International Journal of Business, Law, and Education
Publisher: IJBLE Scientific Publications Community Inc.
IJBLE
Volume 7, Number 2, 2026
https://ijble.com/index.php/journal/index

Reconstructing Mutual Legal Assistance for Digital Financial Crime: Addressing the Sovereignty Paradox and Web3 Disruption

Aida Ardini[1], Usman Manor[2]
[1]Faculty of Law, Universitas Prima Indonesia, PUI-PT Criminal Law and Green Economy
[2]University of Indonesia Coordinating Ministry of Human Development and Culture Affairs
Email: aidardini@unprimdn.ac.id [1], manorusman@gmail.com [2]

ABSTRACT
The expansion of cross-border digital finance within the ASEAN Economic Community has increased both legitimate financial integration and exposure to digitally enabled financial crime involving blockchain, virtual assets, decentralized finance (DeFi), and Web3 infrastructures. These developments create a legal tension between borderless, rapidly moving digital activity and mutual legal assistance (MLA) mechanisms that remain primarily state-centred and territorially organized. This study assesses the normative adequacy of the 2004 ASEAN Treaty on Mutual Legal Assistance in Criminal Matters for Web3-related digital financial crime and develops a model for legal reconstruction. Using normative and prescriptive legal research, the study combines statutory, conceptual, comparative, and law-reform approaches with Critical Legal Studies, regulatory-lag analysis, and policy-oriented legal research. The analysis identifies three principal constraints: formalistic application of dual criminality, time-sensitive reliance on Central Authority procedures, and a territorial sovereignty paradigm that may be poorly aligned with distributed digital evidence and rapidly transferable virtual assets. The study proposes a framework of regional juridical reciprocity comprising secure electronic mutual legal assistance (e-MLA), a substantive approach to dual criminality, greater convergence on core digital-financial offences and investigative standards, and stronger inter-agency coordination with proportionate emergency asset-preservation mechanisms. The proposed model does not displace state sovereignty; rather, it seeks to make sovereignty operationally compatible with timely, rights-respecting, and interoperable cross-border enforcement in the Web3 era.

Keywords:
Mutual Legal Assistance; Digital Financial Crime; ASEAN; Web3; Sovereignty; Cross-Border Law Enforcement

DOI. https://doi.org/10.56442/ijble.v7i2.1556

INTRODUCTION

Digital transformation has fundamentally reshaped the architecture of modern finance. Advances in high-speed connectivity, artificial intelligence, cloud computing, big data, and distributed ledger technology have produced an increasingly integrated cross-border financial ecosystem (Goyal et al., 2026; D. Zhao et al., 2023). Digitalization no longer functions merely as an auxiliary layer of conventional finance; it increasingly enables economic activity to operate through infrastructures that are partially independent of traditional financial intermediaries (Azeez N. P. et al., 2022). These developments enhance transaction efficiency, broaden financial inclusion, and accelerate capital mobility, while simultaneously creating legal challenges concerning the misuse of digital financial technologies.

Blockchain technology is central to this transformation and constitutes an important technological foundation of the Web3 ecosystem (Sarkhosh et al., 2025). In contrast to Web2 architectures that typically depend on centralized platforms for data and transaction management, many Web3 applications employ distributed networks and cryptographic consensus mechanisms. Such infrastructures enable peer-to-peer transactions and have supported the development of crypto-assets, smart contracts, decentralized finance (DeFi), non-fungible tokens (NFTs), and decentralized autonomous organizations (DAOs) (Lekhi, 2023; Sarathy, 2026). Financial digitalization has therefore evolved beyond payment-system modernization into a transnational economic infrastructure whose operations may extend across multiple national jurisdictions (Y. Zhao & Cheng, 2024).

The same features that support innovation also create opportunities for financial misconduct. Permissionless access, pseudonymous participation, cross-jurisdictional transactions, and the absence of a single controlling intermediary can complicate attribution, supervision, and enforcement (Sarkhosh et al., 2025). Criminal actors may exploit blockchain-based infrastructures to conceal beneficial ownership, transfer assets rapidly across jurisdictions, and misuse DeFi protocols in connection with money laundering, terrorism financing, investment fraud, ransomware, market manipulation, and other forms of cyber-enabled financial crime. These developments contribute to a shift from predominantly territorial offending toward network-based criminal activity that is more difficult to address through conventional enforcement mechanisms (Wu et al., 2023).

The cross-border structure of blockchain transactions intensifies this difficulty because a single case may involve offenders, victims, virtual assets, service providers, and electronic evidence located in several jurisdictions at the same time. This creates a sovereignty paradox: criminal jurisdiction remains largely organized around territorial state authority, whereas digital transactions can occur across borders with limited regard for geographic boundaries (Situmeang et al., 2026). Investigators may therefore encounter obstacles when seeking electronic evidence, tracing assets, freezing or seizing virtual assets, and recovering proceeds located outside their domestic jurisdiction. Divergent criminal laws, evidentiary rules, procedural requirements, and legal-assistance practices can further delay enforcement responses to rapidly moving digital assets (Dolgieva, 2023).

Against this background, international legal cooperation is not merely supplementary but essential to effective transnational enforcement. Mutual legal assistance (MLA) provides a formal framework through which states may assist one another in obtaining evidence, examining witnesses, tracing and confiscating assets, and facilitating the execution of judicial measures (Putri et al., 2025). Yet MLA systems were largely designed around conventional forms of criminality and may be poorly matched to decentralized infrastructures, real-time asset transfers, and cryptographically secured data (Krasniqi & Stefanova, 2024). The legal challenge is therefore to preserve legitimate sovereignty and due-process safeguards while improving the capacity of cross-border cooperation to respond to digitally mediated financial crime.

This challenge is particularly salient in Southeast Asia. The expansion of digital financial services, e-commerce, internet connectivity, and crypto-asset use has accompanied deeper economic integration under the ASEAN Economic Community (AEC), which has increased the movement of goods, services, investment, and capital across borders (Ishikawa, 2021). Greater integration also enlarges the operational space for transnational digital financial crime (Simanjuntak et al., 2022). Crypto-asset laundering, digital investment fraud, business email compromise, ransomware, terrorism financing through virtual assets, and the misuse of DeFi platforms may involve actors and financial flows distributed across several ASEAN jurisdictions. Accordingly, national enforcement alone is insufficient; effective responses require legal mechanisms capable of bridging differences among domestic legal systems.

ASEAN states sought to strengthen such cooperation through the Treaty on Mutual Legal Assistance in Criminal Matters, adopted in 2004 (ASEAN MLA Treaty). The Treaty provides a regional legal basis for assistance involving evidence gathering, witness examination, searches and seizures, and the tracing and recovery of criminal proceeds (Arifin et al., 2024; Putri et al., 2025). It represented an important step beyond reliance on ad hoc diplomatic channels. Nevertheless, its normative architecture was developed within a predominantly territorial and state-centred model of criminal justice, raising questions about its adequacy for contemporary digital financial crime.

The Treaty predates the widespread use of blockchain, virtual assets, smart contracts, and DeFi. Consequently, it does not expressly address many operational problems now associated with blockchain-based electronic evidence, rapid virtual-asset transfers, assets distributed across multiple wallets or networks, or cooperation with virtual asset service providers. The dual criminality requirement may also create friction where ASEAN member states regulate crypto-assets, DeFi activities, and novel digital offences differently (L. S. F. Lin, 2025). Variations in institutional capacity, regulatory development, and technological readiness further complicate the coordination of cross-border enforcement (Nguyen & Ngo, 2026).

Existing scholarship addresses several components of this problem but rarely integrates them. Studies of MLA generally emphasize evidence exchange, cross-border investigation, and asset recovery (Vermeulen & Kusak, 2023), while related research examines anti-money-laundering and counter-terrorism-financing standards. By contrast, scholarship on blockchain and virtual assets often focuses on regulation, financial governance, consumer protection, or the supervision of virtual asset service providers (López Rodríguez, 2025). Research on Web3 and DeFi remains heavily concentrated in technology, cybersecurity, and digital-economy fields, leaving their implications for international legal-assistance mechanisms comparatively underdeveloped (Bayan et al., 2025).

The literature is therefore fragmented. MLA research commonly proceeds from conventional assumptions about territorial jurisdiction and identifiable intermediaries, whereas blockchain and Web3 scholarship tends to emphasize technological innovation and domestic regulatory challenges (Badkul et al., 2025). The interaction between these two domains—specifically, how decentralized digital infrastructures affect the normative design of international legal cooperation—remains insufficiently examined. This gap is particularly significant in ASEAN because member states differ in legal traditions, regulatory maturity, digital readiness, and approaches to virtual assets (Eg Tan & Ang, 2022).

Three specific gaps follow from this fragmentation. First, limited scholarship directly evaluates the normative adequacy of the 2004 ASEAN MLA Treaty for Web3-related digital financial crime. Second, insufficient attention has been given to how dual criminality, jurisdiction, and evidence-exchange rules should operate when transactions and evidence are decentralized and cross-border. Third, Critical Legal Studies (CLS) has rarely been used to examine the structural gap between technological change and the legal frameworks governing regional cooperation. This study addresses these gaps by critically assessing the Treaty's normative capacity and by developing a reconstruction model for MLA cooperation that is more responsive to Web3-based financial crime.

The study proceeds from the proposition that technological change affects not only criminal modus operandi but also the conditions under which states exercise cross-border enforcement authority. The central problem is therefore not limited to whether the ASEAN MLA Treaty is implemented correctly; it concerns whether the Treaty's underlying normative design remains adequate for technologies that evolve faster than formal legal reform. Legal reconstruction is accordingly understood here as more than procedural modernization. It involves reconsidering the conceptual foundations of international legal cooperation in a decentralized digital financial environment.

Critical Legal Studies provides the principal theoretical lens for this inquiry because it enables scrutiny of the relationship among legal doctrine, institutional power, and social change (Brison, 2018). CLS challenges the assumption that law operates as a fully neutral and self-contained system, emphasizing instead the political, economic, and institutional conditions that shape legal rules (Vincentius Setyawan & Bariah Safrut, 2025). In this study, CLS is used to examine the extent to which the MLA regime retains assumptions associated with conventional crime—such as territoriality, identifiable actors, and centralized institutional control—and whether those assumptions remain defensible in a decentralized and pseudonymous digital environment.

The analysis is further informed by the concept of regulatory lag, understood as a mismatch between the pace of technological development and the capacity of legal institutions to formulate and implement appropriate norms and enforcement mechanisms (Aspray & Doty, 2023). In the Web3 context, such lag may appear in rules governing blockchain-based evidence, the identification of pseudonymous actors, the tracing of assets moving across multiple networks, and coordination among authorities dealing with decentralized financial protocols (Krasniqi & Stefanova, 2024). These limitations may weaken MLA processes that continue to depend on bureaucratic procedures and territorially bounded jurisdiction while digital assets and evidence move at substantially greater speed (Gavaghan & Charlesworth, 2025).

A policy-oriented legal research perspective complements this critical framework by treating legal analysis as a basis for developing institutional and regulatory solutions (Demir, 2020; Gerrard, 2020). The study therefore examines both law as it is and the legal arrangements that may be required to address emerging digital-financial risks (Khan et al., 2025). Its prescriptive component considers electronic mutual legal assistance (e-MLA), a substantive interpretation of dual criminality, greater regional harmonization of core digital-financial offences, and stronger technology-supported coordination among competent authorities.

On this basis, the study asks two related questions: to what extent is the normative architecture of the 2004 ASEAN MLA Treaty adequate for Web3-based digital financial crime, and what form of legal reconstruction could better reconcile state sovereignty with the need for timely cross-jurisdictional enforcement? These questions treat adaptability as a core criterion of international legal cooperation, alongside legality, due process, and respect for national jurisdiction.

The study lies at the intersection of international criminal law, cyber law, digital-financial governance, and regulatory transformation. Unlike research that examines MLA primarily as a procedural mechanism (James & Gladyshev, 2016) or blockchain principally as a technological and domestic regulatory issue (McGregor, 2019), this article integrates both domains within a single analytical framework. Its principal contribution is a reconstruction model for ASEAN MLA grounded in CLS, regulatory-lag analysis, and policy-oriented legal research, with the aim of making regional cooperation more responsive to Web3-related financial crime.

Accordingly, the study has three objectives: (1) to assess the normative adequacy of the 2004 ASEAN MLA Treaty in relation to Web3-based digital financial crime; (2) to identify doctrinal and institutional constraints that may impede timely cross-border cooperation; and (3) to formulate a reconstruction model that strengthens regional legal cooperation while preserving legitimate sovereignty and due-process safeguards. The study is intended to contribute both to legal scholarship on transnational digital crime and to policy debates on the future design of ASEAN mutual legal assistance.

METHOD

This study employs normative and prescriptive legal research to assess the capacity of the 2004 ASEAN Treaty on Mutual Legal Assistance in Criminal Matters to address blockchain-enabled digital financial crime, decentralized finance (DeFi), and the broader Web3 ecosystem (Irawan et al., 2025). The inquiry does not attempt to measure implementation outcomes empirically. Instead, it evaluates the coherence and adequacy of the applicable legal framework and develops a reform model directed toward law as it ought to be. This design is appropriate because the central research problem concerns the compatibility between the Treaty's normative assumptions and the changing structure of transnational digital crime.

Four complementary legal approaches are used: statutory, conceptual, comparative, and law-reform approaches. The statutory approach examines relevant international, regional, and domestic legal instruments, including the ASEAN MLA Treaty, the United Nations Convention against Transnational Organized Crime (UNTOC), the United Nations Convention against Corruption (UNCAC), Financial Action Task Force (FATF) standards, and rules concerning money laundering, virtual assets, and cybercrime in ASEAN member states (Bisset, 2023). The conceptual approach examines doctrines of sovereignty, dual criminality, jurisdiction, asset recovery, and regulatory lag (Zanghellini, 2017). The comparative approach considers selected international practices, including mechanisms developed in the European Union such as the European Investigation Order, Eurojust cooperation, and electronic legal-assistance initiatives (Alshaer et al., 2024; Putri et al., 2025). The law-reform approach is then used to formulate institutional and doctrinal reforms responsive to financial-technology developments and cross-jurisdictional enforcement needs (El Harras & Salahddine, 2025; Sukardi, 2022; Zagaris, 2019).

The analytical framework combines Critical Legal Studies, regulatory-lag analysis, and policy-oriented legal research. CLS is used to interrogate the assumptions underlying territorial sovereignty, dual criminality, and centralized decision-making through national Central Authorities (Arifin et al., 2024). Regulatory-lag analysis explains the temporal and institutional mismatch between fast-moving digital-financial technologies and slower processes of legal adaptation (Alsmadi & Alshehadeh, 2025). Policy-oriented legal research provides the prescriptive basis for translating those findings into feasible reform proposals (Demir, 2020; Gerrard, 2020).

The legal materials comprise primary, secondary, and tertiary sources collected through library-based legal research. They include treaties, legislation and regulations, official documents and institutional reports, judicial or administrative materials where relevant, and scholarly literature indexed in databases such as Scopus, Web of Science, HeinOnline, SpringerLink, and JSTOR. The materials are analyzed qualitatively (Mitchell, 2023) through five stages: identification and classification of applicable norms; grammatical, systematic, and teleological interpretation; comparative assessment of selected international practices; critical evaluation of normative and institutional constraints; and formulation of a prospective ASEAN MLA reconstruction model. This process is designed to produce prescriptive legal arguments rather than empirical estimates of enforcement performance.

RESULTS AND DISCUSSION

1. Reframing Contemporary Financial Crime: From Physical to Networked Jurisdiction

Digital transformation has altered not only the instruments of economic exchange but also the structure of financial crime. Conventional economic offences are typically conceptualized as conduct occurring within identifiable physical settings, involving ascertainable actors, objects, evidence, and jurisdictions (Alkhaldi, 2026; Troyanovskiy, 2021). Blockchain, virtual assets, distributed ledgers, smart contracts, and Web3 infrastructures challenge these assumptions because relevant conduct may occur through decentralized and cross-jurisdictional networks (Gómez-Quintero et al., 2024; L. S. F. Lin, 2025). Contemporary financial crime can therefore be less dependent on a specific intermediary or geographic location and more dependent on distributed technological infrastructures.

This shift has direct implications for international legal cooperation. Cross-border criminal-law mechanisms, including the ASEAN MLA Treaty, remain strongly influenced by a territorial model in which states exercise jurisdiction principally within defined geographic boundaries (Ryngaert, 2025; Talmon, 2022). Within that model, locus delicti, evidence collection, asset confiscation, and the execution of judicial measures are ordinarily linked to a particular territory. Digital financial crime weakens this correspondence between physical space and legal space, contributing to what has been described as the deterritorialization of criminal activity (Cubides-Cardenas et al., 2025; Qin, 2026).

a. Pseudonymity and Cyber-Laundering

The changing architecture of finance also affects the mechanisms through which illicit transactions are conducted. Conventional money laundering commonly involves regulated financial institutions that generate administrative records through Know Your Customer (KYC), Customer Due Diligence (CDD), and suspicious-transaction reporting requirements (Jindal et al., 2022; Kristian et al., 2022).

Blockchain-based assets, DeFi protocols, and smart contracts can facilitate peer-to-peer transactions without reliance on conventional financial intermediaries (Palurovic & Gross, 2026; Salami, 2021). This changes the relationship among actors, assets, and jurisdictions and can reduce the practical utility of investigative models centred on identifiable financial institutions and transaction locations.

A central difficulty is pseudonymity. Although many blockchains provide transparent and persistent transaction records, wallet addresses do not necessarily disclose the legal identity or beneficial owner behind a transaction. Cryptographic tools and privacy-oriented network architectures may therefore make attribution more difficult even where transactional data remain visible (Bellaby, 2018; Liu, 2025). Investigations consequently require more than conventional account tracing; they may depend on blockchain analytics, transaction metadata, off-chain records, and the correlation of multiple sources of electronic evidence.

Tracing can be further complicated by privacy-oriented technologies and transaction-obfuscation techniques. Privacy coins, mixing services, chain hopping, and cross-chain bridges may fragment transaction trails across different networks and increase the analytical burden on investigators (Cinal et al., 2026). These practices are associated with forms of cyber-laundering in which the concealment and movement of criminal proceeds occurs substantially within digital infrastructures rather than through the physical transfer of funds (De Sanctis, 2019). The classic stages of placement, layering, and integration may therefore overlap or occur in compressed sequences, making the origin and destination of assets harder to establish in a timely manner.

DeFi adds another layer of complexity because functions such as token swaps, lending, liquidity provision, and cross-chain transfers may occur through protocols that do not resemble conventional financial institutions. Where no clearly identifiable intermediary is subject to KYC, CDD, or reporting obligations, traditional anti-money-laundering strategies that depend on regulated gatekeepers may be less effective (Sukardi, 2022). Digital financial crime thus raises a governance problem as well as a technological one: the regulatory system must respond to financial activity that can be coordinated through software, dispersed actors, and multiple jurisdictions.

These characteristics affect the normative operation of MLA. Requests for cross-border assistance generally need to identify, with sufficient specificity, the persons, assets, evidence, or investigative acts concerned. In digital financial cases, that threshold may be difficult to satisfy when attribution remains uncertain and assets can move across multiple networks before an assistance request is processed. Requested states may likewise face difficulties where the relevant object is not a conventional bank account or tangible asset but distributed electronic data, wallet information, or virtual assets associated with several jurisdictions (L. Lin et al., 2023).

The investigative logic consequently expands from ‘follow the money’ toward ‘follow the data’ and, in some cases, ‘follow the algorithm’ (Manavadaria et al., 2025). Effective tracing may require analysis of wallet addresses, transaction metadata, smart-contract code, private-key control, and interactions across blockchain networks. From a CLS perspective, this exposes a structural assumption embedded in conventional MLA: that the identity of the suspect, the location of evidence, and the situs of assets can be linked to a clearly defined national jurisdiction. Web3-related financial crime makes that assumption less reliable. The challenge for ASEAN is therefore not merely to digitize existing procedures, but to reconstruct cooperation in a manner that accommodates networked evidence and assets while preserving legal certainty, human rights, and due process.

b. Fragmentation of Locus Delicti

Digital infrastructures also complicate the classical concept of locus delicti, traditionally used to connect criminal conduct to a state's territorial jurisdiction (Hawley-Morelos & Cortes-Perez, 2024). Conventional doctrine generally assumes a meaningful geographic relationship among the offender, the victim, the conduct, the evidence, and the resulting harm. That assumption becomes less stable where criminal activity is executed through globally distributed infrastructure and where legally relevant acts occur in several locations at once.

Within Web3 environments, different elements of a single offence may be distributed across several jurisdictions (Wu et al., 2023). An offender may act from one state, use virtual private networks or cloud services in another, target victims elsewhere, and transfer proceeds through DeFi protocols, wallets, or virtual asset service providers operating across multiple jurisdictions. Because neither the offender nor the asset must move physically, a single criminal episode may generate several plausible jurisdictional connections simultaneously.

This produces what may be described as a fragmented locus delicti. Relevant connecting factors may include the location of offenders and victims, servers or data storage, service providers, validator nodes, and points at which virtual assets are converted or controlled. Distributed ledgers may replicate transaction data across many nodes, meaning that electronic evidence is not necessarily under the exclusive control of one territorial authority (Chang, 2018). The bilateral requesting-state/requested-state logic of conventional MLA can therefore become difficult to apply where evidence and infrastructure are functionally distributed across multiple legal orders.

Fragmentation also increases the possibility of concurrent jurisdiction. States may assert authority on territorial, nationality, protective, or other recognized jurisdictional bases, creating overlapping claims that require coordination (Akhyar & Saptawati, 2025). Without effective mechanisms for prioritization and cooperation, parallel claims can delay investigations, increase the risk that volatile evidence will be lost, and create uncertainty over which authority should lead. In this environment, locus delicti is better understood not solely as a geographic point but as a set of networked legal and factual connections.

From a CLS perspective, this fragmentation demonstrates that territorial jurisdiction is a historically contingent legal construction rather than a complete description of how contemporary digital activity occurs. As economic and criminal conduct becomes more transnational and decentralized, a purely territorial paradigm may lose explanatory and regulatory capacity (S et al., 2025). The resulting mismatch is not merely procedural; it is structural. One consequence is greater scope for regulatory arbitrage, because actors can exploit differences among the jurisdictions connected to the same digital activity.

c. Regional Regulatory Arbitrage

Digital-economy regulation has developed unevenly across ASEAN. Differences in substantive criminal law, supervisory capacity, licensing rules, and enforcement priorities create opportunities for regulatory arbitrage, whereby actors structure conduct through jurisdictions perceived to impose lower legal or compliance costs (Pollman, 2019). In the context of virtual assets and DeFi, these disparities may allow illicit actors to route transactions, hold assets, or provide services through jurisdictions with less-developed regulatory frameworks or weaker supervisory capacity.

Some ASEAN jurisdictions have adopted relatively detailed virtual-asset and anti-money-laundering frameworks, including measures informed by FATF standards, while others remain at different stages of regulatory development. Such divergence may enable criminal networks to shift transactions, asset custody, or laundering activity toward jurisdictions with lower levels of oversight (McCarthy-Jones & Turner, 2024). Regional economic integration can therefore produce not only legitimate mobility but also jurisdiction-shopping incentives where legal regimes remain materially uneven.

Dimension	2004 ASEAN MLA Paradigm	Characteristics of Web3 Financial Crime	Implications for Mutual Legal Assistance
Object of Evidence	Physical documents, conventional accounts, and identifiable records	Blockchain records, wallet addresses, control credentials, and virtual assets	Evidence and asset-related data may be distributed across several jurisdictions
Offender Attribution	Identification supported by KYC/CDD and institutional records	Pseudonymous identities and cryptographic or privacy-enhancing tools	Greater difficulty in identifying persons and specifying the object of an MLA request
Locus Delicti	Primarily linked to territorial jurisdiction	Distributed infrastructure and cross-border transactions	Fragmented jurisdictional connections and possible concurrent claims
Transaction and Evidence Speed	Formal processing may require sequential administrative steps	Asset transfers and smart-contract execution may occur near real time	Procedural delay can reduce the practical value of assistance
Regulatory Convergence	Assumes sufficient correspondence between domestic legal regimes	Divergent rules for digital assets and related conduct across ASEAN	Regulatory arbitrage and friction in applying dual criminality

Table 1. Comparison of the ASEAN MLA Paradigm, Web3 Financial Crime, and Implications for Mutual Legal Assistance

Regulatory divergence has direct implications for MLA because differences in offence definitions, the legal status of virtual assets, and the obligations imposed on virtual asset service providers can complicate the application of dual criminality (Chystokletov et al., 2025). Assistance may become difficult not because the underlying conduct is harmless or the evidence is necessarily weak, but because the requesting and requested states characterize the relevant conduct differently. From a CLS perspective, this demonstrates that barriers to cooperation are partly produced by asynchronous national legal development within an economically integrated region. Without greater convergence on core digital-financial offences and investigative standards, regulatory arbitrage will continue to undermine the normative capacity of MLA as a regional enforcement instrument.

2. Structural and Doctrinal Frictions in the ASEAN MLA Framework

The preceding analysis suggests that the principal difficulty is not simply the state's capacity to identify offenders or trace criminal proceeds; it is the mismatch between the characteristics of digital financial crime and the legal assumptions embedded in regional cooperation. The ASEAN MLA Treaty was developed in an era when transnational enforcement focused largely on offences such as narcotics trafficking, human smuggling, corruption, and money laundering through formal financial institutions (Arifin et al., 2024). Its architecture consequently assumes that evidence and investigative objects can be associated with particular state jurisdictions and that assistance can proceed through structured intergovernmental procedures (Ishii, 2025). Virtual assets, distributed ledgers, and cross-network transactions weaken these assumptions and generate friction between established legal processes and contemporary digital-financial realities.

The resulting friction is doctrinal as well as technical. Dual criminality, centralized coordination through national Central Authorities, and territorial sovereignty are designed to protect legality, accountability, and domestic jurisdiction (Soler, 2019). Yet when applied rigidly to rapidly moving, cross-jurisdictional digital activity, the same safeguards may delay cooperation or render assistance ineffective in practice. A credible evaluation of ASEAN MLA must therefore examine not only administrative performance but also whether the doctrines underlying the Treaty remain proportionate and adaptable to digital financial crime.

a. The Dual Criminality Constraint

Dual criminality is a longstanding safeguard in mutual legal assistance. In general terms, it permits a requested state to condition assistance on whether the relevant conduct would also constitute an offence under its own law (Ruiz Yamuza, 2019). The principle protects legislative sovereignty and prevents a state from being compelled to support enforcement against conduct that its legal system does not criminalize. For widely harmonized conventional offences, this requirement often presents fewer difficulties because the underlying conduct is criminalized across jurisdictions.

Digital financial crime complicates that premise. ASEAN states regulate virtual assets, DeFi, smart contracts, mixing services, and digital-asset market conduct at different speeds and through different legal techniques (Soeparna & Nugroho, 2026). Conduct treated as a criminal offence in one jurisdiction may be regulated administratively, prohibited through licensing rules, or not specifically addressed in another. Similar harmful conduct can therefore produce different legal consequences depending on the jurisdiction through which it is assessed.

This creates a potential dual-criminality constraint in cross-border investigations. A requesting state may characterize a digital-asset transaction as part of a laundering, fraud, or market-manipulation scheme, while the requested state may lack an equivalent offence or may classify the conduct differently. The obstacle therefore arises from normative disparity rather than solely from evidentiary weakness. In such circumstances, the practical capacity of MLA depends substantially on the degree of substantive convergence among domestic legal systems (Le Nguyen, 2012).

From a CLS perspective, dual criminality should not be treated as a mechanically neutral doctrine. Its operation depends on assumptions about the comparability and pace of national legal development. In a rapidly changing digital economy, those assumptions may fail where technological innovation precedes legislative adaptation. A rigidly formal interpretation can consequently transform regulatory lag into an obstacle to cooperation and create opportunities for actors to exploit differences among national legal regimes. The policy challenge is therefore to preserve the sovereignty-protecting function of dual criminality while reducing unnecessary dependence on identical offence labels or legislative formulations.

b. Temporal Constraints of Central-Authority Procedures

A second difficulty concerns institutional timing. ASEAN MLA procedures rely on designated Central Authorities to receive, assess, transmit, and coordinate requests for assistance. This structure promotes legality, accountability, and compliance with domestic procedure. In cases involving conventional documents, witnesses, or tangible property, the time required for formal processing may be compatible with the evidentiary needs of the investigation (Ayers et al., 2023).

Digital financial cases are more time-sensitive. Electronic data may be altered or deleted, virtual assets can be transferred across multiple wallets and networks within a short period, and service arrangements may change rapidly (Sukardi, 2022). Each additional layer of administrative review can therefore reduce the practical value of eventual assistance. The problem is not that Central Authorities are inherently unsuitable, but that conventional document-based workflows may be too slow for evidence and assets capable of moving in near real time.

This mismatch may be described as temporal paralysis: legal authority remains formally available, yet its practical utility diminishes because action occurs after the relevant asset or evidence has moved beyond immediate reach. In virtual-asset investigations, even relatively short delays can significantly increase tracing complexity. The critical question is therefore not only whether assistance will ultimately be provided, but whether it can be provided within a timeframe that preserves evidentiary and enforcement value.

The temporal problem supports a transition toward secure, standardized electronic MLA processes capable of accelerating authentication, transmission, and status tracking while preserving judicial oversight and due-process guarantees. The objective should not be speed at any cost, but procedural design proportionate to the volatility of digital evidence and assets. Without such adaptation, hierarchical and paper-dependent cooperation mechanisms risk remaining structurally slower than the criminal activity they are intended to address (Fichtelberg et al., 2025).

c. Sovereignty and the Governance of Transnational Digital Crime

Territorial sovereignty remains a foundational principle of cooperation among ASEAN states. MLA is premised on the authority of each state to control investigative measures within its territory and to refuse assistance where specified national interests, security concerns, or public-order considerations are engaged (Arifin et al., 2024). This orientation is consistent with the broader ASEAN emphasis on non-interference and respect for sovereignty (Suzuki, 2019).

These principles remain important to regional legitimacy, but their application to digital financial crime creates tension. Blockchain-enabled laundering, cross-platform fraud, and other cyber-enabled financial offences may involve actors, victims, service providers, data, and assets located in several countries simultaneously (Hasan et al., 2025). A model that treats territorial sovereignty as an exclusively defensive barrier can therefore make cooperation heavily dependent

International Journal of Business, Law, and Education
Publisher: IJBLE Scientific Publications Community Inc.
IJBLE
Volume 7, Number 2, 2026
https://ijble.com/index.php/journal/index

on sequential political and administrative decisions, even where the relevant conduct is structurally transnational.

A CLS analysis does not require sovereignty to be discarded; rather, it asks how sovereignty should be interpreted under changed technological conditions. Geographic boundaries remain legally significant, but they no longer exhaust the locations at which economic and criminal activity can occur (Sidorenko et al., 2021). The more sustainable approach is to understand sovereignty as compatible with rule-based cooperation: states retain jurisdiction while accepting common standards for timely information exchange, asset preservation, evidence gathering, and procedural safeguards. The central question is therefore how to design cooperation that is fast and interoperable without sacrificing legality, proportionality, or rights protection.

3. Paradigmatic Reconstruction: Toward Regional Juridical Reciprocity

The preceding sections show that the limitations of the ASEAN MLA framework are not reducible to administrative inefficiency. They reflect a deeper mismatch between a state-centred, territorially organized cooperation model and a digital-financial environment in which data, assets, and relevant actors may be decentralized and distributed across jurisdictions. The 2004 framework assumes that states remain the principal institutional gatekeepers for information, evidence, and enforcement authority (Lee, 2022). Although that assumption remains legally important, it is increasingly incomplete where private service providers, distributed infrastructures, and real-time asset movements shape the practical conditions of investigation. Reform should therefore move beyond editorial amendment toward a model of regional juridical reciprocity based on legal trust, institutional interoperability, and minimum substantive convergence.

Regional juridical reciprocity, as proposed here, does not displace state sovereignty. It reconceptualizes sovereignty as compatible with shared responsibility for transnational risks affecting the integrity of the regional financial system (Goldmann, 2022). Member states would retain domestic jurisdiction while committing to interoperable procedures for information exchange, preservation and freezing of assets, collection of electronic evidence, and coordination of investigations under agreed regional legal standards. The purpose is to transform cooperation from discretionary administrative exchange into a more predictable, rule-based form of regional legal collaboration.

a. Institutionalizing a Secure e-MLA Platform

The first component is the modernization of MLA through a secure electronic mutual legal assistance (e-MLA) platform. Conventional workflows frequently depend on sequential correspondence, document authentication, and transmission between investigating authorities and national Central Authorities (Arifin et al., 2024). These procedures serve important legal functions but generate institutional transaction costs when repeated manually. In digital-financial investigations, where evidence and assets may be highly time-sensitive, a secure electronic platform could reduce avoidable administrative delay without eliminating the legal review performed by competent authorities.

This study proposes that such a platform may use permissioned distributed-ledger technology (DLT) where DLT provides a demonstrable governance advantage over conventional secure databases. Unlike public blockchains, a permissioned architecture would restrict access to authorized institutions (Dash et al., 2023). Each request could be assigned a unique digital identifier and authenticated through secure electronic signatures, with an auditable record of submission, receipt, review, and action. The legal objective is not to adopt blockchain for its own sake, but to create a tamper-evident and interoperable record that improves accountability while protecting investigative confidentiality.

Automation could also be used for limited administrative functions. Rule-based validation may verify the identity of the requesting authority, identify missing mandatory fields, acknowledge receipt, route the request to the competent authority, and provide status notifications. Such automation should not determine substantive legality or replace judicial and prosecutorial discretion. Its purpose is to remove repetitive administrative friction so that human decision-makers can focus on necessity, proportionality, evidentiary sufficiency, and rights protection.

A well-designed e-MLA system could therefore improve both speed and accountability. Chronological logging would make it easier to identify where delays occur, reduce risks of lost documentation, and support institutional audit. These features may also strengthen inter-state trust by creating a consistent record of procedural compliance (Stafford et al., 2022). Digitalization should thus be understood as a governance reform: technology is useful only insofar as it improves the reliability, security, and timeliness of legal cooperation.

b. Reinterpreting Dual Criminality Through a Substantive Approach

The second component concerns the interpretation of dual criminality. A requirement based on identical offence names or highly similar statutory wording is poorly suited to a region in which digital-asset regulation develops unevenly. Where one state legislates earlier than another, formal differences in legal terminology may obstruct cooperation even when both legal systems condemn the underlying harmful conduct (Vũ, 2023). The relevant reform is therefore interpretive as well as legislative.

This study proposes a shift from formal to substantive dual criminality. Under this approach, the requested authority would assess whether the underlying conduct, considered in substance, would amount to criminal wrongdoing under both legal systems, rather than requiring identical nomenclature or statutory classification. Conduct involving fraud, concealment of criminal proceeds, unlawful appropriation, deceptive asset manipulation, or comparable protected legal interests could therefore satisfy the requirement despite differences in legislative technique.

A substantive approach is better able to accommodate technological change because new modus operandi often emerge before legislatures develop technology-specific offences. If cooperation depends on identical legal wording, criminal innovation will repeatedly exploit the interval between technological development and legislative reform (Sadouk, 2023). Focusing on the substance and unlawfulness of the conduct provides greater adaptability while retaining a legal threshold that protects requested states from assisting with conduct they do not recognize as criminal.

This approach nevertheless requires regional guidance. ASEAN should develop a common framework identifying core categories of digital financial misconduct and minimum elements relevant to MLA assessment. Such guidance need not harmonize every aspect of domestic criminal law. Its purpose would be to establish sufficient substantive convergence to support predictable cooperation while allowing national legal systems to retain their own offence structures and procedural safeguards.

c. Integrating Financial Intelligence and Law-Enforcement Coordination

The third component is a more proactive model of cross-agency coordination. Conventional MLA is typically triggered after a domestic investigation has already identified a need for assistance from another jurisdiction. For rapidly moving digital assets, a purely reactive sequence may be too slow because significant transfers can occur before a complete formal request is prepared (James, 2017). MLA should therefore operate alongside, rather than in isolation from, earlier intelligence and preservation mechanisms.

Operational coordination among Financial Intelligence Units (FIUs), police, customs authorities, immigration agencies, and virtual-asset supervisory bodies could improve the speed and quality of cross-border responses. FIUs can analyze suspicious financial flows, investigative authorities can develop criminal cases, and other agencies can contribute information relevant to identity, movement, asset control, or service-provider relationships. Properly governed information sharing may therefore produce a more complete intelligence picture before formal evidentiary assistance is sought (Licari et al., 2025).

A complementary mechanism is emergency asset preservation. Where there are reasonable and legally defined grounds to believe that virtual assets are at imminent risk of transfer, member states could permit a temporary preservation or freezing request for a strictly limited period pending submission of a complete MLA application (Dimitras, 2026). Such a mechanism should be exceptional, proportionate, time-bound, subject to judicial or equivalent independent oversight, and accompanied by procedures through which affected parties can challenge unlawful or excessive measures.

Institutional coordination could be supported by an ASEAN Digital Financial Crime Coordination Hub responsible for strategic information exchange, regional risk analysis, capacity building, and the facilitation of multi-jurisdictional cooperation. The proposed hub would not replace domestic authorities or exercise supranational prosecutorial power. Its function would be to improve interoperability and reduce dependence on slow bilateral communication in cases that are inherently regional in scope (Panke & Starkmann, 2021).

Taken together, these reforms form the proposed model of regional juridical reciprocity. A secure e-MLA architecture addresses avoidable procedural delay and accountability; substantive dual criminality reduces barriers created by divergent legislative terminology; and integrated intelligence, preservation, and law-enforcement coordination improves operational responsiveness. These elements are mutually reinforcing. Their purpose is not to weaken sovereignty, but to make sovereignty functional in an environment where effective protection of national and regional financial systems increasingly depends on timely, rights-respecting cross-border cooperation.

CONCLUSION

This study concludes that the principal challenge facing the 2004 ASEAN MLA Treaty in relation to digital financial crime lies in a normative mismatch between its territorially organized cooperation model and the characteristics of Web3-based financial activity. Blockchain, DeFi, virtual assets, and smart contracts can distribute actors, evidence, and assets across multiple jurisdictions and allow transactions to occur at a speed that conventional legal-assistance procedures were not designed to match. As a result, assumptions concerning locus delicti, territorial control, identifiable intermediaries, and sequential administrative cooperation are increasingly strained.

Using a CLS perspective and the concept of regulatory lag, the analysis identifies three interrelated constraints: formalistic application of dual criminality, time-sensitive dependence on centralized administrative workflows, and a sovereignty paradigm that may be interpreted too defensively for inherently transnational digital activity. These constraints do not establish, by themselves, that the ASEAN MLA Treaty is empirically ineffective; rather, they demonstrate vulnerabilities in its normative and institutional design that may impede timely cross-border cooperation in digital-financial cases.

The article therefore proposes regional juridical reciprocity as a framework for reconstruction. Its principal components are a secure e-MLA mechanism; a substantive interpretation of dual criminality; greater convergence around core digital-financial offences and investigative standards; stronger coordination among law-enforcement agencies, FIUs, and relevant supervisory authorities; and narrowly defined emergency preservation measures for volatile digital assets. The model preserves state jurisdiction while treating timely, interoperable cooperation as part of the shared responsibility of ASEAN member states in addressing transnational financial threats.

The study contributes to international legal scholarship by shifting the analysis of MLA from procedural administration alone to the legal assumptions that structure cross-border cooperation. Combining CLS, regulatory-lag analysis, and policy-oriented legal research provides a framework for explaining why conventional cooperation mechanisms may become less responsive as the technological environment changes. From a policy perspective, the proposed model offers a conceptual basis for future modernization of ASEAN MLA while retaining legality, proportionality, due process, and sovereignty as core constraints on reform.

The study is limited by its normative design and does not empirically evaluate the implementation of MLA in each ASEAN member state. Future research should therefore test the proposed framework through comparative case studies, interviews with competent authorities, analysis of processing times and refusal grounds, and assessment of institutional and digital readiness across ASEAN jurisdictions. Such empirical work is necessary to determine which elements of the proposed reconstruction are operationally feasible and whether they produce measurable improvements in cross-border digital-financial investigations.

References

Akhyar, A., & Saptawati, G. A. P. (2025). A systematic literature review to address overlapping laws in Indonesia. *Bulletin of Electrical Engineering and Informatics*, *14*(3), 2338–2346. https://doi.org/10.11591/eei.v14i3.8407

Alkhaldi, M. A. A. (2026). Technological Enhancements in Subject Matter and Procedural Jurisdiction for Economic Crimes. In N. Al-Ramahi, A. M. A. Musleh Al-Sartawi, & M. Kanan (Eds.), *Artificial Intelligence in the Digital Era* (Vol. 594, pp. 627–638). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89771-9_45

Alshaer, H., Md. Said, M. H., & Rajamanickam, R. (2024). Mutual legal assistance and extradition under anti-money laundering laws: A comparative analysis between Palestine and Malaysia. *Journal of Money Laundering Control*, *27*(2), 413–426. https://doi.org/10.1108/JMLC-03-2023-0053

Alsmadi, A. A., & Alshehadeh, A. R. (2025). Systematic Literature Review on Financial Technology Security. *2025 International Conference on Business Intelligence for Technology Innovation (ICBITI)*, 1–6. https://doi.org/10.1109/ICBITI65527.2025.11500801

Arifin, R., Rodiyah, Waspiah, Ridzqi Amandha, A., & Yunita Krisnawati, E. (2024). The Direction of Indonesia's Legal Policy on the ASEAN Mutual Legal Assistance Treaty in Criminal Matters: A Path to Law Reform in Cross-Border Crime Enforcement in Southeast Asia. *Journal of Law and Legal Reform*, *5*(2), 749–782. https://doi.org/10.15294/jllr.v5i2.3206

Aspray, W., & Doty, P. (2023). Does technology really outpace policy, and does it matter? A primer for technical experts and others. *Journal of the Association for Information Science and Technology*, *74*(8), 885–904. https://doi.org/10.1002/asi.24762

Ayers, K., Roberts, M., & Pettolina, M. (2023). Physical Evidence Collection Techniques. In *Encyclopedia of Forensic Sciences, Third Edition* (pp. 155–170). Elsevier. https://doi.org/10.1016/B978-0-12-823677-2.00117-3

Azeez N. P., A., Imdadul Haque, M., & Akhtar, S. M. J. (2022). Digital Payment and Economic Growth: Evidence from India. *Applied Economics Quarterly*, *68*(2), 79–93. https://doi.org/10.3790/aeq.2022.1418301

Badkul, S., Kishor, A., Juchnevicius, E., & Madvariya, S. (2025). Blockchain and the Future of Digital Evidence: Opportunities and Challenges for Law Enforcement. In B. N. Mukherjee, R. Uduwerage-Perera, M. Mathew, & S. Kumar Tripathi (Eds.), *Rethinking the Police for a Better Future* (pp. 287–297). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-83173-7_19

Bayan, T., Yazici, A., & Banach, R. (2025). Permissionless Blockchain Recent Trends, Privacy Concerns, Potential Solutions and Secure Development Lifecycle. *Future Internet*, *17*(12), 547. https://doi.org/10.3390/fi17120547

Bellaby, R. W. (2018). Going dark: Anonymising technology in cyberspace. *Ethics and Information Technology*, *20*(3), 189–204. https://doi.org/10.1007/s10676-018-9458-4

Bisset, A. (2023). The Mutual Legal Assistance Treaty for Core Crimes: A Project in Need of Purpose. *Nordic Journal of International Law*, *92*(2), 218–247. https://doi.org/10.1163/15718107-bja10056

Brison, S. J. (2018). *Contemporary Perspectives on Constitutional Interpretation* (S. J. Brison & W. Sinnott-Armstrong, Eds.; 1st ed.). Routledge. https://doi.org/10.4324/9780429501364

Chang, H. (2018). Is distributed ledger technology built for personal data? *Journal of Data Protection & Privacy*, *1*(4), 410. https://doi.org/10.69554/DKOX7451

Chystokletov, L., Khytra, O., Yosyfovych, D., Dolynska, M., & Kardashevskyy, Y. (2025). Issues of virtual assets legal regulation: Possible social and economic consequences. *Social and Legal Studios*, 290–298. https://doi.org/10.32518/sals1.2025.290

Cinal, A., Kubiak, P., Kutyłowski, M., & Wechta, G. (2026). Anamorphic Monero Transactions: The Threat of Bypassing Anti-money Laundering Laws. In V. Nicomette, A. Benzekri, N. Boulahia-Cuppens, & J. Vaidya (Eds.), *Computer Security – ESORICS 2025* (Vol. 16054, pp. 103–123). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-07891-9_6

Cubides-Cardenas, J., Hernández-Alvarado, C. E., Jimenez-Reina, J., & Roncancio-Bedoya, A. F. (2025). Regional cooperation against transnational organized crime: Challenges and opportunities in the Western Hemisphere. *Frontiers in Political Science*, *7*, 1657969. https://doi.org/10.3389/fpos.2025.1657969

Dash, S., Parida, P., Sahu, G., & Khalaf, O. I. (2023). Artificial Intelligence Models for Blockchain-Based Intelligent Networks Systems: Concepts, Methodologies, Tools, and Applications. In A. K. Tyagi (Ed.), *Advances in Systems Analysis, Software Engineering, and High Performance Computing* (pp. 343–363). IGI Global. https://doi.org/10.4018/978-1-6684-6697-1.ch019

De Sanctis, F. M. (2019). *Technology-Enhanced Methods of Money Laundering: Internet As Criminal Means*. Springer International Publishing. https://doi.org/10.1007/978-3-030-18330-1

Demir, F. (2020). Participatory Government. In F. Demir, *Public Management Reform in Turkey* (Vol. 20, pp. 83–115). Springer International Publishing. https://doi.org/10.1007/978-3-030-41648-5_3

Dimitras, K. P. (2026). JUDICIAL EFFICIENCY IN THE ERA OF DIGITAL ASSETS: PERSPECTIVES ON SMART TECHNOLOGIES. *Access to Justice in Eastern Europe*, *9*(2). https://doi.org/10.33327/AJEE-18-9.2-a0001973

Dolgieva, M. (2023). Criminal law protection of public relations in field of digital financial assets and digital currency. *Gosudarstvo i Pravo*, (11), 132. https://doi.org/10.31857/S102694520023126-9

Eg Tan, E., & Ang, B. (2022). ASEAN Ambiguity on International Law and Norms for Cyberspace. *Baltic Yearbook of International Law Online*, *20*(1), 133–162. https://doi.org/10.1163/22115897_02001_008

El Harras, M., & Salahddine, M. A. (2025). Tracking financial crime through code and law: A review of RegTech applications in anti-money laundering and terrorism financing. *Corporate Law and Governance Review*, *7*(3), 73. https://doi.org/10.22495/clgrv7i3p7

Fichtelberg, A., Fox, N., & Lin, K. (2025). *Crime Without Borders: An Introduction to International Criminal Justice* (2nd ed.). Routledge. https://doi.org/10.4324/9781003729440

Gavaghan, C., & Charlesworth, A. (2025). Technology's Ability to Escape the Legal

System. In R. Brownsword & L. A. DiMatteo (Eds.), *The Cambridge Handbook of the Governance of Technology* (1st ed., pp. 71–90). Cambridge University Press. https://doi.org/10.1017/9781009522519.008

Gerrard, M. B. (2020). An Environmental Lawyer's Fraught Quest for Legal Tools to Hold Back the Seas. *Daedalus*, *149*(4), 79–95. https://doi.org/10.1162/daed_a_01818

Goldmann, M. (2022). Financial Stability. In J. Klabbers (Ed.), *The Cambridge Companion to International Organizations Law* (1st ed., pp. 391–421). Cambridge University Press. https://doi.org/10.1017/9781108574242.018

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, *157*, 103338. https://doi.org/10.1016/j.futures.2024.103338

Goyal, V., Misra, D., Gupta, S., Arulini, K., & Sundharesalingam, P. (2026). A Review of FinTech Innovations and Networking Technologies in the Digital Financial Ecosystem. In B. Virdee, S. D. Correia, A. Swaroop, N. Thakur, & S. D. Shetty (Eds.), *Proceedings of International Conference on Artificial Intelligence and Networks* (Vol. 1921, pp. 117–130). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-23219-9_10

Hasan, W. A., Hameed, S. S., Fattah, A. I., Mutlak, S. J., Shwayyea, R. T., & Dakhil, A. J. (2025). Blockchain-Assisted Trust and Transparency in Cross-Border Digital Asset Management System. *2025 3rd International Conference on Cyber Resilience (ICCR)*, 1–6. https://doi.org/10.1109/ICCR67387.2025.11292289

Hawley-Morelos, H., & Cortes-Perez, O. I. (2024). Crime Scene and Feminicide: Crime Scene Investigation and Processing Standards. In O. I. Cortes-Perez (Ed.), *Forensic Victimology and Femi(ni)cide* (pp. 173–243). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-72512-8_6

Irawan, B., Mulyanti, D., Budiaman, H., Rahman, Y. M., & Taufiqurrohman, A. (2025). Perspective of State Sovereignty in Law Enforcement Related to Cyberlaw Jurisdiction. *LAW REFORM*, *21*(1), 120–134. https://doi.org/10.14710/lr.v21i1.68760

Ishii, Y. (2025). *International Law and the Investigation of Transnational Crimes* (1st ed.). Oxford University PressOxford. https://doi.org/10.1093/9780198957089.001.0001

Ishikawa, K. (2021). The ASEAN Economic Community and ASEAN economic integration. *Journal of Contemporary East Asia Studies*, *10*(1), 24–41. https://doi.org/10.1080/24761028.2021.1891702

James, J. I. (2017). How Businesses Can Speed Up International Cybercrime Investigation. *IEEE Security & Privacy*, *15*(2), 102–106. https://doi.org/10.1109/MSP.2017.40

James, J. I., & Gladyshev, P. (2016). A survey of mutual legal assistance involving digital evidence. *Digital Investigation*, *18*, 23–32. https://doi.org/10.1016/j.diin.2016.06.004

Jindal, P., Kaur, J., & Sood, K. (2022). Process Innovation and Unification of KYC Document Management System with Blockchain in Banking. In K. Sood, R. K. Dhanaraj, B. Balusamy, & S. Kadry (Eds.), *Blockchain Technology in Corporate Governance* (1st ed., pp. 197–216). Wiley.

https://doi.org/10.1002/9781119865247.ch9

Khan, A., Jillani, M. A. H. S., Ullah, M., & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, *28*(2), 408–423. https://doi.org/10.1108/JMLC-07-2024-0113

Krasniqi, B., & Stefanova, E. P. (2024). Exploring Web3 Challenges: Implications for Investigative Techniques and Evidence Acquisition in Digital Forensics. *2024 International Conference Automatics and Informatics (ICAI)*, 254–259. https://doi.org/10.1109/ICAI63388.2024.10851563

Kristian, W., Alfajri, M. I., Oktavia, B., Nofitriandi, A., & Teguh, W. (2022). Risk Invalidation of Data in Banking Information System in Indonesia. *2022 International Conference on Information Management and Technology (ICIMTech)*, 333–338. https://doi.org/10.1109/ICIMTech55957.2022.9915040

Le Nguyen, C. (2012). Towards the effective ASEAN mutual legal assistance in combating money laundering. *Journal of Money Laundering Control*, *15*(4), 383–395. https://doi.org/10.1108/13685201211265971

Lee, E. Y. J. (2022). Legal Development of the ASEAN Community Building. In E. Y. J. Lee (Ed.), *ASEAN International Law* (pp. 1–18). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-3195-5_1

Lekhi, P. (2023). Web 3.0 Revolution in the Finance Industry: Exploring Blockchain and Decentralized Finance. In P. Lekhi & G. Kaur (Eds.), *Advances in Web Technologies and Engineering* (pp. 23–32). IGI Global. https://doi.org/10.4018/978-1-6684-9919-1.ch002

Licari, C., Rinaldi, G., & Ficara, A. (2025). Criminal Network Construction and Analysis from Italian Civil Cases: A Case Study. In H. Cherifi, M. Donduran, L. M. Rocha, C. Cherifi, & O. Varol (Eds.), *Complex Networks & Their Applications XIII* (Vol. 1189, pp. 181–193). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-82435-7_15

Lin, L. S. F. (Ed.). (2025). *Innovations in Cryptocrime and Financial Fraud:* IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0675-9

Lin, L., Zhang, L., Xu, F., & Gabriel, B. M. V. (2023). Research on Cross-Border Electronic Evidence Network Forensics Cooperation and Response Mechanism. In J. H. Abawajy, Z. Xu, M. Atiquzzaman, & X. Zhang (Eds.), *Tenth International Conference on Applications and Techniques in Cyber Intelligence (ICATCI 2022)* (Vol. 170, pp. 429–437). Springer International Publishing. https://doi.org/10.1007/978-3-031-29097-8_51

Liu, H. (2025). INTERFERENCE TORTS IN THE DIGITAL ASSET WORLD. *The Cambridge Law Journal*, *84*(1), 115–142. https://doi.org/10.1017/S0008197325000042

López Rodríguez, A. M. (2025). Consumer protection in blockchain-based metaverses: A comparative study of cross-border legal gaps and platform governance. *Frontiers in Blockchain*, *8*, 1675735. https://doi.org/10.3389/fbloc.2025.1675735

Manavadaria, M. S., Sharma, R. K., Parasar, A., Chauhan, A., Jeyaprakash, N., Mohaideen, A., & Bhoopathy, V. (2025). Machine Learning for Fraud Detection and Financial Crimes: In C. Kaunert, A. Raghav, K. Ravesangar, & B. Singh

(Eds.), *Forensic Intelligence and Deep Learning Solutions in Crime Investigation* (pp. 183–206). IGI Global. https://doi.org/10.4018/979-8-3693-9405-2.ch010

McCarthy-Jones, A., & Turner, M. (2024). Dark Networks, Transnational Crime and Security: The Critical Role of Brokers. *Journal of Illicit Economies and Development*, *5*(1), 58–69. https://doi.org/10.31389/jied.226

McGregor, B. V. (2019). Understanding Cryptocurrencies, Blockchain Technology and Regulations. In S. Chishti, T. Craddock, & R. Courtneidge (Eds.), *The PayTech Book* (1st ed., pp. 110–113). Wiley. https://doi.org/10.1002/9781119551973.ch32

Mitchell, M. (2023). Analyzing the law qualitatively. *Qualitative Research Journal*, *23*(1), 102–113. https://doi.org/10.1108/QRJ-04-2022-0061

Nguyen, H. X. M., & Ngo, V. T. N. (2026). Bamboo in the Storm: A Vietnamese Perspective on Data Sovereignty and Trust in the Digital Economy. In J. Nakagawa, T. Hamada, & Y. Ishikawa (Eds.), *Geopolitical Risks and Geoeconomics in International Economic Law* (pp. 235–253). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-6996-0_13

Palurovic, S., & Gross, J. (2026). Decentralized finance. In R. Beck (Ed.), *Elgar Encyclopedia of Cryptocurrencies, Blockchain and DLT* (pp. 75–82). Edward Elgar Publishing. https://doi.org/10.4337/9781035339969.00021

Panke, D., & Starkmann, A. (2021). Trajectories of regional cooperation: A comparative analysis. *Comparative European Politics*, *19*(1), 1–25. https://doi.org/10.1057/s41295-020-00226-1

Pollman, E. (2019). Tech, Regulatory Arbitrage, and Limits. *European Business Organization Law Review*, *20*(3), 567–590. https://doi.org/10.1007/s40804-019-00155-x

Putri, E. E., Silviani, N. Z., & Tantimin, T. (2025). Mutual Legal Assistance in Corruption Offenses' Asset Recovery: A Comparative Study between Indonesia and Singapore. *Uti Possidetis: Journal of International Law*, *6*(2), 260–277. https://doi.org/10.22437/up.v6i2.40835

Qin, X. (2026). Cross-National Criminal Police Cooperation. In S. Guo & Y. Gu (Eds.), *Global Justice* (pp. 135–162). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-8485-7_7

Ruiz Yamuza, F.-G. (2019). CJEU case law on double criminality. The Grundza-Piotrowski paradox?: Some notes regarding the Puigdemont case. *ERA Forum*, *19*(3), 465–484. https://doi.org/10.1007/s12027-019-00553-1

Ryngaert, C. (2025). The concept of jurisdiction in international law. In A. Orakhelashvili (Ed.), *Research Handbook on Jurisdiction and Immunities in International Law* (pp. 37–51). Edward Elgar Publishing. https://doi.org/10.4337/9781035331086.00007

S, S., S, N., I, G., S R, R., V, R., & Bala C K, R. P. (2025). A Survey on the Evolution of Business Models From Web2 to Web3: Adoption and the Future of Digital Enterprises. *2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF)*, 1–8. https://doi.org/10.1109/ICECONF65644.2025.11379418

Sadouk, R. (2023). International Cooperation, Criminal Justice and Human Rights: The Missing Link. *International Annals of Criminology*, 1–28.

https://doi.org/10.1017/cri.2023.18

Salami, I. (2021). Challenges and Approaches to Regulating Decentralized Finance. *AJIL Unbound*, *115*, 425–429. https://doi.org/10.1017/aju.2021.66

Sarathy, R. (2026). Web3. In R. Beck (Ed.), *Elgar Encyclopedia of Cryptocurrencies, Blockchain and DLT* (pp. 292–297). Edward Elgar Publishing. https://doi.org/10.4337/9781035339969.00066

Sarkhosh, H., Maroof, U., & Barradas, D. (2025). The Dark Art of Financial Disguise in Web3: Money Laundering Schemes and Countermeasures. *2025 APWG Symposium on Electronic Crime Research (eCrime)*, 1–18. https://doi.org/10.1109/eCrime66972.2025.11327832

Sidorenko, E. L., Kubantsev, S. P., & Khisamova, Z. I. (2021). International Financial and Information Security Strategies: Key Aspects of Preventing Criminal Threats. In S. I. Ashmarina, J. Horák, J. Vrbka, & P. Šuleř (Eds.), *Economic Systems in the New Era: Stable Systems in an Unstable World* (Vol. 160, pp. 479–488). Springer International Publishing. https://doi.org/10.1007/978-3-030-60929-0_61

Simanjuntak, E. L., Naili, Y. T., & Adji Samekto, F. X. (2022). Free Movement of Judgments in Cross-Border Money Laundering Crimes: A Legal Stance Toward the ASEAN Legal Integration. In E. Y. J. Lee (Ed.), *ASEAN International Law* (pp. 217–228). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-3195-5_13

Situmeang, S. M. T., Kamilia, E. R., Lutfiyah, N., & Aurora, D. M. (2026). Enforcement of the universality principle in combating cybercrime as a transnational crime. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, *16*(1), 70–88. https://doi.org/10.35295/sz.iisl.2411

Soeparna, I. I., & Nugroho, S. A. (2026). Digital Silk Road or Cyber Silk Curtain? Geo-Economics and Legal Dynamics of China's Belt and Road Initiative Within ASEAN Under the RCEP Framework. In J. Nakagawa, T. Hamada, & Y. Ishikawa (Eds.), *Geopolitical Risks and Geoeconomics in International Economic Law* (pp. 215–234). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-6996-0_12

Soler, C. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-335-1

Stafford, I., Cole, A., & Heinz, D. (2022). *Analysing the Trust–Transparency Nexus: Multi-Level Governance in the UK, France and Germany*. Policy Press. https://doi.org/10.51952/9781447355236

Sukardi. (2022). Financial Crime on Investigation in Industrial Revolution 4.0 Era. *International Journal of Criminology and Sociology*, *9*, 695–708. https://doi.org/10.6000/1929-4409.2020.09.66

Suzuki, S. (2019). Why is ASEAN not intrusive? Non-interference meets state strength. *Journal of Contemporary East Asia Studies*, *8*(2), 157–176. https://doi.org/10.1080/24761028.2019.1681652

Talmon, S. (Ed.). (2022). State Jurisdiction and Immunities. In *German Practice in International Law* (1st ed., pp. 139–154). Cambridge University Press. https://doi.org/10.1017/9781009085687.006

Troyanovskiy, V. M. (2021). Economic analysis of one type of criminal activity. *2021*

14th International Conference Management of Large-Scale System Development (MLSD), 1–4. https://doi.org/10.1109/MLSD52249.2021.9600192

Vermeulen, G., & Kusak, M. (2023). Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance After the European Investigation Order. *European Journal on Criminal Policy and Research*, *29*(4), 647–667. https://doi.org/10.1007/s10610-023-09539-9

Vincentius Setyawan, & Bariah Safrut. (2025). *Rethinking Law and Justice: The Core Principles of Critical Legal Studies against Legal Formalism*. https://doi.org/10.5281/ZENODO.17332128

Vũ, H. A. (2023). Practices of Mutual Legal Assistance in Criminal Matters between Vietnam and Southeast Asia Countries (Pt. 64 - 78). *International Journal of Criminal Justice Sciences*, *18*(1). https://doi.org/10.5281/zenodo.4756205

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). What Financial Crimes Are Hidden in Metaverse? Taxonomy and Countermeasures. In H. Huang, J. Wu, & Z. Zheng (Eds.), *From Blockchain to Web3 & Metaverse* (pp. 181–214). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-3648-9_7

Zagaris, B. (2019). Constructing a Financial Enforcement Regime to Reallocate Assets from the “Bad Guys” to the “Good Guys.” In M. G. Manwaring, *Gray Area Phenomena* (1st ed., pp. 93–108). Routledge. https://doi.org/10.4324/9780429041662-5

Zanghellini, A. (2017). A Conceptual Analysis of Conceptual Analysis in Analytic Jurisprudence. *Canadian Journal of Law & Jurisprudence*, *30*(2), 467–491. https://doi.org/10.1017/cjlj.2017.21

Zhao, D., Yuan, J., & Chen, W. (2023). Financial Consumer Protection in Fintech Field. In D. Zhao, J. Yuan, & W. Chen, *FinTech and SupTech in China* (pp. 93–102). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-5173-4_5

Zhao, Y., & Cheng, L. (2024). A bibliometric study of research trends in cross-border cybercrime. *International Journal of Legal Discourse*, *9*(1), 1–31. https://doi.org/10.1515/ijld-2024-2001