess economic value. In judicial practices, the aforementioned case indirectly recognizes virtual currencies' property attributes in terms of criminal law, which can be managed, transferred, have value, and be subject to property crimes. However, in some judicial cases, virtual currencies have been regarded as "data", particularly in cases involving illegal acquisition, control, or intrusion into computer systems. For instance, in the case of Xu for illegally obtaining data from a computer information system and illegally controlling a computer information system. The defendant Xu hacked into the server of a virtual currency trading platform, illegally obtained and transferred thousands of USDT and cashed them out as Chinese Yuan. The court held that Xu violated national regulations by using technical means to obtain data stored or processed in another party's computer, constituting the crime of illegally obtaining data from a computer system, and ultimately sentenced him to three years' imprisonment along with an order to make restitution and fines. Although the prevailing view tends to recognize the property attributes of virtual currencies, some judgement still treats them as "data stored in computers" especially in cases involving illegal acquisition or intrusion into a computer system, emphasizing their form as a digital carrier. Certain scholars argue that the essence of virtual currencies is data and refute the view of treating them as "property".

DOI: 10.54254/2753-7048/2026.ZJU31824

Their views are basically based on three grounds: firstly, virtual currencies cannot be interpreted as "shares, stocks, bonds, or other property" owned by individuals as stipulated in the fourth paragraph under Article 92 of the Criminal Law; secondly, the Civil Code does not classify virtual currencies as "objects", and their anonymity conflicts with the principle of publicity in property rights; thirdly, virtual currencies do not fall under statutory property interests such as stocks or negotiable instruments and cannot be analogized to "property". At the same time, based on the technical nature of virtual currencies and multiple judicial precedents, it can be argued that criminal law should protect data security and network order rather than the "property value" of virtual currencies [5].

### 3.2. The difficulty in applying the money laundering offence

Article 191 of the Criminal Law stipulates that, for the subjective element of the crime of money laundering, the perpetrator has to "know" that the funds they are dealing with are illicit proceeds and still deliberately conceal or disguise their source and nature. However, in money laundering cases involving virtual currencies, determining the perpetrator's "knowing" has become a major difficulty [6]. To begin with, even if virtual currencies do not have the status of legal tender in China and trading and speculation activities are comprehensively prohibited, judicial practices still recognize their property attributes and commercial activities related to virtual currencies remain legal as civil activities. Perpetrators can easily conceal their money laundering intentions by citing various reasons (such as normal cryptocurrency trading or blockchain experimentation). Judicial authorities often find it difficult to presume the perpetrator's "knowing commission" of the crime based on the connection between the funds and upstream crimes. It is because most criminal cases involving virtual currencies entail an extremely complex and difficult-to-trace chain, with numerous participants, meticulous division of labor, and loose connections among members.

As a result, many participants may not understand the true intentions of the project they are engaged in, making it impossible for the judiciary to clearly establish the cognitive element. Furthermore, judicial interpretations normally propose using behaviors such as "transaction prices significantly deviating from the market" or "rapid inflow and outflow of funds" as objective grounds for presuming "knowing". However, in the virtual currency trading market, such behaviors are actually normal trading activities and cannot serve as strong evidence to prove "knowing". Compounded by the inherent anonymity and cross-border nature of virtual currencies, determining the consistency between "subjective knowing" and "objective knowing" becomes the greatest obstacle. Whether the perpetrator subjectively "knows" is the foundation for establishing the criminal facts [7]. Therefore, proving "knowing" in money laundering cases is extremely difficult in judicial practice. The technical characteristics of virtual currencies, combined with the complexity of money laundering networks, render traditional "presumption of knowing" models inapplicable to these new forms of money laundering.

## 4. Governing money laundering crimes from the perspective of criminal law

### 4.1. Clarifying the legal attributes of virtual currencies

When virtual currencies serve as the object of money laundering crimes, the ambiguity in the legal attributes in terms of criminal law leads to difficulties in identifying them as "proceeds of crime and the benefits derived therefrom". The Civil Code has classified virtual currencies as virtual property, recognizing their "property" attributes. However, the Criminal Law does not explicitly specify

DOI: 10.54254/2753-7048/2026.ZJU31824

whether or not virtual currencies fall within the scope of regulation under Article 191 on the crime of money laundering. If they are deemed as "data", they do not meet the traditional criteria of "property", making it impossible to convict under the money laundering offense. Thus, behaviors of using virtual currencies to conceal or disguise illicit proceeds may be interpreted as a violation of Article 312 instead of Article 191. There is an essential distinction between the money laundering offense and the offense of concealing or disguising criminal proceeds under Article 312 of the Criminal Law. The former applies only to "property" derived from seven specific categories of serious crimes, while the latter covers illegal proceeds and benefits from all crimes. However, the latter carries lighter penalties in terms of both types of punishment and the range of imprisonment compared to the former [8]. Some perpetrators may harbor a fluke mentality, weighing the costs and benefits before knowingly committing the act, hoping to exploit blind spots in the system of offense classifications to avoid the money laundering charge and receive a lighter sentence. Such phenomena are unfavorable to efforts in governing money laundering crimes. Although current judicial practice has generally recognized the property attributes of virtual currencies, judicial consensus does not equate to legislative confirmation. Therefore, the legal attributes of virtual currencies should be clarified, and be endowed with "property value" under Criminal Law.

Legislatively confirming that virtual currencies fall under "other property" as stipulated in Article 92 of the Criminal Law, thereby subsuming them within the scope of privately owned property of citizens, will allow them to serve as objects of property crimes. This will clarify the incrimination standards and reduce controversies arising from the ambiguity of attributes. At the same time, the description of the money laundering offense could be supplemented to specify that using virtual currencies to conceal criminal proceeds constitutes money laundering conduct, making it subject to all possible penalties under Article 191. This will provide a foundation for judicial authorities and citizens to accurately interpret the legal provisions. Chinese judicial practice itself shows a growing tendency to recognize the property attributes of virtual currencies [9]. Therefore, accelerating legislation on digital property, granting virtual currencies legal status, and classifying them as non-financialized commodities represent viable options for considerations [10].

### 4.2. Adopting a new presumption model for "knowing"

In 2024, the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Money Laundering Cases, promulgated by relevant authorities, provided the guidance for the first time in Article 3 on how to understand the abstract concept of "knowing or ought to know". The provision generally states that determining "knowing or ought to know" must consider the information accessed or received by the perpetrator, the amount and conversion methods of the illicit funds handled, abnormal circumstances in transactions and accounts, as well as a comprehensive examination of all evidence in the case, including the perpetrator's professional experience, relationship with upstream criminals, statements and defenses, and testimony from co-defendants. However, this interpretation remains grounded in the patterns of traditional money laundering crimes involving funds and does not generalize or explain whether anomalous transaction behaviors on the blockchain involving virtual currencies can be used to presume "knowing".

Therefore, on-chain anomalous activities should be incorporated into the scope of reference. Specifically, four types of behaviors should be established as bases for presumption. Firstly, the on-chain receiving address has been associated with regulated platforms or known criminal addresses. If the receiving addresses has appeared in regulatory announcements or judicial freezing notices, this indicates that the perpetrator has accessed a contaminated fund pool and has a high probability of involvement in money laundering activities. Secondly, the perpetrator deliberately severs the source

DOI: 10.54254/2753-7048/2026.ZJU31824

trail by using coin mixers, cross-chain bridges, or privacy coins. For example, in a money laundering case that happened in 2023, the defendant deliberately used a coin mixer to split illicit funds and made funds unable to be traced. Ultimately, the court treated "use of coin mixer" as a key basis for presuming "knowing". Virtual currency transactions inherently possess strong privacy features but actively employing tools such as coin mixers in scenarios where privacy protection is unnecessary, and without providing a reasonable explanation for the usage, can be regarded as an attempt to obstruct tracing of the source and consequently highly suggest the concealment for illegal activities. Thirdly, OTC quotes are significantly deviated from the market midpoint price without reasonable explanations. The OTC market refers to the over-the-counter market, a decentralized financial market where transactions occur directly between buyers and sellers rather than through traditional exchanges. If a perpetrator's account consistently quotes prices on OTC that are 5 basis points below or above the market midpoint, accompanied by large-scale of splitting of funds, this will align with classic arbitrage models of "disconnected cash-out" or "premium laundering" indicating substantial risks of financial crimes for such accounts. Finally, the target account rapidly splits funds into multiple cold wallets in a short amount of time. A cold wallet is an offline method of storing virtual currencies. Its core feature is that it is not connected to the internet, thereby significantly reducing the risk of theft by hackers, viruses, or network vulnerabilities. If a perpetrator, within 48 hours, splits a single large amount fund into numerous small portions of virtual currencies and disperses them into multiple cold wallets, this behavior bears a strong similarity to traditional money laundering techniques and can serve as an inference of money laundering conduct. In summary, when a suspect's account exhibits one or more of the aforementioned behaviors, it can be presumed that the perpetrator concealed the proceeds of upstream crimes while "knowing" of their illicit nature.

## 5. Conclusion

Money laundering involving virtual currencies has evolved from sporadic individual cases into a structured industrial chain. The technical complexity of this crime, coupled with the lag in legal frameworks, has rendered traditional criminal law governance models ineffective. This article identifies the dilemmas in current governance system in two primary aspects. First of all, in terms of legal attributes, the Civil Code has already affirmed the status of virtual currencies as virtual property, yet criminal law continues to leave them suspended between "property" and "data". This results in imbalanced sentencing when Article 191 (money laundering) and Article 312 (concealing or disguising criminal proceeds) of the Criminal Law both concur. Secondly, in terms of proving subjective "knowing", blockchain technologies such as on-chain anonymity have severed the empirical basis for presuming "knowing" in money laundering offenses, causing traditional "abnormal transaction" indicators to fail in the highly volatile virtual currency market. In response, this article proposes legislative measures and adds "digital assets" as an illustrative example under "other property" in Article 92 of the Criminal Law. Meanwhile, it suggests to inserts an explicit provision on "money launder via virtual currencies" in Article 191. On the judicial front, it suggests directly presuming that a person "ought to have known" based on four categories of conduct: the on-chain address having previously received frozen assets; actively using coin mixers; OTC quotes continuously deviating from the market price by more than 5%; and splitting funds into multiple cold wallets within 48 hours. Only through such multidimensional approaches can achieve a dynamic balance between encouraging financial technological innovation and safeguarding national financial security and help to fundamentally curb the high incidence of money laundering crimes using virtual currencies.

DOI: 10.54254/2753-7048/2026.ZJU31824

## References

[1] Chainalysis (2025) The 2025 Crypto Crime Report. Chainalysis Inc.
[2] Guidara, A. (2022) Cryptocurrency and money laundering: A literature review. Corporate Law and Governance Review, 4(2), 36-41.
[3] Prendi, L., Borakaj, D. and Prendi, K. (2023) The new money laundering machine through cryptocurrency: Current and future public governance challenges. Corporate Law and Governance Review, 5(2), 84-91.
[4] Leuprecht, C., Jenkins, C. and Hamilton, R. (2023) Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. Journal of Financial Crime, 30(4), 1036-1054.
[5] Zhang, C. (2022) The criminal law attributes of virtual currency and protection paths. Zhejiang Social Sciences, (11), 52-59.
[6] Wardani, A., Ali, M. and Barkhuizen, J. (2022) Money laundering through cryptocurrency and its arrangements in money laundering act. Lex Publica, 9(2), 49-66.
[7] Lü, H. (2023) Dilemmas in punishing virtual currency-related criminal crimes and legal safeguards. Tribune of Political Science and Law (Journal of China University of Political Science and Law), (4), 173-184.
[8] Shi, Y. and Wang, Y. (2019) Criminal governance of Bitcoin money laundering crimes. Journal of National Prosecutors College, 27(2), 47-62.
[9] Xu, D. (2025) The identification of the legal nature of virtual currency and the coordination mechanism with judicial disposal. Judicial Application, (11), 133-147.
[10] Lu, J. and Liu, J. (2025) Governance strategies for virtual currency money laundering crimes: An analysis from a risk perspective. Beijing Social Sciences, (2), 105-116.