Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR28074

Research on the Rules for Adjudicating Evidence in Virtual Currency Crimes

Yifei Kang

Law School, East China University of Science and Technology, Shanghai, China
19301302609@163.com

Abstract. As a novel asset form within the digital economy, virtual currency crime activities are increasingly prevalent, challenging traditional criminal evidence rules. The three defining characteristics of virtual currency crime—anonymity, cross-border circulation, and technological dependency—create significant difficulties in evidence assessment. Specifically, these include excessive reliance on verbal evidence such as confessions, complex verification of involved fund flows, and difficulties in accurately determining the value of involved virtual currencies. To address this, approaches such as employing diversified chains of evidence for analysis, implementing differentiated verification of evidence content, and refining comprehensive valuation mechanisms for involved virtual currencies should be adopted. This will advance the refinement of evidence verification rules for virtual currency crimes, providing theoretical support for combating emerging criminal activities and safeguarding judicial fairness.

Keywords: Virtual currency crime, Blockchain, Evidence assessment

1. Introduction

In recent years, as a novel asset form in the digital era, virtual currency has become a significant focus in legal theory and judicial practice.

In 2025, the Central Political and Legal Affairs Conference proposed conducting legislative research on emerging fields such as virtual currency and data ownership rights.Unlike traditional currency crimes, virtual currency crimes exhibit characteristics such as anonymity, ease of cross-border movement, and high liquidity. Consequently, traditional evidence rules for currency crimes are difficult to apply. Currently, academic attention to evidence rules for virtual currency crimes remains limited, yet such offences are proliferating in practice. In light of this, this paper seeks to establish and refine evidence rules for virtual currency crimes by examining their distinctive characteristics.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.BR28074

2. The essence of virtual currency crime

2.1. Relevant definitions of virtual currency crime

Virtual currencies may be defined from both technical and legal perspectives. Technologically, encrypted virtual assets underpinned by blockchain, distributed ledger technology, and smart contracts are collectively termed "virtual currencies". From a legal perspective, the European Banking Authority (EBA) defines virtual currency as "a digital representation of value that is not issued by a central bank or public authority, is not necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be electronically transferred, stored or traded." In 2014, China's five ministries issued the "Notice on Preventing Bitcoin Risks," explicitly stating that virtual currencies such as Bitcoin are not issued by monetary authorities, lack monetary attributes such as legal tender status and compulsory circulation, and are not genuine currencies. Instead, they constitute specific virtual commodities without legal status equivalent to currency and cannot nor should they circulate as currency in the market.

Virtual currency crime refers to activities where perpetrators covertly commit offences by exploiting the technical characteristics of the underlying blockchain technology supporting virtual currencies—namely decentralisation, anonymity, global circulation, and transaction convenience—using virtual currencies possessing dual attributes of data and property as criminal tools, objects, or means [1].

2.2. Characteristics of virtual currency crimes

Firstly,Anonymity. The commission of virtual currency crimes relies on the coordination of private keys, public keys, and wallet addresses. Private keys, as randomly generated cryptographic codes, control ownership of virtual currency; public keys are derived from private keys to calculate wallet addresses; wallet addresses, being hash values of public keys, serve as transaction destinations without direct linkage to real identities. The diverse forms of wallets in virtual currency transactions provide criminals with varied anonymity methods. The anonymity of virtual currency crime can be categorised into two types: firstly, address anonymity, wherein the address generated from the public key conceals the criminal's true identity; secondly, transaction anonymity, whereby although transaction records are publicly recorded on the blockchain, the identity information of both parties remains encrypted and protected. Both methods conceal the criminal's identity, complicating the subsequent identification of criminal evidence.

Secondly,Cross-border liquidity. Unlike traditional currencies, virtual currencies enable swift cross-border transactions and transfers with extensive reach. Criminals exploit this characteristic, endowing virtual currency crimes with high cross-border liquidity. Given the cross-border nature of virtual currency transactions, criminals can exploit regulatory disparities between nations. They establish servers in jurisdictions with lax oversight to conduct transactions, thereby evading legal pursuit and enforcement in specific countries. Furthermore, the swift transferability of virtual currency allows criminals to rapidly move funds across borders through blockchain transactions, creating significant obstacles for subsequent investigative efforts. This cross-border movement presents three primary legal impediments to evidence collection: firstly, divergent cross-border e-discovery regulations across nations entail substantial costs in establishing legal validity and encounter political obstacles; secondly, complex judicial procedures and insufficient judicial authority often result in missed opportunities for timely evidence gathering; thirdly, constraints imposed by technological and commercial factors hinder effective governmental oversight.

DOI: 10.54254/2753-7048/2025.BR28074

Thirdly,Technological Dependency. At the core of virtual currencies lies blockchain technology. This distributed ledger employs a peer-to-peer approach to record all virtual currency transactions, thereby ensuring transaction security and credibility [2]. Virtual currency crimes exhibit a dependency on blockchain-centric technologies, manifesting primarily in two aspects. Firstly, the execution of criminal acts necessitates specific technical means. Offenders exploit advanced applications of blockchain's distributed ledger technology, encryption techniques, and other sophisticated methods to perpetrate offences. These technologies inherently confer a high degree of technical specialisation upon the criminal acts themselves. Secondly, criminal evidence predominantly exists as electronic data stored within blockchain ledgers. This electronic data possesses virtual and fluid characteristics, necessitating specialised technical methods and tools for its collection, preservation, and authentication. Traditional approaches for verifying physical or documentary evidence are inapplicable. Consequently, the authentication of evidence in virtual currency crimes is inseparable from the application of digital technologies such as blockchain and cryptography.

3. Challenges in evidence authentication for virtual currency crimes

3.1. Inapplicability of traditional verification rules

3.1.1. Difficulties in legitimacy assessment

In the field of virtual currency crimes, the core dilemma in evidence determination lies in the fact that traditional evidence rules are difficult to be effectively applied. Especially when dealing with numerous blockchain-related evidence, if the traditional electronic evidence rules are forcibly applied, a series of negative effects will arise. Traditional electronic data recognition rules emphasise the complete documentation and verification of the data collection, extraction, custody, and transfer chain, requiring procedures like inspection records and video documentation of extraction processes to ensure legal compliance. However, owing to the anonymity and widespread circulation of virtual currencies, transaction records inherently reside across globally distributed nodes. Investigators often cannot directly "extract the original storage medium" nor visually verify the evidence collection process through means such as "viewing recordings". Furthermore, the legal boundaries of commonly employed technical methods—such as remote examination and implanted programme forensics—remain contentious, creating tension between procedural legitimacy and personal information protection.

Concurrently, the liquidity and cross-border nature of virtual currencies further complicate the determination of their legitimacy. Funds involved in cases may rapidly circulate across multiple jurisdictions, with relevant electronic data stored on overseas servers or distributed networks. Traditional evidentiary rules governing domestic evidence collection procedures prove difficult to apply directly in cross-border scenarios. Judicial authorities must engage in international cooperation to obtain evidence from foreign entities, such as requesting user registration information from overseas exchanges or data from communication platforms via letters rogatory. In practice, despite procedural requirements for overseas evidence transfer outlined in the Provisions of the People's Procuratorate on Handling Cybercrime Cases, reliance solely on foreign police investigation reports or statements from Chinese embassies/consulates often proves insufficient. Even when data is obtained, its admissibility assessment, compliance review of extraction procedures, and methods for corroboration with other evidence exceed the scope of current

DOI: 10.54254/2753-7048/2025.BR28074

regulations. Consequently, electronic evidence in virtual currency crimes lacks fixed, applicable rules for establishing its legitimacy in practice [3].

3.1.2. Difficulties in authenticity assessment

The challenge in verifying the authenticity of evidence in virtual currency crimes primarily manifests in electronic evidence, the predominant form. The key to an electronic evidence's admissibility lies in its carrier and the data it contains accurately reflecting the factual truth of a case, thereby proving or disproving a particular fact [4]. Consequently, the authenticity of electronic evidence content necessitates rigorous scrutiny. Scholar Gong Shanyao contends that the current verification of electronic evidence authenticity must be conducted in conjunction with other case evidence through corroboration. This process focuses more on whether the case facts themselves genuinely occurred, constituting an assessment of the case's factual truth [5].

This corroborative model manifests as authenticity verification through uniqueness confirmation, primarily achieved via two pathways: Firstly, authenticity is established through the self-verification of electronic data. Trace data and attribute information generated during the creation and manipulation of electronic data constitute its unique system of characteristic matching points. The greater the number and distinctiveness of these matching points, the stronger the effect of self-corroboration. When the electronic data itself can be corroborated by its own trace data and attribute information, it signifies that the data's inherent characteristics align with its characteristic matching point system, thereby establishing a preliminary determination of its formal authenticity. Secondly, authenticity is established through external cross-verification among evidence. When multiple pieces of evidence mutually corroborate to form a logically coherent and substantively consistent evidentiary framework, each individual piece of evidence within that framework becomes a distinct characteristic matching point. Should the collective characteristic matching points of the entire evidentiary framework align with the relevant circumstances of the criminal facts under investigation, the authenticity of the framework as a whole is validated, thereby reinforcing the authenticity of each individual piece of evidence within it [6].

However, this mode of authenticity determination through corroboration harbours certain vulnerabilities. Under this approach, ascertaining the truth of case facts relies on the verification achieved through the consistency of information. As long as different pieces of evidence exist that reveal the same fact or point to the same information, they are generally regarded as having reached a level of corroboration, thereby validating their authenticity [7]. Consequently, the method of determining case facts shifts from substantive judicial discretion based on experience and logic to a formalistic examination of consistency in the informational content of multiple pieces of evidence. Should this corroboration mechanism be codified in legislation, fact-finding would become solely focused on accumulating corroborative evidence, transforming into a purely objective method of proof. This risks obscuring the inherent risks associated with the formal authenticity of electronic evidence.

Some scholars hold opposing views, arguing that the formal authenticity of electronic evidence is a prerequisite for its admissibility. If electronic evidence is subject to carrier contamination, data tampering, or unclear origins during extraction, storage, or transmission, its probative value cannot be reliably guaranteed even if its content corroborates other evidence [8]. The examination process should therefore consider both formal and substantive dimensions, establishing a triple-verification model encompassing "carrier – data – content." This approach would technically and legally safeguard both the authenticity and probative value of electronic evidence.

DOI: 10.54254/2753-7048/2025.BR28074

3.1.3. Difficulty in establishing relevance

Evidence must demonstrate logical relevance to the facts under consideration, capable of positively or negatively influencing factual determinations. The anonymity inherent in blockchain technology within virtual currencies makes establishing logical connections between "wallet addresses – IP addresses – actors" critical for admissibility. On this point, most scholars concur that in the absence of direct identity links, transaction records on the blockchain or IP addresses alone cannot independently prove a substantive connection between the actor and the crime. This is particularly true when mixing services or anonymous networks are employed, significantly increasing the probabilistic nature of the evidence chain. The relevance of virtual currency evidence should not be confined to technical dimensions alone; rather, it should form a closed chain of evidence through legal presumptions combined with other circumstantial evidence. The author contends that establishing the relevance of evidence in virtual currency crimes requires striking a balance between technical evidence and legal presumptions.

3.2. Excessive costs of adjudicating electronic evidence

Evidence of virtual currency offences is predominantly preserved in electronic form, making the collection, examination, and preservation of such evidence a critical category. Consequently, virtual currency crime cases involve vast volumes of electronic data—including blockchain transaction records, wallet address information, cross-platform communication content, and fund flow records—whose extraction, preservation, and analysis necessitate specialised technical tools and third-party services. In practice, judicial authorities must verify whether original electronic data media have been transferred and preserved, examine whether the electronic data content has been altered, assess the relevance of the electronic data to the case, and determine whether the collection and extraction process can be replicated. Furthermore, complex cases may necessitate multiple instances of data recovery, on-chain tracing, or cross-border investigative assistance, significantly elevating case handling costs. Furthermore, the examination and admissibility of electronic evidence necessitates judges and prosecutors possessing a certain level of technical literacy. Without such expertise, they may struggle to make substantive judgements on technical reports and expert opinions, thereby prolonging litigation cycles and increasing the consumption of judicial resources.

Take the cost of admitting cross-border electronic evidence as an example. Article 77 of the Supreme People's Court's Interpretation on the Application of the Criminal Procedure Law of the People's Republic of China stipulates that courts must verify the source of materials, the provider, the time of provision, the extractor, and the time of extraction. Where evidence from abroad is submitted by a party to the proceedings, it must also be authenticated by the competent authority of the country of origin. Firstly, at the evidence collection stage, as virtual currency transactions frequently involve overseas exchanges or offshore registered entities, investigative authorities often must submit formal requests or utilise indirect channels to obtain user real-name information, IP login logs, or internal transaction records. This process is not only protracted but also incurs substantial costs. Secondly, during evidence conversion and review, cross-border electronic data frequently requires technical reconstruction and evidence adaptation domestically due to format discrepancies, inconsistent hash checks, or incomplete blockchain records. Investigative authorities must engage judicial appraisal institutions with blockchain forensics credentials to perform integrity verification, timestamp alignment, and transaction path reconstruction on the original data, issuing formal expert opinions. Such technical services command substantial fees per instance. Should the funds in question have undergone multiple coin mixes or cross-chain transfers, repeated resource

DOI: 10.54254/2753-7048/2025.BR28074

investment becomes necessary for successive rounds of tracing, resulting in a significant cumulative cost effect. Finally, during the court review stage, judges must also assess the reliability of technical report conclusions based on their relevant professional expertise. For instance, in the Chen Mouzhi money laundering case, [9]the court had to assess whether the Bitcoin on-chain analysis report provided with assistance from the Shanghai Headquarters of the People's Bank of China met evidentiary standards, as this institution is not a statutory judicial appraisal body.

This illustrates that the cost of admitting cross-border electronic evidence extends beyond direct economic and temporal expenditure, being deeply embedded within the complex structure of procedural translation, technical adaptation, and judicial certification. Enhancing the certification costs of electronic evidence without compromising its legitimacy and authenticity represents an urgent evidentiary challenge requiring resolution in the governance of virtual currency crimes.

3.3. Limited technical certification capabilities

The authentication of evidence in virtual currency crimes heavily relies on specialised technical expertise, particularly in areas such as blockchain tracing, on-chain data analysis, and the valuation of encrypted assets. Currently, judicial authorities generally lack personnel with the requisite technical capabilities, and case handlers possess limited understanding of underlying technologies like blockchain and cryptography, making it difficult for them to independently conduct substantive reviews of complex electronic evidence. This internal deficiency in technical capacity means judicial practice remains reliant on external technical support, thereby increasing legal risks and uncertainties in the evidence authentication process.

According to relevant regulations, electronic data authentication must be conducted by institutions possessing statutory accreditation. However, no unified technical standards or operational protocols have yet been established for virtual currency authentication, and institutions with statutory accreditation remain scarce. In practice, tasks such as transaction analysis and fund flow tracing involving virtual currencies are often undertaken by commercial entities, industry associations, or financial institutions lacking judicial authentication qualifications. For instance, in the judgment (2019) Hu 0115 Xing Chu 4419, [10] the Shanghai Headquarters of the People's Bank of China directed commercial banks to analyse virtual currency transactions related to the case and provided analytical conclusions to public security authorities. This activity possessed the core elements of judicial appraisal, yet lacked corresponding legal authorisation and accreditation. It functioned as appraisal in practice but lacked the statutory designation. Such practices of "substituting analysis for formal appraisal" may possess technical expertise, but circumvent procedural norms governing the initiation, execution, and review of formal appraisals. Consequently, the technical reports produced exhibit significant flaws in their evidentiary standing, readily inviting dispute.

Furthermore, the absence of clear standards in virtual currency appraisal, coupled with inconsistent recognition criteria and operational procedures across institutions, further undermines the reliability and credibility of appraisal opinions. This not only increases the difficulty and cost of judicial review but also shifts risks inherent in technical judgements to the court's determination phase, heightening the uncertainty of adjudication outcomes.

3.4. Inconsistent standards for determining the value of virtual currencies

Regarding the valuation of virtual currencies involved in cases, there exists no uniform rule or standard for assessment. Consequently, different cases inevitably employ varying criteria, leading to

DOI: 10.54254/2753-7048/2025.BR28074

significant discrepancies in valuation outcomes. In judicial practice, in the case of "Zhang Guihua, Zhang Xiaohua et al. on charges of fraud" [11], the court directly recognised the amount of RMB defrauded from victims or the amount of RMB used to purchase ETH coins as the fraud amount. The victims' losses were calculated by reference to the average exchange rate between ETH coins and RMB at the time the defendants sold and converted them. Conversely, in the case of "Yan Weijie, Zheng Jiajia, Wang Zhengzhong et al. Organising and Leading Pyramid Scheme Activities" [12], the value of the virtual currency USDT was determined by referencing its price on major international virtual currency trading platforms during the same period. This was then combined with the defendants' confessions and investors' statements, and after conversion and reference, the final criminal amount for the case was established.

Within academic discourse, differing perspectives exist regarding how to determine the value of virtual currencies. Some scholars contend that criminal law protects the actual consideration paid by victims to acquire virtual currency, rather than speculative gains arising from market fluctuations. They argue that adopting market prices at the time of the offence or proceeds-of-crime prices as valuation standards would conflict with the negative assessment of virtual currency-related financial activities under prior legislation. Consequently, they oppose such approaches and propose establishing a progressive valuation framework prioritising "the victim's actual investment costs" as the primary basis [13]. Conversely, other scholars propose using the "proceeds of crime amount" as the valuation benchmark. This view holds that the criminal amount should reflect the actual illegal profits gained by the perpetrator, determined by the sum obtained from selling the virtual currency after committing the crime. This approach better reflects proportionality of punishment and avoids the valuation difficulties caused by market price fluctuations. Additionally, scholar Li Xuejian advocates the "negotiable instrument theory," positing that virtual currencies should be treated as bearer instruments in their entirety. Their speculative market value should fall within the scope of criminal law protection. This approach supports determining the criminal amount based on the market price on trading platforms at the time of the offence, while emphasising the principle of "own risk" to prevent disproportionately lenient or severe sentencing [14]. The author favours the third perspective. Valuing solely based on the initial investment cost fails to accurately reflect the severity of the offence and risks judicial injustice due to volatile price fluctuations. Determining the amount using the market price at the time of the offence better aligns with the principle of proportionality between crime and punishment, while also providing clear and operational criteria for judicial practice.

4. Pathways for refining evidence recognition rules in virtual currency crimes

First, employ diversified methods for analysing evidence chains. Utilising multifaceted approaches to evidence chain analysis can enhance the rules for admitting evidence in virtual currency crimes. However, due to characteristics such as anonymity, proving evidence involving virtual currencies requires comprehensive collection and analysis methods, employing technical means to overcome challenges in admissibility. To this end, judicial authorities should prioritise technologies such as virtual currency chain tracing. Through technological advancement, they can establish the correlation between suspects and criminal acts while clarifying the evidence chain of fund flows. In practice, several enterprises have developed technical tools to track the circulation of virtual currencies involved in cases. For instance, the "Wunian Virtual Currency Crime Early Warning and Tracking Platform" developed by Zhongke Chain Security features functions such as virtual currency traceability and on-chain address anonymity penetration.

DOI: 10.54254/2753-7048/2025.BR28074

Secondly, differentiated approaches to identification should be adopted. The financial circulation processes in virtual currency crimes are complex, involving diverse transfer methods. Judicial practice must employ differentiated identification methods, analysing each case individually. For instance, when dealing with the flow of funds from fiat currency to virtual currency, the key lies in obtaining the fiat currency's fund accounts and transaction details to establish the flow chain of fiat currency and the specific amount of assets involved. Conversely, for the flow of funds between different virtual currencies, evidence such as fixed virtual currency wallet addresses, detailed registration information of wallet addresses, and transaction records of coin-to-coin exchanges and over-the-counter transactions is required to accurately ascertain the specific flow of funds involved between virtual currency accounts.

Thirdly, streamline the methods for proving virtual currency involved in cases. Judicial authorities may appropriately simplify the methods for proving virtual currency involved in cases. Given the transnational nature of evidence in virtual currency crimes, simplified proof methods for cybercrimes may be established to address these challenges. For instance, the comprehensive determination method is a simplified proof approach proposed to tackle the issue of vast volumes of case-related data. Where the flow of virtual currency funds cannot be fully ascertained, the comprehensive determination approach may be adopted. This involves establishing the total amount of criminal proceeds and the pattern of criminal conduct based on representative facts already verified, statistical regularities, and the overall consistency of fund flows, without requiring individual proof for each transaction. Furthermore, where technical or cross-border factors prevent full clarification of certain aspects, the nature of funds and criminal intent may be legally inferred through criminal presumption. This approach must be undertaken while safeguarding the defendant's right to defence, incorporating existing evidence, prevailing transaction practices, and platform regulations.

Fourthly, refine the comprehensive valuation mechanism for virtual currencies involved in cases. Given the absence of unified judicial standards for valuing virtual currencies domestically and their significant price volatility— Prices vary across different trading platforms, and even at the same point in time, significant price differentials exist for mainstream virtual currencies such as Bitcoin and USDT across different exchanges. In response to this characteristic, it is recommended to adopt a comprehensive value assessment mechanism. This involves using the objective market transaction price at the time of the criminal act as a basis, combined with factors such as the timing of the crime, the number of incidents, the actual amount of profit gained by the perpetrator, the nature of the legal interests infringed upon by the criminal act, and the severity of the circumstances. This approach enhances the objectivity and fairness of valuation outcomes, improves litigation efficiency while upholding substantive justice, and flexibly addresses the practical challenges of diverse and volatile virtual currency pricing. It provides judicial practice with a clear and operational pathway for value assessment.

5. Conclusion

The rise of virtual currencies, while facilitating modern life, has also introduced new criminal forms and evidentiary challenges that pose significant tests for criminal justice governance. This paper clarifies the characteristics of virtual currency crimes and analyses the practical difficulties encountered. It endeavours to establish a scientific, integrated system for the evidentiary recognition of virtual currency crimes, thereby resolving the judicial dilemmas in this area and achieving balanced development between technological innovation and the advancement of the rule of law.

DOI: 10.54254/2753-7048/2025.BR28074

References

[1] Huang Guangxiao: Digital Currency, Tsinghua University Press, 2020 edition, p. 2.
[2] Hu Ming: "On the Disposal of Virtual Currency in Criminal Cases, " published in Modern Jurisprudence, Issue 6, 2024, p. 104.
[3] Liu Yang and Li Bingqian: "Evidentiary Challenges and Practical Responses in Virtual Currency-Related Cyber Financial Crimes, " published in Criminological Research, p. 222.
[4] Wang Minyan: "Formation and Authenticity Assessment of Electronic Evidence, " published in Law, Issue 6, 2017, pp. 183-192.
[5] Gong Shanyao: "Clarifying the Functions and Practical Application of Blockchain Evidence Preservation for Digital Evidence, " Journal of Dalian University of Technology, Issue 5, 2023, p. 113.
[6] Wang Qiguo and Wang Xiaoxia: "Corroborative Evidence in Cybercrime", published in People's Procuratorate, Issue 3, 2018, p. 63.
[7] Chen Ruihua: "The Relationship Between Subjective and Objective Elements in Criminal Standards of Proof", published in China Law Review, Issue 3, 2014, pp. 177-195.
[8] Cui Shiqun: "On the Examination of Formal Authenticity of Electronic Data: A Study of Digital Currency Crime Cases, " Journal of Northeastern University, Issue 5, 2023, p. 131.
[9] Criminal Judgment of the Pudong New Area People's Court of Shanghai (2019) Hu 0115 Xing Chu 4419.
[10] Shanghai Pudong New Area People's Court Criminal Judgment (2019) Hu 0115 Xing Chu 4419.
[11] Criminal Judgment (2019) Su 0507 Xing Chu 354 of Xiangcheng District People's Court, Suzhou City, Jiangsu Province.
[12] Anhui Province Hefei Shushan District People's Court Criminal Judgment No. Wan 0104 Xing Chu 39.
[13] Cai Rong: "Reflection and Reconstruction of Rules for Determining the Value of Crimes Involving the Illegal Acquisition of Digital Currency, " published in Legal Application, Issue 3, 2024, p. 102.
[14] Li Xuejian: "On the Criminal Law Characterisation of Cryptocurrency Infringement", Journal of Gansu University of Political Science and Law, 2025, p. 10.