

Civil liability for damage caused by AI-executed smart contracts in the Banking Sector

Nguyen Ngoc Anh Tien¹, Do Bach Thanh Van², Tran Phu Khang²

¹ Lecturer, Faculty of Economic Law, Ho Chi Minh University of Banking, Ho Chi Minh City, Vietnam

² Ho Chi Minh University of Banking, Ho Chi Minh City, Vietnam

DOI: <https://doi.org/10.66856/ijl.2026.12.3.12263>

Abstract

Commercial banks increasingly rely on artificial intelligence not only to score credit but also to negotiate, conclude and self-execute contracts through smart-contract code, from automated loan disbursement to algorithmic trade-finance and treasury agreements. When such a contract causes damage, whether through an erroneous disbursement, an unauthorised transfer or a flawed automated negotiation, existing civil-liability doctrine struggles to answer a basic question: who is legally responsible, the bank that deployed the system, the vendor that built it, or the customer who accepted it? This article examines the theoretical nature of AI-concluded and AI-executed smart contracts, analyses the doctrinal basis for allocating civil liability for the damage they cause, and compares the approaches of the European Union, the United States, the United Kingdom and Singapore with the current legal framework of Vietnam. The article finds that Vietnamese law, despite recent legislative progress through the Law on Electronic Transactions and the Law on Artificial Intelligence, still lacks a clear rule attributing the acts of an autonomous banking system to a specific legal person and lacks a risk-based liability regime suited to opaque, self-executing code. The article proposes concrete lessons for Vietnam, including a statutory attribution rule, a rebuttable presumption of fault for high-risk banking AI, mandatory audit trails, and contractual risk-allocation and insurance mechanisms between banks and technology vendors.

Keywords: Smart contracts, artificial intelligence, civil liability, banking law, Vietnam

Introduction

Banks have moved beyond using artificial intelligence merely to score risk. Many credit institutions now deploy AI systems that negotiate the terms of a facility, generate the clauses of an agreement, and trigger a smart contract that automatically transfers funds, releases collateral or adjusts an interest rate once a coded condition is met. Trade-finance letters of credit, treasury and repo agreements, robo-advisory mandates and consumer loan disbursement are increasingly concluded and performed with little or no human intervention at the moment the obligation arises ^[1]. This shift is efficient, but it detaches the classical moment of contract formation, the meeting of minds between two human parties, from the person who ultimately bears the consequences of the bargain.

The legal difficulty becomes acute when something goes wrong. An oracle feeding false market data into a smart contract can trigger a wrongful margin call; a negotiation agent can commit the bank to a facility on terms nobody at the bank reviewed; a coding error in a disbursement contract can release funds to the wrong account; and once the code executes, it cannot be recalled in the way a human employee's decision can be countermanded before completion. Civil liability doctrine, built around fault, capacity and intention, was not designed for a contracting party that is code operating without real-time human decision. This creates uncertainty for banks, technology vendors, customers and courts alike about who must compensate the loss.

The matter is urgent for Vietnam. The State Bank of Vietnam is preparing sector-specific rules on the safe application of AI in banking ^[2], while the Law on Artificial Intelligence (Law No. 134/2025/QH15) and the Law on Electronic Transactions (Law No. 20/2023/QH15) have begun to build a general framework for automated systems

^[3, 4]. None of these instruments, however, was drafted with the specific problem of smart-contract liability in banking in mind. This article therefore asks how civil liability for damage caused by AI-concluded and AI-executed smart contracts in banking should be allocated, and what Vietnam can learn from the approaches taken in the European Union, the United States, the United Kingdom and Singapore.

Materials and Methods

To examine the practice of AI-driven contracting in banking, the author relies on secondary data from regulatory publications and industry reports on smart-contract and AI adoption in trade finance, treasury and lending, together with the disclosures of the State Bank of Vietnam and Vietnamese commercial banks. The article uses doctrinal legal analysis to interpret the relevant provisions of the Vietnamese Civil Code 2015, the Law on Electronic Transactions 2023 and the Law on Artificial Intelligence 2025. A comparative legal method is then applied to the liability frameworks of the European Union, the United States, the United Kingdom and Singapore, focusing on how each jurisdiction attributes the acts of an automated system to a legal person and allocates the burden of proving fault or defect. Finally, analytical and evaluative methods are used to identify the gaps in Vietnamese law and to formulate recommendations suited to the banking sector.

Results and Discussion

1. Theoretical issues concerning AI-concluded and AI-executed smart contracts

The concept of a smart contract

A smart contract is a set of instructions, usually written as software code running on a distributed ledger or on the bank's own system that automatically performs a contractual obligation once predefined conditions are satisfied, without

requiring a separate act of performance by either party ^[5]. In banking practice, a smart contract may release a loan tranche once a covenant is verified, transfer collateral once a margin threshold is crossed, or settle a trade-finance instrument once a shipping document is confirmed by an external data feed, known as an oracle. The code does not merely record the agreement; it performs it.

The concept of AI-concluded contracts

An AI-concluded contract goes a step further than a smart contract that merely executes pre-agreed terms. Here, an AI agent, typically a system built on machine-learning or generative models, participates in forming the terms themselves: it negotiates a price, selects a counterparty, drafts a clause, or accepts an offer on behalf of the bank without a human reviewing that specific decision at the time it is made ^[6]. The human principal defines the system's objectives and constraints in advance, but the particular bargain that emerges is the product of the system's own processing of data that did not exist, or could not be foreseen in detail, when the human set the parameters. This is what distinguishes an AI-concluded contract from an ordinary electronic contract executed through a fixed algorithm or a simple online form.

Distinguishing features relevant to liability

Three features of AI-concluded and AI-executed smart contracts complicate the attribution of civil liability. First, autonomy: the specific term or the specific act of performance is not authored by a natural person at the moment it occurs, which strains the classical requirement that a contracting party possess intention and capacity. Second, opacity: many AI systems, particularly those built on complex models, cannot fully explain why a given term was offered or why a given execution condition was considered satisfied, which makes it difficult to reconstruct fault after the fact ^[7]. Third, irreversibility: once a smart contract executes on a ledger or through an automated payment rail, the transfer of funds or collateral is often technically final, so that the loss crystallises before any human can intervene. Together these features mean that ordinary contract doctrine, which assumes a human party who can be shown to have intended or negligently caused an outcome, must be adapted rather than simply applied.

2. The basis of civil liability for damage caused by AI-driven smart contracts in banking

Contractual liability and tortious liability

Two distinct bases of liability may apply. Where the AI-concluded smart contract is itself a valid agreement between the bank and its customer, a defective term or a flawed execution that causes loss to the customer is, in principle, a breach of a contractual obligation, engaging the bank's liability for non-performance or improper performance under general contract law. Where the damage falls on a third party who is not privy to the smart contract, for example a counterparty misled by an autonomous negotiation, the applicable basis is tortious or extra-contractual liability, which in most civil-law systems, including Vietnam's, requires proof of an unlawful act, damage, a causal link and, in most cases, fault ^[8]. Because a smart contract does not pause for a human decision, the customary distinction between the bank's own fault and an intervening third-party cause becomes harder to draw, since

the "act" that caused the damage was performed by code that the bank chose to deploy but did not directly control at the moment of the loss.

The attribution problem

The central doctrinal difficulty is attribution: whose act is the act of the AI system? Three candidates typically compete for responsibility. The bank, as deployer, benefits commercially from the system and is best placed to select, configure, monitor and insure against its risks, which supports treating the system's acts as the bank's own acts for civil-liability purposes, in the same way that an employer answers for an employee acting within the scope of employment. The technology vendor, as developer, controls the design, training data and safety testing of the system and may be liable in product-liability terms if the system was defective when supplied, independently of any fault on the part of the bank that deployed it. The customer, finally, bears responsibility only to the extent that the loss resulted from the customer's own instructions, misuse of the interface, or failure to review a term that a reasonable customer should have queried. None of these three positions is exclusive; in most cases, liability should properly be shared, but no single provision of Vietnamese law currently states how that sharing should occur when the intervening cause is autonomous code rather than a human agent.

Types of damage typical of banking practice

In banking, the damage caused by AI-concluded and AI-executed smart contracts commonly falls into four categories: erroneous or unauthorised disbursement or transfer of funds caused by a coding or configuration error; loss caused by a flawed automated negotiation that commits the bank, or binds the customer, to terms that a human would not have accepted; loss caused by manipulated or inaccurate oracle data that triggers an unwarranted execution, such as a wrongful margin call or an incorrect interest reset; and loss caused by the system's failure to perform when a condition that should have triggered execution was not correctly recognised, leaving an obligation unfulfilled at a critical moment, for example in a time-sensitive trade-finance settlement.

Comparative legal experience

1. European Union

The European Union has approached the problem primarily through product-safety and product-liability law rather than through a bespoke AI-contract-liability regime. The recast Product Liability Directive, Regulation (EU) 2024/2853, expressly extends the concept of a "product" to software and AI systems, and introduces a rebuttable presumption that a product was defective, and that the defect caused the damage, once the claimant shows that the defendant failed to disclose relevant technical or algorithmic information, easing the claimant's burden in cases of algorithmic opacity ^[9]. In 2025 the European Commission withdrew its separate proposal for an AI Liability Directive, which would have created a general presumption of causal fault for high-risk AI systems, leaving Member States' general tort law, supplemented by the Product Liability Directive and the Artificial Intelligence Act, Regulation (EU) 2024/1689, to govern most claims ^[10, 11]. The Artificial Intelligence Act classifies AI systems used for creditworthiness assessment as high-risk and imposes duties of risk management, data

governance, logging, transparency and human oversight, which, while primarily regulatory rather than compensatory, create documentary evidence that a claimant can use to establish fault under ordinary tort rules. The Union's approach therefore relies on a strengthened evidentiary presumption rather than on a rule that directly attributes a smart contract's autonomous act to a specific person.

2. United States

United States law does not treat an AI-concluded contract as void merely because no natural person reviewed the specific term at issue. The Uniform Electronic Transactions Act, adopted in nearly every state, provides that a contract may be formed by the interaction of an "electronic agent" and an individual, or between two electronic agents, and that a person is bound by the actions of an electronic agent that the person has chosen to use, even if no individual was aware of or reviewed the agent's specific actions^[12]. This attribution rule effectively treats the deploying party as the author of its own agent's acts, which resolves the contract-formation question but does not, by itself, resolve who ultimately bears the loss between the bank and its technology vendor. That allocation is generally left to the ordinary law of negligence, breach of warranty and product liability, together with the contractual indemnities that banks negotiate with their software vendors, and to sector-specific supervisory expectations such as the Federal Reserve's model-risk-management guidance, which requires banks to validate and monitor the models they deploy^[13].

3. United Kingdom

The United Kingdom has developed the most direct doctrinal analysis of smart-contract liability among the jurisdictions examined. The UK Jurisdiction Taskforce's Legal Statement on Cryptoassets and Smart Contracts concluded that a smart contract can satisfy the ordinary requirements of offer, acceptance, consideration and intention to create legal relations under English law, so that a coded contract is, in principle, enforceable like any other^[14]. Building on this, the Law Commission's 2021 report on smart legal contracts recommended that existing contract law, rather than a new statutory regime, is generally adequate to resolve disputes over automated performance, while flagging that the treatment of coding errors, the allocation of the risk of an unintended automatic execution, and the interaction between on-chain finality and off-chain remedies required further clarification through case law and standard contract drafting^[15]. The English approach therefore favours contractual risk allocation, negotiated indemnities and carefully drafted "kill switch" or override clauses over statutory attribution rules.

4. Singapore

Singapore combines a general attribution rule with sector-specific supervisory principles. Sections 13 and 14 of the Electronic Transactions Act provide that an expression of will or other statement is not without legal effect merely because it was generated by an automated system, and that a party who uses an automated system to form a contract is bound by the resulting contract, subject to limited relief where an individual made an input error and the system gave no opportunity to correct it^[16]. For the financial sector specifically, the Monetary Authority of Singapore's FEAT principles and its subsequent guidelines on AI risk

management place explicit responsibility on the board and senior management of a financial institution for the outcomes of the AI systems it deploys, reinforcing, at the level of prudential supervision, the same attribution that the Electronic Transactions Act establishes at the level of private law^[17]. This layered structure, a general civil-law attribution rule combined with sector-specific accountability duties, is the model most directly relevant to Vietnam's banking sector.

The Vietnamese legal framework and its shortcomings

Vietnamese civil law was not drafted with autonomous contracting in mind. The Civil Code 2015 defines a civil transaction as an act reflecting the will of a subject and requires that the parties to a contract have the intention to establish, change or terminate civil rights and obligations, a formulation that assumes a human or corporate will behind every clause^[18]. The Code's provisions on liability for breach of obligation, and its general tort provision, both premise liability on the fault of the person who caused the damage, without addressing how fault should be assessed when the immediate cause of the damage is an autonomous system rather than a natural person's direct act^[18].

The Law on Electronic Transactions 2023 takes a first step toward closing this gap. Article 34 recognises transactions performed in whole or in part through an automated information system and provides that the person who deploys such a system is responsible for the results the system produces, in the same manner as if that person had performed the transaction directly^[4]. This is functionally similar to the attribution rules of Singapore and the United States, and it is a workable foundation for AI-concluded banking contracts. However, Article 34 was drafted before Vietnam's dedicated AI legislation and does not distinguish between a fixed, deterministic script and a system exhibiting the autonomy and opacity of a modern AI negotiation agent, nor does it address how liability should be divided between the deploying bank and the vendor that supplied the system. The Law on Artificial Intelligence, Law No. 134/2025/QH15, adopts a risk-based classification and is likely to place AI systems used in banking, including systems used for credit decisions and automated transaction processing, within the high-risk category, triggering duties of conformity assessment, registration, human oversight and incident reporting^[3]. These duties strengthen the evidentiary record that a court could later use to assess fault, in a manner similar to the European Artificial Intelligence Act, but the law does not itself state a rule of civil liability or a rule for allocating loss between deployer and developer, leaving that question to future decrees and to general civil law. The State Bank of Vietnam's draft Circular on the safety, risk management and conditions for the application of AI in banking likewise focuses on prudential safeguards, human oversight and customer notification rather than on compensation for damage once a loss has already occurred^[2].

Taken together, Vietnamese law today provides an attribution rule of general application through the Law on Electronic Transactions, a set of prudential duties through the Law on Artificial Intelligence and the draft Circular of the State Bank, and a fault-based civil-liability regime through the Civil Code, but it does not connect these three layers into a coherent rule for AI-concluded and AI-executed smart contracts in banking. There is no

presumption easing the customer's burden of proving fault in the face of an opaque model, no clear default rule dividing liability between the bank and its technology vendor, and no requirement that a bank maintain the kind of auditable log that would allow a court to reconstruct why a smart contract executed as it did.

Lessons for Vietnam

Drawing on the comparative experience examined above, several concrete reforms would strengthen Vietnam's framework for civil liability arising from AI-concluded and AI-executed smart contracts in banking. These reforms are not offered as a single, once-and-for-all statute; because AI-driven contracting is itself a moving target, each recommendation is framed so that it can be implemented incrementally, through decree, circular and supervisory guidance, and can be revised as the technology and market practice evolve.

First, the attribution rule in Article 34 of the Law on Electronic Transactions should be clarified, by decree or by sectoral circular, to state expressly that the acts and outputs of an AI system used to conclude or perform a banking contract are attributed to the credit institution that deploys the system, following the approach of Singapore's Electronic Transactions Act and the United States' Uniform Electronic Transactions Act ^[4, 12, 16]. As currently drafted, Article 34 speaks broadly of an "automated information system" and does not distinguish between a fixed, rule-based script that simply executes a pre-agreed instruction and a modern AI agent that negotiates a term or selects a counterparty on its own initiative. A clarifying decree should therefore confirm that this distinction does not matter for attribution: whether the system is deterministic or adaptive, its output remains the legal act of the credit institution that chose to deploy it, configured its objectives and put it into commercial use. This would remove any doubt that a smart contract negotiated or executed without contemporaneous human review is nonetheless a valid and attributable act of the bank, and it would give courts a clear starting point from which to allocate loss, rather than leaving them to debate, in every dispute, whether an AI-generated term can be treated as an act of the bank at all. A clear attribution rule also benefits customers directly, because it removes the risk that a bank could argue that an unfavourable or erroneous AI-generated term is not binding precisely because no employee reviewed it.

Second, Vietnam should introduce a rebuttable presumption of fault, or of defectiveness, for high-risk banking AI systems, modelled on the European Union's recast Product Liability Directive, under which a bank or vendor that fails to disclose the technical information needed to assess the system's design or training bears the burden of proving that the system was not the cause of the customer's loss ^[9]. In practice, a customer harmed by an opaque credit-scoring or contract-negotiation model has no way to obtain the training data, the model architecture or the internal logs that would allow a conventional fault-based claim to succeed, while the bank and its vendor hold all of this information. Reversing the burden of proof once the claimant has shown a plausible link between the AI system and the loss, and once the defendant has failed to produce the relevant technical documentation on request, would correct this structural imbalance without requiring the claimant to reconstruct the internal reasoning of a system that was never designed to be

explained to a layperson. This shifts the practical difficulty of proving fault in an opaque system away from the customer, who has no access to the model, and toward the party that built or deployed it, and it also gives banks and vendors a strong incentive to keep the kind of documentation, testing records and validation reports that the Law on Artificial Intelligence's conformity-assessment regime already anticipates, so that compliance with the AI Law and defence against a civil claim become mutually reinforcing rather than separate exercises.

Third, the duties of logging and record-keeping already implicit in the Law on Artificial Intelligence and the draft Circular of the State Bank should be made explicit for smart contracts specifically, requiring banks to retain an auditable record of the data, parameters and version of the model that produced a given contractual term or a given execution decision, so that a dispute can be reconstructed after the fact ^[2, 3]. At a minimum, such a record should capture the version of the model in use at the moment of contract formation or execution, the input data or market feed that triggered the decision, any human override or approval step that took place, and the identity of the vendor responsible for that version of the system. Because a smart contract, once executed, cannot simply be undone, the value of this record lies less in preventing the loss than in allowing a court, a supervisor or an internal compliance function to establish afterwards exactly which version of the system acted, on what information, and whether the outcome fell inside or outside its intended design parameters. Without such a record, both the rebuttable presumption proposed above and the ordinary fault-based claim under the Civil Code would be difficult to apply in practice, because neither the customer nor the court would have any reliable way to test the bank's account of what happened.

Fourth, because the deploying bank and the technology vendor will often share responsibility in practice, the State Bank of Vietnam should encourage, through supervisory guidance, standard contractual terms between banks and AI vendors that allocate risk clearly, including indemnities, service-level commitments on model accuracy and availability, and a requirement that vendors carry professional-liability insurance proportionate to the scale of banking deployment, an approach consistent with the contractual risk-allocation model favoured in the United Kingdom ^[14, 15]. Left to ordinary commercial negotiation, smaller banks and fintech partners often have limited bargaining power against large technology vendors, and vendor contracts may disclaim liability for exactly the kind of loss that a smart contract is most likely to cause, such as an incorrect execution triggered by a defect in the underlying code. Supervisory model clauses, of the kind that the State Bank already issues for other categories of outsourcing and technology risk, would give banks a benchmark against which to negotiate, would make indemnity and insurance terms more consistent across the sector, and would ensure that when a loss does occur, the customer is not left trying to establish which of two contracting parties, the bank or its vendor, is ultimately responsible, since that question would already have been settled, as between the bank and the vendor, by the underlying commercial contract.

Fifth, consistent with the principle of adaptive, ongoing supervision that already underlies Vietnam's emerging AI governance framework, the State Bank should consider a

regulatory sandbox specifically for smart-contract banking products, allowing new AI-concluded contract structures to be tested under supervisory observation before they are deployed at scale, so that liability rules can be refined based on observed practice rather than fixed in advance for a technology that continues to change quickly^[2, 6]. A sandbox of this kind would allow the State Bank to observe, in a controlled environment and with a limited customer base, how a given smart-contract structure actually performs, including how frequently oracle data proves unreliable, how often human override is exercised, and what kinds of disputes arise, before the same structure is rolled out across the wider market. The lessons learned within the sandbox could then feed directly into the calibration of the presumption of fault, the scope of the mandatory logging duty, and the content of the standard vendor contract terms described above, so that the liability regime as a whole develops through an iterative and evidence-based process rather than through a single legislative act that risks becoming outdated as soon as the underlying technology changes. This approach is also consistent with the broader lesson of the comparative survey above: no jurisdiction examined in this article has treated AI-contract liability as a problem that can be solved once, and each instead relies on a combination of general private-law rules, sector-specific supervisory duties and continuous regulatory learning.

Conclusion

AI-concluded and AI-executed smart contracts are no longer a theoretical possibility for the banking sector; they already determine how loans are disbursed, how trade-finance instruments settle and how treasury positions are managed. When such a contract causes damage, the autonomy, opacity and irreversibility of the underlying code make it difficult to apply civil-liability doctrine that was built around a human party's fault and intention. The comparative experience of the European Union, the United States, the United Kingdom and Singapore shows a common direction of travel: attributing the acts of an automated system to the person who deploys it, easing the evidentiary burden faced by the party harmed by an opaque system, and relying on contractual risk allocation between deployer and developer to divide the loss in practice. Vietnamese law has taken the first step toward this model through the Law on Electronic Transactions and the Law on Artificial Intelligence, but it has not yet connected these instruments into a coherent civil-liability regime for banking smart contracts. A clearer attribution rule, a rebuttable presumption of fault for high-risk systems, mandatory audit trails and standard risk-allocation contracts between banks and vendors would together give Vietnamese courts, banks and customers the certainty that this fast-growing form of banking practice currently lacks. Such reforms are essential in the future.

References

1. Thi truong Tai chinh Tien te. AI in banking: from credit scoring to fraud prevention, 2025. Available at: <https://thitruongtaichinhiente.vn/ai-trong-ngan-hang-tu-cham-diem-tin-dung-den-phong-chong-gian-lan-70341.html> [Accessed 28 July 2026]
2. State Bank of Vietnam. Draft Circular on safety, risk management and conditions for the application of artificial intelligence in the banking sector, 2026. Available at: <https://tapchinganhang.gov.vn/hoan-thien-phap-ly-ve-ung-dung-tri-tue-nhan-tao-trong-hanh-trinh-chuyen-doi-so-ngan-hang-17099.html> [Accessed 28 July 2026]
3. National Assembly of Vietnam. Law No. 134/2025/QH15 on Artificial Intelligence, 2025. Available at: <https://english.luatvietnam.vn/law-no-134-2025-qh15-dated-december-10-2025-of-the-national-assembly-on-artificial-intelligence-422299-doc1.html> [Accessed 28 July 2026]
4. National Assembly of Vietnam. Law No. 20/2023/QH15 on Electronic Transactions, Article 34, 2023.
5. Werbach K, Cornell N. Contracts Ex Machina. *Duke Law Journal*, 2017;67:313-382.
6. Kolt N, Maas MM, Hadfield-Menell D, et al. Lessons from complex systems science for AI governance. *Patterns*, 2025, 6(8). Available at: [https://www.cell.com/patterns/fulltext/S2666-3899\(25\)00189-8](https://www.cell.com/patterns/fulltext/S2666-3899(25)00189-8) [Accessed 28 July 2026]
7. Agentic AI and Financial Governance, 2026.
8. Civil Code of Vietnam, Law No. 91/2015/QH13, Articles 116, 119, 351, 584.
9. Regulation (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products (recast Product Liability Directive). *Official Journal of the European Union*, 2024.
10. European Commission. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final, withdrawn 2025.
11. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, 2024.
12. Uniform Electronic Transactions Act, Section 14 (Automated Transactions), National Conference of Commissioners on Uniform State Laws, 1999.
13. Modulos. Operationalise the EU AI Act in financial services, 2025. Available at: <https://www.modulos.ai/industries/financial-services/> [Accessed 28 July 2026]
14. UK Jurisdiction Taskforce. Legal Statement on Cryptoassets and Smart Contracts, LawTech Delivery Panel, 2019.
15. Law Commission of England and Wales. Smart Legal Contracts: Advice to Government, 2021. Available at: <https://lawcom.gov.uk/project/smart-contracts/> [Accessed 28 July 2026]
16. Electronic Transactions Act 1998 (Cap. 88A, Singapore), sections 13-14.
17. Monetary Authority of Singapore. Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector, 2018. Available at: <https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat> [Accessed 28 July 2026]
18. Civil Code of Vietnam, Law No. 91/2015/QH13, Articles 116, 119, 351, 584.