Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD29518

Generative Logic of Virtual Currency Money Laundering Risks and Comprehensive Governance Approaches

Yuyang Liu

School of Government Administration, Shanghai Lixin University of Accounting and Finance, Shanghai, China
221530128@stu.lixin.edu.cn

Abstract. Virtual currencies, owing to their technical characteristics such as anonymity, decentralisation, and instantaneous cross-border flows, have become a "grey area" for money laundering activities. Models such as dark web transactions and coin mixing services further exacerbate the concealment and complexity of these risks. Despite China's prohibitive regulatory policies, underground and cross-border transaction trends have intensified. Compounded by institutional deficiencies—including inconsistent global legal characterisation, inadequate inter-departmental and cross-border coordination, regulatory gaps for emerging business models, and ineffective oversight of Virtual Asset Service Providers (VASPs)—anti-money laundering monitoring and enforcement face severe challenges. This paper analyses typical virtual currency money laundering patterns and regulatory shortcomings based on the risk generation logic of overlapping technological characteristics and regulatory environments. It proposes a comprehensive governance approach: clarifying the "non-financial virtual commodity" nature of virtual currencies and refining the regulatory framework; strengthening VASPs' end-to-end compliance and AML obligations; enhancing traceability capabilities through intelligent monitoring and blockchain analysis; and deepening international and domestic multi-departmental collaboration under the FATF framework. This research holds significant theoretical and practical implications for preventing financial risks and safeguarding economic security.

Keywords: Virtual Currency, Money Laundering Risk, Anti-Money Laundering, Regulatory Framework, Virtual Asset Service Providers (VASPs)

1. Introduction

In recent years, virtual currencies such as Bitcoin and Ethereum have garnered global attention and experienced rapid development due to their decentralised nature, ease of cross-border circulation, and transactional anonymity. They have become an asset allocation choice for some investors and have permeated everyday transactions. However, these characteristics render them a "grey area" for money laundering. Criminals exploit these currencies to circumvent traditional financial oversight, employing methods such as coin mixing and darknet transactions to conceal the origin and nature of funds. This renders money laundering more covert, complex, and transnational, threatening global financial security, economic order, and social stability. Despite heightened regulatory efforts

© 2025 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.LD29518

worldwide, the unique technological architecture of virtual currencies, lagging global regulatory coordination, and evolving money laundering techniques have allowed the associated risks to proliferate. In 2019, the FATF established international anti-money laundering standards for virtual currencies, requiring nations to "either prohibit effectively or regulate effectively". China, having defined virtual currencies as "virtual commodities" since 2013, explicitly classified related activities as illegal financial operations by 2021, establishing prohibitive regulation. However, this prohibition has catalysed underground and cross-border trading trends, presenting new challenges for anti-money laundering monitoring and crime suppression. Systematic research into the risk generation logic and governance pathways is urgently required.

Against this backdrop, this paper dissects the logic of money laundering risk generation, explores its evolutionary pathways, and constructs a comprehensive governance framework. This holds significant theoretical and practical implications for preventing financial risks, maintaining market order, and safeguarding national economic security. The analysis proceeds in three parts: first, introducing the logic of virtual currency money laundering risk generation; second, examining deficiencies in the current virtual currency regulatory framework; and finally, exploring integrated governance pathways to address these risks.

2. Literature review

The emergence of virtual currency money laundering risks stems from the combined effects of technological characteristics and the regulatory environment. Technologically, decentralisation removes transactions from traditional clearing and settlement processes, enabling peer-to-peer exchanges without intermediaries, thereby hindering regulatory intervention. Anonymity conceals transaction participants through encrypted addresses, while coin mixing services further sever address associations, making it difficult to trace suspicious addresses back to real users. Transnational characteristics enable virtual currencies to flow freely across borders via overseas platforms. From a regulatory perspective, while China's prohibition policies mitigate certain risks, they do not entirely ban private transactions. Users privately exchange virtual currencies via platforms like WeChat and Alipay, and the decentralised nature of these transactions increases monitoring difficulties. Internationally, some jurisdictions have not fully implemented FATF standards, creating regulatory loopholes. Money launderers exploit regulatory disparities between countries to transfer funds, exacerbating the cross-border transmission of risks. Most scholars propose governance pathways addressing these risks. Within legal and regulatory frameworks, advocates argue for clarifying the legal nature of virtual currencies. One scholar suggests enacting a Digital Property Act to define them as "non-financial virtual commodities," regulating transactions under "personal overseas investment" scenarios [1]. Others emphasise implementing FATF standards, advocating stringent crackdowns on illegal exchanges under prohibition policies to sever transaction channels [2]. Technologically, central banks should develop "network-wide search systems" to locate illegal platforms, integrating bank fund flows and IP address data to identify suspicious transactions. Concurrently, blockchain address resolution technologies should be explored to link exchange wallets with users' real-name information for fund tracing. Regarding VASP regulation, proposals include incorporating domestic VASPs into anti-money laundering obligations, mandating KYC compliance and suspicious transaction reporting, while establishing an access regime for overseas VASPs to implement approval management for foreign platforms servicing domestic users. Internationally, efforts centre on advancing global regulatory harmonisation through the FATF framework, sharing technical expertise via the Eurasian Anti-Money Laundering Organisation, and strengthening cross-border evidence-gathering cooperation to

DOI: 10.54254/2753-7048/2025.LD29518

obtain AML intelligence from overseas exchanges, thereby enhancing transnational enforcement efficiency.

3. The genesis logic of virtual currency money laundering risks

3.1. The inherent characteristics of virtual currencies provide fertile ground for money laundering risks

3.1.1. Anonymity hinders identity tracing

Virtual currencies operate on blockchain technology, where participants' identities in transactions are typically represented by cryptographic addresses rather than real names and identity information as in traditional financial transactions. Virtual currency protocols do not require participants to provide identity information or undergo identity verification, nor do they generate historical transaction records linked to real-world identities [2]. This anonymity makes it difficult for law enforcement agencies to trace fund flows and transaction entities through account information, as is possible within traditional financial systems, thereby greatly facilitating money launderers in concealing the origins and destinations of funds.

3.1.2. Challenges to traditional regulatory models from decentralised architecture

Decentralisation is the defining characteristic distinguishing virtual currencies from fiat money. At its core, the decentralised architecture of virtual currencies dismantles the centralised control inherent in traditional financial systems, offering a "natural refuge" for money laundering activities across multiple dimensions including transaction structures, power distribution, and regulatory alignment. Virtual currency communities are collectively maintained by nodes distributed across the entire network. Transactions are facilitated through peer-to-peer (P2P) technology, bypassing the clearing and settlement stages inherent in traditional centralised exchanges. Consequently, the operational process does not involve any trusted third parties. This decentralised nature renders traditional centralised oversight ineffective, allowing virtual currency transactions to operate outside the purview of financial regulation.

3.1.3. Ease of cross-border movement and instantaneous transactions

Regarding cross-border ease, virtual currency transactions are inherently borderless. Unlike traditional financial instruments, virtual currencies can facilitate fund transfers or value exchanges globally via the internet, unrestricted by geographical boundaries [2]. Under conventional financial systems, cross-border fund transfers require multiple layers of scrutiny from banks and foreign exchange authorities, adhering to stringent foreign exchange controls. Virtual currencies, however, operate on decentralised blockchain networks, enabling unrestricted transmission between global nodes with only internet access required. Regarding transaction immediacy. Presently, virtual currencies operate via internet trading platforms with round-the-clock trading, involving participants worldwide. This enables the instantaneous movement of virtual currency assets between different nations and trading entities at any time. As evidenced by the virtual currency transaction records of X Coin Network involved in the underground money exchange virtual currency laundering case, virtual currency transactions are remarkably convenient and swift. Criminal proceeds can be laundered within minutes or even tens of seconds. By the time authorities detect leads and initiate investigations, the illicit funds have already been thoroughly laundered [3].

DOI: 10.54254/2753-7048/2025.LD29518

3.2. Typical modus operandi and process of virtual currency money laundering

3.2.1. Fund transfers facilitated through darknet transactions and illicit marketplaces

The dark web differs significantly from the mainstream internet people know, as it encompasses numerous online marketplaces where transactions occur anonymously. Access requires specific software tools, and conducting business on the dark web substantially complicates investigative efforts for law enforcement agencies. The specific process is relatively straightforward: criminals directly purchase virtual currency with illicit proceeds via the dark web, thereby avoiding leaving traces on exchanges. Transactions are typically conducted one-to-one with third parties, after which the funds are withdrawn through legitimate exchanges [4]. The dark web's illicit markets teem with unlawful transactions such as narcotics trafficking and arms dealing, often facilitated by virtual currencies. Money launderers exploit these platforms to convert illicit funds into digital assets, which are then transferred through intricate transactions to other dark web accounts or legitimate exchanges, ultimately achieving capital laundering.

3.2.2. Utilising coin mixing services to obscure fund origins

Coin mixing is a process designed to enhance the privacy of cryptocurrency transactions. On the public ledgers of Bitcoin and other cryptocurrencies, transaction records are visible to all, meaning theoretically anyone can see the sender, recipient, and amount of a transaction. Mixing services complicate the tracing of original funds by blending cryptocurrency from multiple users [5]. Mixers can disrupt transparent transaction records on the blockchain, obscuring the funds' original source. Furthermore, some money launderers may utilise mixers to disperse funds across multiple wallets, increasing the difficulty of tracing.

3.2.3. Innovative money laundering models through emerging formats such as Non-Fungible Tokens (NFTs)

The anonymity mechanisms and cross-border liquidity inherent in NFT transactions provide covert pathways for illicit funds. Money laundering may be concealed through fabricated transactions, price manipulation, or artificially inflated NFT valuations [6]. Money launderers construct intricate networks of related transactions, tightly linking NFT dealings with other legitimate or illicit business activities to obscure fund origins and flows. On one hand, they utilise shell companies or affiliated entities to participate in NFT minting, issuance, and trading. These shell companies appear to operate normally while secretly undertaking the task of transferring illicit funds.

4. Current state of virtual currency money laundering systems and regulation

4.1. Lagging and ambiguous legislation

In China, virtual currency-related business activities have been explicitly defined as illegal financial activities. However, the legal attributes of virtual currencies themselves remain unclear and undefined. This uncertainty in legal classification directly hinders the precise formulation of anti-money laundering rules within China's virtual currency sector and impedes the effective implementation of existing anti-money laundering measures. Within virtual currency transaction scenarios, the rights and obligations of involved parties—including transacting individuals and platforms—lack clear legal foundations for delineation. This creates significant obstacles for law

DOI: 10.54254/2753-7048/2025.LD29518

enforcement agencies. When authorities seek to trace fund flows in virtual currency money laundering cases, identify responsible parties, and pursue legal accountability, they frequently encounter difficulties due to unclear jurisdictional boundaries, thereby impairing investigative efficiency and outcomes.

Globally, nations have yet to establish uniform standards defining the legal nature of virtual currencies, exhibiting significant disparities and numerous ambiguities. Different jurisdictions categorise virtual currencies differently: some recognise them as property, while others deny them legally recognised monetary attributes. This leads to uncertainty in applying relevant criminal charges (such as illegal business operations, money laundering, or fraud) under national criminal codes [7]. These international legal discrepancies pose severe challenges in cross-border virtual currency money laundering cases. Differing legal classifications of virtual currencies across jurisdictions result in divergent legal provisions and enforcement standards, hindering effective international judicial cooperation. Criminals exploit these legal gaps to transfer laundered virtual currency funds between countries and regions, evading national law enforcement sanctions and substantially increasing the difficulty of combating cross-border virtual currency money laundering. Concurrently, most existing global anti-money laundering regulations are designed based on the operational models and characteristics of traditional financial systems. As an emerging domain, virtual currencies exhibit fundamental differences from traditional finance in transaction patterns and capital flow mechanisms. Consequently, conventional AML frameworks struggle to fully accommodate the virtual currency sphere, suffering from regulatory gaps and mismatched provisions that fail to effectively cover diverse virtual currency money laundering scenarios.

Presently, China has established an anti-money laundering legal framework centred on the Anti-Money Laundering Law, underpinned by the Criminal Law, and supplemented by multi-tiered normative legal documents. This system has played a vital role in anti-money laundering efforts within the traditional financial sector.

However, within the governance of virtual currency money laundering, this legal framework remains imbalanced. From a legal applicability perspective, while the existing Criminal Law can effectively cover virtual currency money laundering activities, the Anti-Money Laundering Law as the primary legislation and related digital property legislation remain incomplete [1]. The Anti-Money Laundering Law has not established specialised anti-money laundering regulations tailored to the characteristics of virtual currencies, while digital property legislation has not clarified the legal status of virtual currencies or the associated rights and obligations. This results in a lack of comprehensive, systematic preliminary legal support for virtual currency anti-money laundering efforts, limiting the applicability and effectiveness of the overall legal framework within the virtual currency domain.

4.2. Inadequacies in cross-departmental and cross-border regulatory coordination mechanisms

Virtual currency transactions span multiple sectors and departments, including finance, cyberspace administration, and public security. However, current regulatory coordination mechanisms between departments remain inadequate, plagued by issues such as poor information sharing and unclear delineation of responsibilities. This hinders the formation of effective synergies among departments when monitoring virtual currency transactions and combating money laundering activities. Regarding cross-border regulation, significant differences in regulatory policies and standards across countries and regions create substantial difficulties for international regulatory coordination and cooperation. The cross-border nature of virtual currency transactions enables criminals to exploit

DOI: 10.54254/2753-7048/2025.LD29518

regulatory disparities between jurisdictions, facilitating the transfer of funds across virtual currency trading platforms in different countries and regions to evade regulatory enforcement.

4.3. Regulatory gaps in emerging sectors such as Decentralised Finance (DeFi) and Decentralised Exchanges (DEX)

DeFi and DEX represent rapidly evolving new business models within the virtual currency sector. However, regulation of these emerging sectors currently lags significantly behind. DeFi platforms utilise smart contracts to decentralise financial services, enabling users to conduct lending, trading, and other operations without traditional financial intermediaries. Yet, the absence of effective oversight renders these platforms vulnerable to exploitation by money launderers.DeFi cryptocurrency pyramid schemes present particular challenges in enfos.rcement due to their DApp-based presentation, hierarchical structures established through cryptocurrency addresses and token transfers, smart contract-driven operational logic, and data storage on blockchain network [8]. Similarly, DEX present regulatory challenges, as their transaction processes rely on no centralised authority and store transaction data in a decentralised manner, making it difficult for regulators to conduct comprehensive, real-time monitoring and scrutiny of trading activities.

4.4. Inadequate regulation of Virtual Asset Service Providers (VASPs)

Virtual asset services provided by VASPs are inherently cross-border in nature. When customer identification and verification measures fail to adequately address anonymity issues arising from non-face-to-face business characteristics or opaque transactions, the virtual asset products and services offered by VASPs present heightened risks of money laundering and terrorist financing. Correspondingly, tracing related funds and identifying counterparties becomes significantly more challenging [9]. VASPs, including virtual currency trading platforms and wallet service providers, play a pivotal role within the virtual currency trading ecosystem. However, current oversight of VASPs exhibits numerous deficiencies. Some VASPs, driven by profit motives, apply lax standards in user identity verification and transaction monitoring.

5. Comprehensive approach to virtual currency money laundering risks

5.1. Refining legal and regulatory frameworks

Legal and regulatory frameworks constitute the fundamental institutional safeguards against virtual currency money laundering risks, with their sophistication directly impacting governance efficacy. When defining the legal status of virtual currencies, it is imperative to transcend current "ambiguous formulations" by integrating their technical characteristics and financial attributes to explicitly position them as "non-financial virtual commodities". This classification acknowledges their civil protection status as digital assets while denying their function as legal tender, thereby providing a unified basis for case characterisation and asset disposal in judicial practice. Concurrently, regulatory responsibilities must be delineated to establish a supervisory system led by the central bank, with coordinated oversight from public security, cyberspace administration, foreign exchange management, and other relevant departments. Specifically, the central bank should oversee virtual currency transaction monitoring and anti-money laundering rule formulation, while public security authorities handle criminal investigations and asset recovery. Cyberspace administration departments should undertake technical identification of illegal platforms to prevent regulatory vacuums or duplication. International regulatory cooperation must address cross-border barriers,

DOI: 10.54254/2753-7048/2025.LD29518

centred on the FATF framework, to promote regulatory cooperation agreements with Belt and Road countries and regions with active virtual currency trading. VASPs establish a cross-border virtual currency transaction information-sharing platform to enable real-time exchange of data including suspicious transaction leads, user identity information, and VASP compliance records. For overseas VASPs providing services within China, implement a "registration-based access + dynamic monitoring + accountability for violations" mechanism, requiring them to establish compliant representative offices domestically.Unregistered entities are prohibited from conducting business operations. Violators shall be subject to financial restrictions implemented in collaboration with international organisations.

5.2. Strengthen the anti-money laundering obligations and responsibilities of Virtual Asset Service Providers (VASPs)

As pivotal hubs in virtual currency transactions, the compliance standards of VASPs directly impact the effectiveness of anti-money laundering risk prevention. Regulatory oversight must be strengthened throughout the entire lifecycle, encompassing entry, operations, and exit. During the entry phase, implement a rigorous approval system requiring VASPs to submit comprehensive AML policy proposals, technical security safeguards, and risk management protocols.VASPs should Conduct substantive reviews of registered capital, technical team qualifications, and internal control systems, granting registration permits only to compliant entities to curb the proliferation of illegal platforms at source.

The implementation of the Know Your Customer (KYC) framework necessitates moving beyond conventional identity verification methods to adopt a “multi-tiered identity verification” approach. Basic verification requires users to provide identification documents and facial recognition data. Enhanced verification for users conducting high-value transactions additionally mandates submission of proof of funds origin (such as bank statements or tax clearance certificates) and occupational background documentation. Institutional users must undergo scrutiny of their business licences, beneficial ownership details, and intended use of funds.

Transaction record retention and suspicious transaction reporting systems must achieve standardisation and timeliness. VASPs should employ tamper-proof storage technologies to comprehensively preserve transaction records, user identity information, risk assessment reports, and other materials, ensuring data remains accessible to regulatory authorities at any time. VASPs establish rapid reporting channels for suspicious transactions. Suspicious transactions detected must be reported to the Anti-Money Laundering Monitoring and Analysis Centre within 24 hours, accompanied by transaction details, risk analysis explanations, and other supporting documents. Cases suspected of criminal activity must be immediately referred to public security authorities, with full cooperation provided for investigation and evidence collection.

5.3. Employ technological means to enhance monitoring and traceability capabilities

The development of virtual currency AML monitoring systems must encompass diverse transaction scenarios. Differentiated monitoring modules should be configured according to the risk characteristics of various transaction models to precisely address money laundering vulnerabilities in each context: For centralised trading platforms, where user account operations and fund flows are centralised, money laundering often manifests as abnormal account logins or concentrated fund transfers. Prioritising monitoring of such behaviours enables timely detection of account compromise or non-compliant fund transfers. For DeFi platforms, which operate via smart contracts

DOI: 10.54254/2753-7048/2025.LD29518

with high transaction anonymity, activities like "high-frequency lending and repayment" and "fund consolidation across multiple addresses" readily become money laundering conduits. Developing smart contract auditing tools that automatically identify these characteristics enables rapid identification of risky contracts. Activating transaction suspension functions for anomalous contracts directly halts further circulation of laundered funds.By shifting investigative approaches, broadening investigative perspectives, and leveraging blockchain's historical and real-time transaction data to screen critical investigative leads, authorities have transitioned from reactive tracking to proactive detection. This enables precise countermeasures against the evolving tactics and tools employed in virtual currency-related crimes [10]. Regarding NFT transactions, their subjective valuation and susceptibility to manipulation make false transactions and value manipulation common money laundering tactics. Establishing price monitoring models that compare transactions against historical prices and market valuations of similar NFTs can effectively identify trades deviating from reasonable value ranges, thereby curbing the transfer of illicit funds through NFT speculation. Furthermore, considering the constant evolution of money laundering methods, the system must possess self-learning capabilities. By analysing transaction patterns from solved cases through deep learning, the system can grasp more patterns of money laundering behaviour, thereby continuously optimising risk identification algorithms. This ultimately enhances adaptability to emerging money laundering models, ensuring monitoring capabilities keep pace with evolving techniques.

For highly concealed money laundering methods such as darknet transactions and coin mixing services, which present significant technical barriers and traceability challenges, single-technology approaches prove insufficient. A dual-pronged defence of "technical countermeasures + source-based suppression" is therefore essential: Regarding technical countermeasures, collaborate with cybersecurity firms to develop dark web monitoring systems. Utilising Tor node analysis and keyword scraping technologies, these systems can penetrate the anonymity shield of the dark web to locate communication trails between cryptocurrency trading platforms and money laundering syndicates, providing critical data support for subsequent investigations. Regarding source suppression, recognising that "instant dial-up IPs", "anonymous wallets", and "coin mixing tools" form the core technical infrastructure for such laundering methods, an illegal technical services blacklist should be established. Precise targeting of enterprises and individuals providing these services—through seizing relevant servers and domains while pursuing legal accountability—can sever the technical supply chain for money laundering at its roots, substantially reducing the feasibility of covert laundering operations.

6. Conclusion

The emergence of virtual currency money laundering risks stems from the convergence of its technological characteristics and regulatory deficiencies. Anonymity hinders identity tracing, decentralisation evades traditional oversight, and instant cross-border flows transcend geographical constraints. These factors, compounded by diverse models such as darknet transactions, coin mixing services, and fictitious NFT trades, create fertile ground for risk proliferation. Furthermore, lagging and ambiguous legislation, inadequate inter-departmental and cross-border coordination, regulatory gaps for emerging sectors, and ineffective oversight of Virtual Asset Service Providers (VASPs) amplify these risks. Addressing these risks requires the establishment of a four-dimensional governance framework that includes institutional, entity, technological, and collaborative dimensions. First, it is essential to clarify the status of virtual currencies as "non-financial virtual commodities" and define regulatory responsibilities to improve legal and supervisory frameworks. Second, strengthening the anti-money laundering obligations of VASPs through end-to-end approval

DOI: 10.54254/2753-7048/2025.LD29518

and compliance reviews will bolster industry defenses. Third, employing technological solutions such as blockchain analysis and intelligent monitoring systems can address challenges related to anonymity tracking and emerging business model supervision. Lastly, deepening international collaboration within the FATF framework, while coordinating efforts across domestic departments and society, will help create a unified governance approach.Only through multidimensional collaborative efforts can virtual currency money laundering risks be effectively curbed, safeguarding financial security and economic order.

References

[1] Lu Jianping, Liu Jia. (2025) Governance Solutions for Virtual Currency Money Laundering Crimes: A Risk-Based Analysis [J]. Beijing Social Sciences, (02): 105-116.
[2] Wu Yun, Xue Hongjiao, Zhu Wei, et al. (2021) Research on Virtual Currency Money Laundering: Inherent Risks, Typology Analysis and Regulatory Responses [J]. Journal of Financial Regulation Research, (10): 1-19.
[3] He Jie. (2024) Regulatory Countermeasures for Cross-Border Virtual Currency Flows [J]. The Banker, (09): 134-137.
[4] Wang Yingjie. (2025) Analysis of Virtual Currency Money Laundering Crimes and Governance Countermeasures [J]. Hebei Legal Vocational Education, 3(06): 45-50.
[5] Wang Jiaxin, Mao Qianang, Yan Jiaqi, et al. (2025) Review of Regulatory Technologies for Blockchain Mixing [J/OL]. Computer Engineering, 1-19 .
[6] Zhang Chen. (2025) Research on Financialisation Risks of Non-Fungible Tokens (NFTs) and Their Prevention Pathways [J]. Science and Finance, (05): 51-56+66.
[7] Wu Yingjia. (2025) Criminal Regulation of Cross-Border Virtual Currency Transfer Crimes: Evolution, Challenges and Responses [J/OL]. Accounting Friend, 1-8 .
[8] Zhang Yunfei, Chen Liang. (2025) Investigative Methods and Governance Strategies for DeFi Virtual Currency Pyramid Scheme Crimes [J]. Journal of the People's Police University of China, 41(06): 23-29+63
[9] Li Sijia. (2022) Anti-Money Laundering Legal Liability of Virtual Asset Service Providers [J]. Hebei Jurisprudence, 40(05): 164-191.
[10] Xie Ling, Sun Meicheng. (2023) Fund Flow Investigation Strategies Based on DeFi Crime Typology Analysis [J]. Journal of the People's Public Security University of China (Natural Science Edition), 29(02): 85-93.