

STABLECOINS: IMPUTATION GAPS AND CHALLENGES OF CIVIL LIABILITY IN THE TOKENIZED ECONOMY

Victor Hugo Gimenez Gonçalves *

Abstract: This article examines whether the use of stablecoins as instruments for financing agribusiness produces civil-liability imputation gaps that are incompatible with traditional dogmatic assumptions. Through a hypothetical-deductive method and a dogmatic-functional approach, the study analyzes stablecoins, tokenized agribusiness financing, decentralized finance, and comparative regulatory frameworks in the European Union, the United States, and Brazil. It argues that the operational decentralization promoted by stablecoins fragments the poles of liability, weakens linear causation, and renders the classical fault paradigm insufficient. The article proposes an interpretive model based on three pillars: layered proportional liability, duties of governance and due diligence, and accountability as an autonomous criterion of imputation. It concludes that civil liability has the dogmatic resources necessary to respond to the tokenized economy, provided that causation, fault, and risk are reconstructed in light of the structural complexity of blockchain-based arrangements.

Keywords: stablecoins; civil liability; tokenized economy; agribusiness financing; blockchain; accountability.

INTRODUCTION

Since its original conception with the Bitcoin protocol in 2008, blockchain technology has caused profound reconfigurations in financial intermediation structures and in the very notion of institutional trust that supports obligations, representing a break from traditional models of trust by replacing centralized intermediaries with distributed consensus protocols.¹ In this context, the emergence of cryptoassets, the proliferation of decentralized finance (DeFi) protocols, and the expansion of processes for tokenizing real-world assets confront law with unprecedented challenges, whose resolution requires not only normative adaptations but also a reassessment of the very dogmatic foundations of civil liability.

As Mafalda Miranda Barbosa observes, the Industrial Revolution represented an inflection point for the dogmatics of civil liability by subjecting the labor environment to the logic of mechanization and, as a result, multiplying the occurrence of harms not always traceable to personally imputable conduct or to the agent's culpable act, thereby

* Master's student in Law, concentration area in Law in Economic and Social Relations, research line in Business Law in the Brazilian and International Economic Order, Milton Campos Law School, Nova Lima/MG, Brazil. Email: vh2g.or@gmail.com / ORCID iD: <https://orcid.org/0000-0002-4794-9761>

¹ Dirk A. Zetsche, Douglas W. Arner & Ross P. Buckley, Decentralized Finance (DeFi), 6(2) Journal of Financial Regulation (Sept. 2020), at 180.

leading to the progressive construction of strict-liability or risk-based hypotheses.² The contemporary technological revolution, marked by system autonomy, decentralization, and self-learning, imposes an analogous yet qualitatively distinct challenge. It is not merely a matter of machines escaping human control, but of entire architectures of economic governance that dispense with identifiable focal agents.

Within this transformative scenario, stablecoins occupy a central position. Designed to offer value stability in an ecosystem marked by volatility, these cryptoassets perform functions as stores of value, means of payment, and settlement instruments in decentralized protocols. Their relevance transcends the speculative universe: stablecoins are increasingly being used as monetary infrastructure for sectoral financing arrangements, including in agribusiness, a sector that accounts for a substantial share of Brazil's Gross Domestic Product and whose production chain is characterized by high contractual complexity, seasonality, and dependence on specialized credit instruments.

The central thesis advanced in this article is that the operational decentralization promoted by stablecoins in agribusiness financing produces a structural fragmentation of the poles of liability, which does not find an adequate response in classical imputation models and requires the construction of specific normative criteria.

The research problem guiding this study may be formulated as follows: to what extent does the use of stablecoins as instruments for financing agribusiness generate civil-liability imputation gaps that are incompatible with traditional dogmatic assumptions, and what interpretive criteria may be constructed to remedy those insufficiencies? The central hypothesis is that the operational decentralization promoted by stablecoins in agribusiness financing produces a structural fragmentation of the poles of liability, which does not find an adequate response in classical models of imputation based on individual fault or on the risk of an activity performed by identifiable subjects, thereby requiring the construction of specific normative criteria grounded in duties of accountability, technological governance, and layered proportional liability.

The article adopts the hypothetical-deductive method, with a dogmatic-functional approach. It conducts a national and foreign bibliographic review on civil liability, blockchain, and cryptoassets, in addition to a comparative analysis of the regulatory frameworks of the European Union (MiCA), the United States (the fragmented SEC/CFTC arrangement), and Brazil (Law No. 14,478/2022 and infralegal acts). It is complemented by the examination of empirical events involving the collapse of stablecoins, especially TerraUSD/Luna, and of their effects on investors and economic agents.

² Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 206.

The research is justified on three levels. On the theoretical level, the tokenization of agribusiness assets backed by stablecoins challenges consolidated assumptions of civil liability and requires the reassessment of categories such as authorship, intermediation, and causation. On the social level, the diffusion of such arrangements in an environment of informational asymmetry may increase the exposure of producers and retail investors to patrimonial losses that are difficult to redress. On the economic-normative level, although tokenization promises to reduce intermediation costs and broaden access to credit, its sustainability depends on a protective legal regime that remains insufficiently delineated in Brazil, given that Law No. 14,478/2022 and infralegal regulation do not structure the civil liability applicable to stablecoin transactions.

I. STABLECOINS AND THE TOKENIZED ECONOMY: CONCEPTUAL AND FUNCTIONAL DELIMITATION

The concept of a stablecoin refers, in general terms, to cryptoassets structured to maintain the parity of their market value with a reference asset, usually a fiat currency such as the United States dollar or, alternatively, a basket of assets.³ Unlike cryptoassets such as Bitcoin, whose price volatility is a constitutive feature, stablecoins were designed to operate as stability instruments within the crypto ecosystem, serving as a bridge between the traditional economy and decentralized finance.⁴

According to Coinbase, the second-largest platform in the sector, stablecoins represent one of the greatest opportunities in the crypto ecosystem because they play a crucial role by allowing market participants to price assets in a common currency and keep assets on the blockchain during periods of high market volatility. For its part, the definition adopted in this article understands stablecoins as cryptoassets endowed with a value-stabilization mechanism in relation to a reference asset, issued by a centralized entity or generated by a decentralized protocol, and performing functions as means of payment, units of account, or stores of value in the DeFi ecosystem.⁵

A. Typology and Stabilization Mechanisms

Scholarship and market practice identify three fundamental categories of stablecoins, each with its own legal implications that require individualized examination. The first category comprises fiat-collateralized stablecoins, in which the issuer maintains reserves in fiat currency (or equivalents, such as short-term government securities)

³ Ahmed Mahrous, Maurantonio Caprolu & Roberto Di Pietro, *Stablecoins: Fundamentals, Emerging Issues, and Open Challenges* (2025), at 1.

⁴ Dirk A. Zetsche, Douglas W. Arner & Ross P. Buckley, *Decentralized Finance (DeFi)*, 6(2) *Journal of Financial Regulation* (Sept. 2020), at 195-196.

⁵ Bank for International Settlements, material cited in the manuscript (2024).

corresponding to the total value of the issued tokens. Tether (USDT) and USD Coin (USDC) are paradigmatic examples.

With respect to this category, the Bank for International Settlements (BIS), an institution recognized as the “central bank of central banks,” adopts the following definition of a fiat-collateralized stablecoin:

Stablecoins are crypto tokens that live on distributed ledgers (i.e., “on-chain”) and promise to be worth always a dollar, providing par convertibility on demand. Stablecoin issuers defend this promise by holding (mostly) fiat-denominated (i.e., “off-chain”) short-term assets, such as Treasuries, high-quality commercial paper, repurchase agreements and bank deposits. The combination of money-like demandable liabilities with backing assets that may become illiquid implies that stablecoin issuers’ liquidity transformation exposes them to runs.⁶⁷

In this context, the BIS institutional definition itself makes it possible to delimit the economic-legal core of the fiat-collateralized arrangement: the promised parity does not derive from an autonomous protocol mechanism, but from confidence in the issuer’s ability to honor immediate redemptions based on off-chain reserves composed of short-term assets. The token’s stability therefore comes to depend directly on the solvency, liquidity management, and degree of transparency of the centralized issuer, introducing counterparty and run risks functionally analogous to those observed in traditional financial institutions.⁸

The implication for civil liability is direct: there is an identifiable issuer, endowed with legal personality, upon which duties to maintain reserves and provide information fall. The breach of those duties constitutes, in principle, a basis for liability for harms caused to token holders.

The problem, however, lies in the persistent opacity of those reserves, because the impossibility of independently verifying the backing makes structurally plausible a divergence between what is publicly asserted and what effectively composes the guarantees. This is illustrated by the action brought by the New York Attorney General against Bitfinex and Tether, both controlled by iFinex (based in Hong Kong), precisely on the allegation that the narrative of full dollar backing did not correspond to reality and that “Tether’s claims that its virtual currency was fully backed by U.S. dollars at all times was a lie”,⁹ evidencing that the mere existence

⁶ Rashad Ahmed, Iñaki Aldasoro & Channele Duley, Public Information and Stablecoin Runs, BIS Working Papers No. 1164 (Jan. 2024), at 1.

⁷ Original quotation in English preserved from the cited source.

⁸ Gary B. Gorton & Jeffery Zhang, Taming Wildcat Stablecoins, 90(3) *University of Chicago Law Review* 909 (2023); Christian Catalini, Alonso de Gortari & Nihar Shah, Some Simple Economics of Stablecoins, 14 *Annual Review of Financial Economics* 117 (2022).

⁹ Gary B. Gorton & Jeffery Zhang, Taming Wildcat Stablecoins, 90(3) *University of Chicago Law Review* 909 (2023), at 917.

of a centralized issuer does not, in itself, guarantee the effectiveness of protection.

The second category comprises crypto-collateralized stablecoins, backed by other cryptoassets through overcollateralization mechanisms managed by smart contracts. DAI, issued by the MakerDAO protocol, exemplifies this type: users deposit cryptoassets (for example, Ether) as collateral and receive DAI in an amount lower than the deposited value, in order to absorb the volatility of the collateral.¹⁰

Here, liability is dispersed among protocol developers, governance-token holders (MKR), and users who maintain collateral positions. There is no centralized issuer in the traditional sense; the system is governed by a decentralized autonomous organization (DAO), whose decisions result from voting among governance-token holders. The question “who answers for the harm?” becomes structurally more complex because the decision that parameterizes liquidation criteria is collective, pseudonymous, and technologically mediated.¹¹

Costa observes that distributed ledger technologies ensure the immutability of transaction history and the transparency of operations, reducing information asymmetries, with benefits in terms of governance and participant responsibility.¹² However, as the author notes, this transparency is technical and not cognitive: the code is open, but it is not understandable to the average user.

The third category, of greatest dogmatic complexity, is that of algorithmic or non-collateralized stablecoins. Devoid of backing in real assets, such stablecoins depend exclusively on algorithms that automatically adjust the supply of tokens in circulation according to price fluctuations, creating economic incentives for participants to arbitrage the price back to parity.¹³

The collapse of the TerraUSD/Luna ecosystem in May 2022, which vaporized more than USD 40 billion in market value in less than a week, constitutes empirical demonstration of the intrinsic fragility of this model and of its capacity to generate systemic-scale harms. According to Krause, algorithmic stablecoins are susceptible to “death spirals,” in which an initial loss of confidence triggers a run for redemptions that, in turn, deepens depreciation until total collapse.¹⁴

¹⁰ Agostino Capponi, Garud Iyengar & Jay Sethuraman, *Decentralized Finance: Protocols, Risks, and Governance*, Foundations and Trends in Finance (2023), at 21-22.

¹¹ Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4(2) *Stanford Journal of Blockchain Law & Policy* (2020).

¹² Isac Silveira da Costa, *O futuro é infungível: tokenização, non-fungible tokens (NFTs) e novos desafios na aplicação do conceito de valor mobiliário*, *Revista de Direito das Sociedades e dos Valores Mobiliários*, special vol., 283 (Dec. 2021), at 290.

¹³ Alexander Lipton, Aetienne Sardon, Fabian Schär & Christian Schüpbach, *Stablecoins, Digital Currency, and the Future of Money* (2020), at 6.

¹⁴ David Krause, *Algorithmic Stablecoins: Mechanisms, Risks, and Lessons from the Fall of TerraUSD* (Marquette University 2024), at 8.

From the perspective of civil liability, the algorithmic stablecoin represents the limiting case of the imputation gap: when the harm results from the failure of a purely automated mechanism, without tangible collateral and without a centralized issuer, the classical assumptions of imputation - fault, individualized causal nexus, and responsible subject - are simultaneously emptied.¹⁵

B. Economic Functions in the DeFi Ecosystem and Infrastructural Relevance

The intermediation function exercised by stablecoins is related to the broader phenomenon of disintermediation promoted by DeFi. As Bonnet points out, decentralized finance promises to replace centralized intermediaries with automated and transparent platforms supported by smart contracts.¹⁶ The promise of cost reduction and financial inclusion, however, does not eliminate risks; rather, it redistributes them among participants frequently deprived of the technical conditions to assess them.¹⁷ The French Autorité de Contrôle Prudentiel et de Résolution (ACPR) defines DeFi as a set of cryptoasset services comparable to financial services, carried out without the intervention of an intermediary, in which the transparency and immutability of computer code replace trust among actors; it is therefore disintermediated finance before it is decentralized finance.¹⁸

C. Operational Definition of the Core Concepts and Analytical Scope

Conceptual precision is an indispensable methodological requirement in a study that moves among diverse disciplines - civil law, financial law, computer science, and economics. It is therefore necessary to establish the operational definitions that guide the analysis. An imputation gap means a situation in which, once harm has occurred, the application of the existing normative criteria for assigning civil liability does not make it possible to identify, with sufficient legal certainty, the subject obliged to repair it, whether because there is no focal agent, because the harmful conduct is fragmented among multiple actors, because proof of causal nexus is impossible, or because of a combination of these factors.¹⁹ The

¹⁵ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018), at 187.

¹⁶ Joris Bonnet, *Blockchain et finance décentralisée* (Ph.D. dissertation, Université de Paris, École doctorale 101, 2024), at 27.

¹⁷ Agata Ferreira, *The Curious Case of Stablecoins - Balancing Risks and Rewards?*, 24(4) *Journal of International Economic Law* 755 (2021); Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022).

¹⁸ Katrin Schuler, Ann Sofie Cloots & Fabian Schär, *On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 10(2) *Journal of Financial Regulation* 213 (2024).

¹⁹ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability*

gap is not equivalent to a mere evidentiary difficulty: it is a dogmatic insufficiency, in which the normative criteria themselves - and not merely the evidence - are inadequate to the phenomenon.²⁰

The tokenized economy designates the set of economic and legal relationships that use tokens recorded on blockchain networks as instruments for representing, circulating, and settling rights, ranging from the tokenization of real-world assets (real estate, receivables, commodities) to the issuance of native cryptoassets. As Costa observes, tokenization is not an ontologically new phenomenon in the abstraction process that allows corporeal or intangible assets to be referenced in data systems; what is new is the technological infrastructure that supports it and the legal effects that derive from it.²¹

Tokenized agribusiness financing means the use of blockchain infrastructure to structure, distribute, and settle credit or investment transactions linked to the agricultural production chain, including, but not limited to, the issuance of tokens representing crop receivables, tokenized agribusiness receivables certificates, and decentralized loans collateralized by agricultural commodity tokens. These transactions may be settled in stablecoins, which introduces the specific layer of risk that constitutes the object of this study.²²

Distributed causation designates the phenomenon whereby the harmful result cannot be attributed to a single conduct but results from the cumulative and interdependent interaction of multiple acts and omissions by diverse agents (human and non-human), distributed across different layers of the tokenized value chain. The expression draws on the concept of distributed liability of distributed ledgers, coined by Zetsche, Buckley, and Arner, but expands it to include the specifically causal dimension of the problem, not merely the subjective dimension of liability.²³

of Distributed Ledgers: Legal Risks of Blockchain, 2018(4) University of Illinois Law Review 1361 (2018); Mafalda Miranda Barbosa, Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova, 1 Revista de Direito da Responsabilidade 206 (2019).

²⁰ Mafalda Miranda Barbosa, Do Nexo de Causalidade ao Nexo de Imputação: Contributo para a Compreensão da Natureza Binária e Personalística do Requisito Causal ao Nível da Responsabilidade Civil Extracontratual (Princípios 2013); Rafael de Freitas Valle Dresch, Fundamentos da Responsabilidade Civil pelo Fato do Produto e do Serviço: Um Debate Jurídico-Filosófico entre o Formalismo e o Funcionalismo no Direito Privado (Livraria do Advogado 2009).

²¹ Isac Silveira da Costa, O futuro é infungível: tokenização, non-fungible tokens (NFTs) e novos desafios na aplicação do conceito de valor mobiliário, Revista de Direito das Sociedades e dos Valores Mobiliários, special vol., 283 (Dec. 2021), at 295; Dayana de Carvalho Uhdre, Blockchain, Tokens e Criptomoedas: Análise Jurídica (Almedina 2021); Demir Murat Aksoy & Zümrüt Ecevit Sati, Tokenization of Real World Assets: An Agricultural Token System Implementation Based on Blockchain Architecture, 2(1) The Journal of Applied Engineering and Agriculture Sciences 24 (2025).

²² Isac Silveira da Costa, work cited in the manuscript on DeFi and tokenization (2022); José Luiz de Moura Faleiros Júnior, Responsabilidade civil e o mercado de criptoativos, in Temas Atuais de Direito Digital (São Paulo, 2023).

²³ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, The Distributed Liability

II. TOKENIZATION OF AGRIBUSINESS FINANCING: CONVERGENCES AND TENSIONS

Brazilian agribusiness is characterized by a complex financing structure, historically organized around typical instruments such as the Rural Product Note (Cédula de Produto Rural - CPR), Agribusiness Receivables Certificates (Certificados de Recebíveis do Agronegócio - CRA), Agribusiness Credit Letters (Letras de Crédito do Agronegócio - LCA), and Agricultural Deposit Certificates (Certificados de Depósito Agropecuário - CDA), governed by Law No. 11,076/2004 and supplementary legislation, subject to the supervision of the CVM and the Central Bank of Brazil, and operating within an institutionalized intermediation chain.

The tokenization of agribusiness assets represents the transposition of this logic to blockchain infrastructure, with promises of reducing operating costs, broadening access to credit, fractionalizing investments, and automating the settlement of obligations.²⁴ As Costa records, there is currently great expectation regarding the possibility of reducing custody, clearing, and settlement costs in operations based on DeFi projects, in which participants in a trading and property-registration system may be nodes of a blockchain network, allowing asset lending, payments, and the granting of guarantees without centralized market infrastructures.²⁵

A. From Securitization to Tokenization

Costa observes that tokenization is not an ontologically new phenomenon in the abstraction process that allows corporeal or intangible assets to be referenced in data systems, with securitization serving as an antecedent of this disruptive technological movement.²⁶ Nevertheless, the imputation problems that emerge from agribusiness tokenization through stablecoins are qualitatively distinct from those encountered in conventional securitization because the agent structuring the operation may be an autonomous protocol without legal personality; settlement

of Distributed Ledgers: Legal Risks of Blockchain, 2018(4) University of Illinois Law Review 1361 (2018), at 1361; Mafalda Miranda Barbosa, Do Nexo de Causalidade ao Nexo de Imputação: Contributo para a Compreensão da Natureza Binária e Personalística do Requisito Causal ao Nível da Responsabilidade Civil Extracontratual (Princípios 2013); Agostino Capponi, Garud Iyengar & Jay Sethuraman, Decentralized Finance: Protocols, Risks, and Governance, Foundations and Trends in Finance (2023).

²⁴ Dayana de Carvalho Uhdre, Blockchain, Tokens e Criptomoedas: Análise Jurídica (Almedina 2021); Yan Chen, Lin William Cong & Jianwei Xia, Blockchain Disruption and Smart Contracts, 35(4) The Review of Financial Studies 1495 (2022).

²⁵ Isac Silveira da Costa, work cited in the manuscript on DeFi and tokenization (2022), at 142.

²⁶ Isac Silveira da Costa, O futuro é infungível: tokenização, non-fungible tokens (NFTs) e novos desafios na aplicação do conceito de valor mobiliário, Revista de Direito das Sociedades e dos Valores Mobiliários, special vol., 283 (Dec. 2021), at 295-296.

occurs through an asset whose stability depends on technological mechanisms subject to failure; participants may operate under pseudonyms on public networks; and the competent jurisdiction is often indeterminate.²⁷

B. Specific Risks of Stablecoins in Tokenized Agribusiness

The risks arising from the use of stablecoins in agribusiness financing transactions may be systematized into four axes, each with distinct implications for the imputation of civil liability: depeg risk, counterparty risk, technological risk, and regulatory risk.

Depeg risk consists of the loss of parity between the stablecoin and its reference asset, an event that directly compromises the value of obligations denominated in it. In the agribusiness context, where production cycles are long and crop costs cannot be postponed, a depeg event may render the entire agricultural operation unviable, spreading losses along the entire production chain.²⁸ The question that emerges is whether the issuer of the stablecoin answers for the harm because of failure to maintain parity, whether the structurer of the transaction answers because of inadequate choice of the settlement asset, or whether both answer jointly and severally.

Counterparty risk, present above all in centralized stablecoins, lies in dependence on the issuer's solvency and probity. Opacity in the composition of reserves and the absence of mandatory independent auditing constitute sources of potential harm over which the investor has no control and, frequently, no adequate information.²⁹ In this configuration, the issuer occupies a position functionally analogous to that of a financial institution and should be strictly liable for failures in reserve management, based on article 927, sole paragraph, of the Brazilian Civil Code, when the issuing activity, by its nature, entails risk to the rights of others.

Technological risk encompasses vulnerabilities in smart contracts, oracle failures, and cyberattacks. Accumulated experience in the DeFi ecosystem demonstrates that such risks are not merely theoretical, having resulted in the theft of billions of dollars through the exploitation of code flaws.³⁰

²⁷ Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022); Agata Ferreira, *The Curious Case of Stablecoins - Balancing Risks and Rewards?*, 24(4) *Journal of International Economic Law* 755 (2021).

²⁸ Bank for International Settlements, *Stablecoins: Risks, Potential and Regulation*, BIS Working Papers No. 1114 (2023); Gary B. Gorton & Jeffery Zhang, *Taming Wildcat Stablecoins*, 90(3) *University of Chicago Law Review* 909 (2023).

²⁹ European Central Bank, *The Expansion of Functions and Uses of Stablecoins*, Financial Stability Review (Nov. 2021); Financial Stability Board, *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report* (July 2023).

³⁰ Massimo Bartoletti, Stefano Lande, Andrea Loddo & Livio Pompianu,

As Divino points out, the dependence of smart contracts on oracles compromises the trustless characteristic of blockchain because the oracle introduces a point of centralization and potential failure into the system.³¹ Bonnet reinforces that “certain authors see in the oracle a weakness, an Achilles’ heel of blockchain,” insofar as the reintroduction of a point of intermediation into a decentralized protocol recreates a vulnerability in the smart contract.³² In tokenized agribusiness, a vulnerability in the smart contract governing the settlement of tokenized CRAs may result in diversion of funds, premature enforcement of collateral, or incorrect distribution of returns.

Regulatory risk, finally, arises from normative uncertainty. The absence of a specific legal regime for stablecoins in Brazil, the uncertainty about the legal classification of receivables tokens, and the overlap of regulatory competences between the CVM and the Central Bank create an environment of insecurity that amplifies all other risks and, paradoxically, makes the imputation of responsibility more difficult. Uhdre observes in this direction that “the potential fluidity of functionalities exercised by tokens may often hinder the framing of operations within the currently established legal structure”.³³ The practical consequence is that tokenized agribusiness financing operations may exist in a regulatory penumbra in which even the applicable civil-liability regime is unclear.³⁴ Uhdre further reinforces that liability in the context of tokenization requires the construction of interpretive frameworks that consider the functional specificity of tokens and the multiplicity of legal relationships arising from them.³⁵

C. Tokenized Value Chain and the Multiplication of Interposed Agents

The analytical decomposition of the value chain in tokenized agribusiness financing transactions reveals at least eight categories of agents: (i) the stablecoin issuer; (ii) the smart contract developer; (iii) the oracle provider; (iv) the trading platform or DeFi protocol; (v) the

Cryptocurrency Scams: Analysis and Perspectives, 9 IEEE Access (2021); Agostino Capponi, Garud Iyengar & Jay Sethuraman, *Decentralized Finance: Protocols, Risks, and Governance, Foundations and Trends in Finance* (2023).

³¹ Stênio Geraldo Lopes Divino, *Smart contracts: conceitos, limitações, aplicabilidade e desafios*, 4(6) RJLB 2771 (2018), at 2790-2792.

³² Joris Bonnet, *Blockchain et finance décentralisée* (Ph.D. dissertation, Université de Paris, École doctorale 101, 2024), at 310; Cristina Argelich Comelles, *Smart Contracts o Code is Law: Soluciones Legales para la Robotización Contractual*, *InDret*, no. 2 (2020).

³³ Dayana de Carvalho Uhdre, *Blockchain, Tokens e Criptomoedas: Análise Jurídica* (Almedina 2021), at 245-246.

³⁴ Nathan Cortez, *Regulating Disruptive Innovation*, 29 *Berkeley Technology Law Journal* 175 (2014); M. X. Caetano, D. R. dos Santos & C. Arrigoni, *Criptomoedas: seus desafios de regulamentação e os impactos a instituições financeiras centralizadas*, 9(3) *International Journal of Professional Business Review* 1 (2024).

³⁵ Dayana de Carvalho Uhdre, *Blockchain, Tokens e Criptomoedas: Análise Jurídica* (Almedina 2021), at 55.

originator of the credits (the rural producer or securitization company); (vi) the validating nodes of the blockchain network; (vii) the smart contract auditors, when they exist;³⁶ and (viii) the investors, who may exercise governance functions if they hold tokens with voting rights. The multiplication of agents, per se, would already constitute a challenge to imputation. The central argument, however, is that the problem is aggravated by three structural characteristics that distinguish the tokenized economy from traditional intermediation chains: pseudonymity, automaticity, and transnationality.³⁷

Pseudonymity, inherent in most public blockchain networks, makes it difficult to identify the responsible subject. As Costa observes, “if ownership occurs through pseudonyms, we are dealing with a bearer-title mechanism,” creating fertile ground for the concealment of assets and making any act of patrimonial constraint by public authorities unfeasible.³⁸ If the developer of a defective smart contract operates under a pseudonym and without a formal link to a registered legal person, the victim’s indemnification claim encounters an insurmountable procedural obstacle, since civil liability presupposes a subject capable of being sued; when that subject is structurally concealed by the network architecture, the reparatory function of the institute itself is emptied.³⁹

Automaticity aggravates the difficulty. When the harm results from the execution of a smart contract - for example, the automatic liquidation of collateral due to an abrupt fall in the stablecoin’s price - there is no human decision at the moment the harm is caused. The code executes the stipulated clause, and the question of who answers for the harm retroacts to the conception of the code, the governance of the protocol, and ultimately the collective decision that parameterized the liquidation criteria.

Barbosa identifies the issue precisely when asking whether liability may be imputed to the creator of the DAO or to the software agent itself.⁴⁰ The author argues that, because the subjectivization of entities endowed with artificial intelligence is rejected, “it can only be seen as an instrument

³⁶ Agostino Capponi, Garud Iyengar & Jay Sethuraman, *Decentralized Finance: Protocols, Risks, and Governance*, Foundations and Trends in Finance (2023).

³⁷ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018); Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022).

³⁸ Isac Silveira da Costa, *O futuro é infungível: tokenização, non-fungible tokens (NFTs) e novos desafios na aplicação do conceito de valor mobiliário*, *Revista de Direito das Sociedades e dos Valores Mobiliários*, special vol., 283 (Dec. 2021), at 299; Silveira, work cited in the manuscript (2018); Dayana de Carvalho Uhdre, *Blockchain, Tokens e Criptomoedas: Análise Jurídica* (Almedina 2021).

³⁹ José de Aguiar Dias, *Da Responsabilidade Civil* (2006); Nelson Rosendal & Felipe Braga Netto, *Responsabilidade Civil: Teoria Geral* (Foco 2024).

⁴⁰ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 223.

used by the debtor to perform its obligations,” with direct liability falling on the developer, grounded in the sphere of risk that the developer holds from the moment it uses a mechanism endowed with artificial intelligence.⁴¹

III. IMPUTATION GAPS AND THE CRISIS OF THE CLASSICAL ASSUMPTIONS OF CIVIL LIABILITY

The dogmatics of civil liability was built on assumptions whose solidity was ensured by the clear identification of the subjects involved in the legal relationship, the materiality of the harm, the linearity of the causal nexus, and the possibility of attributing fault or risk to a determined agent.⁴² The tokenized economy, and specifically transactions with stablecoins, challenges each of these assumptions simultaneously, producing what this article calls systemic imputation gaps.

The position sustained here is that these gaps do not result merely from legislative absence, but from structural incompatibility between the dogmatic foundations of the institute and the architecture of tokenized transactions.⁴³ The consequence is that even the analogical or extensive application of the current provisions - articles 186, 187, 927, and the sole paragraph of article 927 of the Civil Code - encounters operational limits that can only be overcome by an interpretive reconstruction of the assumptions.

According to Dayana de Carvalho Uhdre:

The challenge, therefore, is to adapt the existing regulatory framework, which was designed for certain known forms of engaging in reproachable conduct - and for that reason became the object of regulation - to these new tools that facilitate the same noncompliant conduct. And, in this search to readapt the existing system to these new forms of socioeconomic transactions, certain challenges and peculiarities may be faced. The potential fluidity of functionalities exercised by tokens, for example, may often hinder the framing of operations within the currently established legal structure.⁴⁴

⁴¹ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 223.

⁴² Nelson Rosenvald & Felipe Braga Netto, *Responsabilidade Civil: Teoria Geral* (Foco 2024), at 586-589.

⁴³ Mafalda Miranda Barbosa, *Do Nexo de Causalidade ao Nexo de Imputação: Contributo para a Compreensão da Natureza Binária e Personalística do Requisito Causal ao Nível da Responsabilidade Civil Extracontratual* (Princípios 2013); Rafael de Freitas Valle Dresch, *Fundamentos da Responsabilidade Civil pelo Fato do Produto e do Serviço: Um Debate Jurídico-Filosófico entre o Formalismo e o Funcionalismo no Direito Privado* (Livreria do Advogado 2009).

⁴⁴ Dayana de Carvalho Uhdre, *Blockchain, Tokens e Criptomoedas: Análise Jurídica*

In addition, José Luiz de Moura Faleiros Júnior notes that the cryptoeconomy, by reconfiguring market dynamics and the modes of operationalizing digital assets, requires a consistent legal response adjusted to its specificities, imposing a rigorous analysis of the civil liability of agents and giving primacy to preventive mechanisms capable of mitigating the risks inherent in cryptoasset transactions, fostering stricter security practices, and increasing transparency in transactions.⁴⁵

A. Fragmentation of the Poles of Liability

Barbosa systematizes the problem of contractual imputation in blockchain environments around three axes: “to whom liability should be imputed when several nodes are involved”; “to what extent the distributed ledger can be held liable for users’ unlawful activities”; and “to what extent liability for harms generated by software agents may be imputed to a subject”.⁴⁶ From this framework, one may infer that, once the commercial nature of the underlying legal relationship is recognized, civil liability must be conceived under the logic of solidarity, as a response to the distributive complexity of functions and the plurality of agents involved.⁴⁷

Fragmentation assumes a particularly acute dimension when decentralized autonomous organizations (DAOs), which govern many DeFi protocols, are considered. As Barbosa records, DAOs are “online digital entities that act by implementing pre-coded rules,” and are frequently used to execute smart contracts and record activity on the blockchain.⁴⁸ Because they act autonomously, one asks whether liability may be imputed to the creator of the DAO; some argue that it should be attributed to the entity itself, which would require granting it legal personality,⁴⁹ a path not yet taken by Brazilian law. The fundamental objection is that, in the absence of legal personality of the DAO, harms generated by its governance decisions (such as changing liquidation parameters in a way that results in losses) remain without a clearly

(Almedina 2021), at 245-246.

⁴⁵ José Luiz de Moura Faleiros Júnior, Responsabilidade civil e criptoeconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024), at 18.

⁴⁶ Mafalda Miranda Barbosa, Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova, 1 Revista de Direito da Responsabilidade 206 (2019), at 219.

⁴⁷ Mafalda Miranda Barbosa, Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova, 1 Revista de Direito da Responsabilidade 206 (2019), at 215-224.

⁴⁸ Mafalda Miranda Barbosa, Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova, 1 Revista de Direito da Responsabilidade 206 (2019), at 220.

⁴⁹ Aaron Wright, The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges, 4(2) Stanford Journal of Blockchain Law & Policy (2020), at 166-172.

imputable passive subject.⁵⁰

B. Causal Nexus and Distributed Causation

The causal nexus, as a structural element of civil liability, acquires particularly controversial contours in the context of the tokenized economy, insofar as the production of harm tends to emerge from polycentric technical-organizational arrangements marked by automation, functional interdependence, and decision-making dispersion. This is precisely the problem captured by the expression distributed liability of distributed ledgers, proposed by Zetzsche, Buckley, and Arner, in showing that, in distributed architectures, the very attribution of liability tends to “distribute” itself, without the legal order immediately offering sufficiently stable normative criteria to impute harmful consequences to determined subjects.⁵¹

This subsection maintains that causation in transactions involving stablecoins applied to sectoral financing of the real economy does not fit adequately within any traditional causal theory, requiring interpretive reconstruction grounded in the notion of spheres of risk.

As Barbosa observes, “in the context of causation grounding liability, it is important to integrate a dimension of *Zurechnungszusammenhang*” (imputation nexus) that goes beyond mere conditionality.⁵² In transactions with stablecoins, the very normality of operations is an unknown, given the novelty of the arrangements and the absence of historical series that would allow patterns to be assessed. There is no sufficient empirical basis to state that an oracle failure is an “adequate” cause of improper liquidation, because the normality pattern of such operations has not yet stabilized.

The theory of the scope of protection of the violated norm, inspired by German law, offers a more promising path by shifting the inquiry to the protective purpose of the norm and to the sphere of risk assumed by the agent. Mafalda Miranda Barbosa’s contribution is decisive on this point. She argues:

Thus, from the outset, we may state that the foundational vein of objective imputation cannot fail to be found in a sphere of risk that

⁵⁰ The multiplication of agents identified in the preceding section does not, by itself, constitute an insurmountable obstacle to imputation: civil law has mechanisms to deal with plurality of agents, such as passive solidarity (article 942 of the Civil Code) and liability for the acts of third parties. The problem lies in the combination of multiplication with pseudonymity, automaticity, and transnationality, which produces what may be designated as fragmentation of the poles of liability.

⁵¹ Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018), at 1374-1402.

⁵² Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 238.

is assumed. It is not enough to contemplate the sphere of risk assumed by the agent in an atomistic way, uprooted from the anthropological-social and worldly fabric in which the agent is inserted. In other words, and relating this to what is pertinently accepted in defining legally relevant conduct, it should be stressed here that, because the reference of meaning from which we depart is the human person, marked by the dialectical encounter between the I, as a component of individuality, and the you, as an enhancer of the full development of personality, it must be compared with the sphere of risk headed by the injured party, by the third parties that terrestrially compose the horizon of that party's action, and also with the general sphere of risk of life. Nor is it alien to this fact that the entire problem is animated by the primary teleology of tort liability, that is, by the eminently reparatory purpose of the institute. The person, by acting, because he or she is free, assumes a role responsibility and must, in the encounter with the other, comply with a series of duties of care. Two hypotheses are therefore theoretically viable: either the person acts invested with a special role/function or is integrated into a concretely defined community of danger, and in this case the sphere of risk capable of grounding the imputational judgment is a priori drawn; or the sphere of risk/responsibility embraced is not sufficiently defined to guarantee the correctness of that judgment.⁵³

Applied to transactions with stablecoins, this doctrinal construction makes it possible to distribute imputation according to the spheres of risk headed by each agent. The issuer of the stablecoin heads the sphere of risk relating to the maintenance of parity; the smart contract developer heads the sphere of risk relating to the correctness of the code; the oracle provider heads the sphere of risk relating to data reliability; and the DeFi protocol operator heads the sphere of risk relating to system governance.

From this perspective, the developer will answer whenever, intentionally or through breach of duties of care inherent in legal traffic, it makes available to blockchain users or to third parties the means by which they come to injure the rights of others.⁵⁴ Consequently, the analysis of the conflict between spheres of risk is the most appropriate hermeneutic resource for delimiting and distributing liability in transactions marked by distributed causation.⁵⁵

⁵³ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 40.

⁵⁴ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 242.

⁵⁵ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018).

C. Information Asymmetry, Duties of Accountability, and Their Limits

In transactions with stablecoins in agribusiness, information asymmetry constitutes one of the most serious sources of potential harms and, at the same time, one of the strongest foundations for constructing duties of imputation.⁵⁶ On one side, stablecoin issuers possess privileged information about the composition of their reserves, the solidity of their stabilization mechanisms, and liquidity risks. On the other, DeFi protocol developers master the source code and know its vulnerabilities. The rural producer or retail investor who participates in the tokenized financing operation generally lacks the technical capacity to assess any of these risks.

This asymmetry is not a mere contingent inconvenience; it is structural and arises from the very architecture of the system. Unlike the traditional capital market, in which disclosure obligations and fiduciary duties are imposed on registered intermediaries, DeFi operations are governed, to a large extent, by the maxim “code is law.” Trust is shifted from the human intermediary to the code, but the code is not accessible to the understanding of the average user.⁵⁷ As Faleiros Júnior points out, “the disruptive effects of blockchain technology have the capacity to generate important repercussions in matters of civil liability, opening room for rereadings of its assumptions and functions”.⁵⁸

The concept of accountability acquires, in this context, singular normative relevance. Comandé defines accountability as the obligation of those who make decisions and choices to justify them before those who suffer the effects of those choices and, eventually, to answer in the appropriate instances for their failures.⁵⁹ Faleiros Júnior proposes an analytical distinction among the terms responsibility, accountability, and liability, whose semantic differentiation, clearer in English, proves particularly useful for properly understanding diverse dimensions of the legal phenomenon of responsabilization.⁶⁰

Within this framework, responsibility refers to the broad duty to answer for conduct, functions, or obligations; accountability refers, in a more specific sense, to the duty of rendering accounts and of justification

⁵⁶ Christian Catalini, Alonso de Gortari & Nihar Shah, Some Simple Economics of Stablecoins, 14 Annual Review of Financial Economics 117 (2022).

⁵⁷ Mafalda Miranda Barbosa, Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova, 1 Revista de Direito da Responsabilidade 206 (2019).

⁵⁸ José Luiz de Moura Faleiros Júnior, Responsabilidade civil e criptoeconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024), at 18.

⁵⁹ Giovanni Comandé, Intelligenza Artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell’IA e il problema della responsabilità, in *Analisi giuridica dell’Economia*, vol. 1 (Antonio Nuzzo & Gustavo Olivieri eds., Il Mulino 2019), at 185.

⁶⁰ José Luiz de Moura Faleiros Júnior, Responsabilidade civil e criptoeconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024), at 18.

before control instances; and liability designates legal subjection to the repair of harms or to the imposition of legal consequences arising from the breach of duties.⁶¹

Transposed to the stablecoin context, accountability imposes on issuers, developers, and protocol operators the duty to render accounts regarding the risks of their activities, regardless of the existence of a direct contractual link with the victim. The thesis sustained is that breach of the duty of accountability constitutes, by itself, an autonomous basis for civil liability, distinct from fault in the classical subjective sense. It is not necessary that the agent acted negligently, recklessly, or incompetently in relation to the specific harmful result; it is enough that the agent breached the duty to provide adequate accounts of the risks of its activity, thereby creating an information asymmetry that contributed to the victim's exposure to harm.

The principal objection to this construction lies in the risk of unduly expanding civil liability. Indeed, if the mere breach of duties of transparency is elevated, by itself, to a sufficient basis for imputation, it opens space for holding peripheral agents in the chain liable for harms whose causal production resulted from the conduct of third parties.

The solution lies in calibrating accountability according to the agent's position in the value chain: the duty to render accounts is more intense for those who exercise greater control over the source of risk and possess a higher level of information. Thus, the stablecoin issuer has a maximum duty of accountability regarding the composition of reserves; the smart contract developer has a qualified duty regarding the security of the code; and the validating node has a residual duty regarding the integrity of processed transactions.⁶²

D. The Insufficiency of Individual Fault and the Problem of Diffuse Authorship

The final axis in the analysis of imputation gaps concerns the inadequacy of the individual fault paradigm as a basis for liability in tokenized transactions. The classical model of subjective liability (article 186 of the Civil Code) presupposes that harm results from the voluntary act or omission, negligence, or imprudence of an identified agent. In transactions with stablecoins, however, harm frequently results from collective decisions mediated by decentralized governance mechanisms, in which no individual participant has determining power over the outcome.⁶³

⁶¹ José Luiz de Moura Faleiros Júnior, Responsabilidade civil e criptoconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024), at 18-19.

⁶² Katrin Schuler, Ann Sofie Cloots & Fabian Schär, On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance, 10(2) Journal of Financial Regulation 213 (2024), at 233.

⁶³ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, The Distributed Liability

Strict liability based on the risk of the activity (article 927, sole paragraph, of the Civil Code) offers a more adequate foundation by dispensing with proof of fault and concentrating the inquiry on the activity performed and the risk inherent to it. The difficulty, however, is to determine who performs the “activity” when it is distributed among multiple agents, none of whom acts alone. The interpretation proposed here is functional: the activity of risk is performed by whoever holds decision-making or technological control over the system’s operating parameters that produced the harm.

In an agribusiness financing transaction through stablecoins, for example, the issuer (by maintaining the stabilization infrastructure), the developer (by defining the logic of the smart contract), and holders of governance tokens with relevant decision-making participation (by parameterizing liquidation criteria) perform activities of risk. The other agents may be called to answer subsidiarily, according to the layered model proposed in section VII.⁶⁴

IV. SYSTEMIC RISKS AND CIVIL LIABILITY

A. Interoperability, Contagion, and Causal Amplification

The interoperability of DeFi, celebrated as a competitive advantage, is transformed, from the perspective of civil liability, into a factor that amplifies harm and disperses causation. When a decentralized lending protocol automatically redirects collateral to another protocol, which in turn uses stablecoins as collateral in a third transaction, the causal chain becomes opaque and multifactorial. Each link in the chain constitutes, simultaneously, a necessary condition of the harmful result and an agent with its own sphere of risk.

Bonnet maintains that concentration in the cryptoasset market increases the vulnerability of the system because an information-technology attack directed at a few relevant intermediaries may affect, in cascade, the issuance, custody, and trading of assets.⁶⁵ From this perspective, the greater the concentration, the lower the risk-dispersion capacity that characterizes the logic of decentralization, producing failure points that become priority targets. In addition, in networks based on proof of work, the concentration of computational capacity in a few agents tends to facilitate attacks and interruptions, because it reduces the number

of Distributed Ledgers: Legal Risks of Blockchain, 2018(4) University of Illinois Law Review 1361 (2018); Aaron Wright, The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges, 4(2) Stanford Journal of Blockchain Law & Policy (2020).

⁶⁴ José Luiz de Moura Faleiros Júnior, Responsabilidade civil e criptoconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024).

⁶⁵ Joris Bonnet, Blockchain et finance décentralisée (Ph.D. dissertation, Université de Paris, École doctorale 101, 2024).

of actors capable of influencing the operation of the network.

The implication for civil liability is objective at the normative level: agents occupying concentrated positions, such as stablecoin issuers with high market share or platforms that concentrate the liquidity of tokenized transactions, must observe more rigorous duties of governance and security, with measures proportional to the risk produced by their centrality.⁶⁶

B. The Preventive and Precautionary Function of Civil Liability

Doctrine has emphasized that the rise of risk-management models shifts the functional axis of civil liability, reordering it toward ex ante vectors of prevention and precaution rather than a predominantly retrospective reconstruction of fault. In this sense, José Luiz de Moura Faleiros Júnior observes that:

Risk management “in real time” therefore implies considering benefits and risks. These risks, although not entirely foreseeable, come to be structured around the preventive and precautionary functions of civil liability, altering the core of the investigation into a possible failure, even regarding the consented use of personal data widely disclosed in financial, payment, and cryptoasset investment-portfolio management structures.⁶⁷

Due diligence, within this framework, ceases to be a mere corporate-governance recommendation and becomes a legal duty of diligence, whose qualified breach should operate as an imputation criterion, especially when the activity increases uncontrollable risks, produces relevant information asymmetries, and induces public trust through signs of security and compliance.

This reconfiguration allows the construction, by functional analogy, of a liability regime for stablecoin issuers and DeFi protocol operators that intermediate agribusiness financing transactions. Just as the contractual and extra-contractual civil liability of rating agencies for harms resulting from defective evaluations is discussed in the traditional financial market, in the terms developed by Frada⁶⁸ and Dotta Neto,⁶⁹ here too one identifies an informational and technological gatekeeper role, capable of influencing decisions and amplifying negative externalities. The economic and technical centrality of these agents, combined with

⁶⁶ Joris Bonnet, *Blockchain et finance décentralisée* (Ph.D. dissertation, Université de Paris, École doctorale 101, 2024).

⁶⁷ José Luiz de Moura Faleiros Júnior, *Responsabilidade civil e criptoconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos*, 13(37) *Revista Fórum de Direito Civil* 11 (Sept./Dec. 2024), at 20.

⁶⁸ Manuel A. Carneiro da Frada, *A Responsabilidade Civil das Agências de Notação do Risco (Rating): Ensaio de Construção Dogmático-Crítica* (Almedina 2018), at 19.

⁶⁹ Milton Dotta Neto, *Responsabilidade Civil das Agências de Rating* (Lumen Juris 2016), at 51.

their ability to modulate risks, reinforces the dogmatic adequacy of an effective liability regime calibrated by the foreseeability of harm, the controllability of risk, and the degree of trust induced in users and investors.

Faleiros Júnior is explicit in stating that:

much more than punishing the agent directly involved in sophisticated transactions involving the blockchain network, it is important to delimit the liability regime of the legal entities involved in this dynamic, notably exchanges, which closely resemble rating agencies and application providers.⁷⁰

Thus, if civil liability begins to incorporate preventive and precautionary functions with greater density, the normative focus falls on structural duties of risk governance, and not merely on the individual conduct of the final user. For stablecoin issuers and DeFi operators, this implies recognizing the breach of due diligence as an organizational failure (institutional fault) or, as the case may be, as a factor objectifying the duty to repair, especially when the activity presents itself as safe, stable, and audited but lacks controls proportional to the risk assumed. In this line, imputation must be constructed from verifiable standards of diligence, transparency, and continuous monitoring, compatible with the complexity of the ecosystem and with the protection of trust in tokenized transactions.

V. INTERNATIONAL EXPERIENCES AND COMPARATIVE REGULATORY FRAMEWORKS

A. European Union: The MiCA Regulation and Issuer Liability

The Markets in Crypto-Assets Regulation (MiCA - Regulation (EU) 2023/1114), approved by the European Parliament in 2023, constitutes the first initiative for systemic and comprehensive regulation of cryptoassets at the supranational level. With respect to stablecoins, MiCA establishes a normative distinction between asset-referenced tokens (ARTs) and e-money tokens (EMTs), imposing on both categories requirements of prior authorization, adequacy of reserves, corporate governance, and issuer liability. Of special relevance are the attribution of responsibility to the issuer for the maintenance and composition of reserves, the guarantee of the right of redemption under predefined conditions, and the duties of adequate disclosure of information to holders, operationalized through a mandatory white paper, periodic reserve auditing, and institutionalized complaint-management

⁷⁰ José Luiz de Moura Faleiros Júnior, Responsabilidade civil e criptoconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024), at 22.

mechanisms.⁷¹

The European model, however, presents relevant limitations for the problem investigated in this study. MiCA was designed for centralized stablecoins issued by identifiable entities domiciled in European jurisdictions, such that algorithmic stablecoins and decentralized-finance (DeFi) protocols operating without a responsible legal person remain, to a large extent, outside its regulatory perimeter. Nor does the regulation discipline the tokenization of agribusiness assets or the use of stablecoins as settlement instruments in sectoral financing transactions. As Bonnet observes, “the main functionalities of decentralized finance are, to date, not addressed by the European legislator,” a gap that the French Autorité des marchés financiers (AMF) itself recognized when launching a public consultation on DeFi in June 2023.⁷²

The relevance of MiCA for this study nevertheless lies in the affirmation of a structuring principle: stablecoin issuers must be subject to duties of governance, transparency, and liability analogous to those applicable to traditional financial institutions.

B. United States: Fragmented Approach and Lessons from Ex Post Enforcement

In the United States, stablecoin regulation remains fragmented among multiple agencies (SEC, CFTC, OCC, FinCEN), without unified federal legislation. The American approach has focused on ex post enforcement actions, especially the judicial and administrative actions brought against Do Kwon and Terraform Labs after the collapse of TerraUSD, which resulted in a securities-fraud conviction.⁷³ The lesson drawn from this experience demonstrates that, when there is an identifiable issuer, traditional liability instruments, including the equation of stablecoins with securities, may be effectively mobilized. It also proves that an exclusively repressive approach, without preventive regulation, does not prevent the occurrence of systemic-scale harms, limiting itself to sanctioning the wrongdoer after losses have materialized.⁷⁴

It was in this context that the United States Congress promoted the

⁷¹ Agata Ferreira, *The Curious Case of Stablecoins - Balancing Risks and Rewards?*, 24(4) *Journal of International Economic Law* 755 (2021); Financial Stability Board, *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report* (July 2023).

⁷² Joris Bonnet, *Blockchain et finance décentralisée* (Ph.D. dissertation, Université de Paris, École doctorale 101, 2024), at 285; Katrin Schuler, Ann Sofie Cloots & Fabian Schär, *On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 10(2) *Journal of Financial Regulation* 213 (2024).

⁷³ David Krause, *Algorithmic Stablecoins: Mechanisms, Risks, and Lessons from the Fall of TerraUSD* (Marquette University 2024).

⁷⁴ Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022); David Krause, *Algorithmic Stablecoins: Mechanisms, Risks, and Lessons from the Fall of TerraUSD* (Marquette University 2024).

approval of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act, Pub. L. No. 119-27), enacted on July 18, 2025, which inaugurated the first unified federal regime for payment stablecoins in the United States, establishing a tripartite structure of issuance authorization, requiring full reserves in highly liquid assets at a 1:1 ratio, prohibiting rehypothecation of reserves, and establishing monthly independent-audit obligations - measures that respond directly to the transparency and reserve-adequacy failures identified as primary vectors of systemic instability.⁷⁵

C. Brazil: Law No. 14,478/2022 and Its Dogmatic Insufficiencies

The insufficiency is at once normative and dogmatic. It is normative because the statute refers matters to infralegal regulation without defining minimum parameters of liability, a gap that the Cryptoassets Legal Framework (Law No. 14,478/2022) did not fully fill, relegating to the triad of resolutions issued by the Central Bank in November 2025 (BCB Resolutions Nos. 519, 520, and 521/2025, effective as of February 2, 2026) the task of filling structural aspects of the regime, such as the authorization requirements for Virtual Asset Service Provider Companies (SPSAVs), patrimonial segregation, and the specific obligations applicable to stablecoins referenced to fiat currency. It is dogmatic because the general instruments of civil liability (articles 186, 187, 927, and the sole paragraph of article 927 of the Civil Code) were not designed to deal with the fragmentation of agents, automaticity of execution, and distributed causation that characterize stablecoin transactions. As Uhdre observes, “the potential fluidity of functionalities exercised by tokens may hinder the framing of operations within the currently established legal structure”.⁷⁶

Moreover, the legal classification of tokens representing agribusiness receivables remains uncertain, and the current regulatory framework does not resolve it satisfactorily. CVM Guidance Opinion No. 40/2022 establishes a tripartite functional taxonomy - payment tokens, utility tokens, and asset-referenced tokens - and adopts the principle of technological neutrality, according to which the use of cryptography or distributed ledger technology is irrelevant for classifying an asset as a security; what is decisive is whether the instrument constitutes a collective investment contract under article 2, item IX, of Law No. 6,385/1976.

Within this framework, tokenized Agribusiness Receivables Certificates (CRA) are necessarily securities by force of Law No. 14,430/2022, whereas tokenized Rural Product Notes (CPR) may or may not be so classified, depending on the presence of the criteria

⁷⁵ Financial Stability Board, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report (July 2023).

⁷⁶ Dayana de Carvalho Uhdre, Blockchain, Tokens e Criptomoedas: Análise Jurídica (Almedina 2021), at 187.

consolidated by the CVM's administrative case law. BCB Resolution No. 520/2025, in turn, imposes specific requirements for stablecoins referenced to fiat currency, including backing assessment, audited financial statements of the issuer, and risk classification, and expressly prohibits algorithmic stablecoins whose reserves are controlled only by algorithms, approaching, in this respect, the preventive approach of the European regulator under MiCA and of the American GENIUS Act.

A regulatory zone of indeterminacy with relevant consequences nevertheless remains: if the tokens are equated with securities, the competence of the CVM and the capital-market liability regime apply; if they are understood as generic financial instruments, competence falls to the Central Bank; if they are qualified as *sui generis* virtual assets, a residual regime applies that is structurally insufficient to protect investors. The overlap of competences between the CVM and the BCB, whose regulatory frameworks operate with partially distinct logics over the same set of instruments, reproduces domestically the jurisdictional fragmentation that international literature identifies as a primary vector of systemic risk in cryptoasset markets.⁷⁷

VI. TOWARD AN IMPUTATION MODEL ADEQUATE TO THE TOKENIZED ECONOMY

The analysis undertaken in the preceding sections evidences that the imputation gaps identified do not arise merely from legislative absence, but from structural incompatibility between the dogmatic assumptions of classical civil liability and the architecture of stablecoin transactions in the tokenized economy. The construction of an adequate imputation model therefore requires the reformulation of legal categories, not merely the enactment of new rules.⁷⁸

The central thesis concluded is that only the conjunction of three interpretive pillars - layered proportional liability, duties of governance and due diligence, and accountability as an autonomous imputation criterion - is capable of providing a dogmatically satisfactory response to the gaps identified. The articulation of these pillars is proposed below.

A. Layered Proportional Liability

The first pillar of the proposed model consists of adopting a regime of layered proportional civil liability, by which the obligation to repair harm is distributed among the agents that make up the tokenized value chain according to the degree of control effectively exercised over the source generating the risk and the level of qualified information they possess.

⁷⁷ Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022); Financial Stability Board, *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report* (July 2023).

⁷⁸ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019).

This regime is structurally distinct both from unrestricted joint and several liability - a mechanism that, by disregarding each agent's functional position in the chain, would disproportionately burden those located at its periphery - and from exclusively individual liability, which is insufficient to adequately protect victims when the principal agent is unidentifiable, located in an inaccessible jurisdiction, or insolvent.⁷⁹ It is therefore a distributive architecture that combines allocative efficiency and protection of the injured party, avoiding both the socialization of risk and a reparatory vacuum.

The layering criterion operates at three functionally distinct levels, structured according to the intensity of the relationship between the agent and the sphere of risk from which the harms may emanate. At the first level are agents endowed with the greatest capacity for control and privileged information about the underlying infrastructure: stablecoin issuers and smart contract developers, the operational cores of the tokenized ecosystem.

These agents should be subject to strict liability grounded in the full risk of the activity performed, pursuant to article 927, sole paragraph, of the Civil Code. The attribution of strict liability to such agents finds precise dogmatic justification in the theory of spheres of risk: by creating and maintaining the technological infrastructure that enables the entire operation, these agents deliberately establish the danger zone from which harms may emerge, becoming the primary holders of the reparatory obligation regardless of fault.⁸⁰ The underlying logic is that whoever obtains the benefits of a risky activity must bear the costs resulting from its materialization.

At the second level are DeFi protocol operators, oracle providers, and smart contract auditors - agents who, without leading the creation of the infrastructure, possess in-depth technical knowledge of its operation and of the systemic vulnerabilities inherent in it. They should be subject to qualified subjective liability, with reversal of the burden of proof against the defendant.⁸¹ The presumption of fault is justified by the structural informational asymmetry that characterizes relationships in this segment: such agents are in an epistemically privileged position to identify failures, anticipate risks, and adopt preventive measures, such that they must demonstrate the adoption of all reasonably required measures of technological due diligence.

As Barbosa observes, within centralized ledgers there is an

⁷⁹ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018).

⁸⁰ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 240.

⁸¹ Nelson Rosenvald & Felipe Braga Netto, *Responsabilidade Civil: Teoria Geral* (Foco 2024).

identifiable validating entity to which liability for third-party interference may be imputed; in decentralized blockchain architectures, such imputation does not operate clearly, making it necessary to verify in concreto whether the agent breached a legally relevant duty.⁸² The reversal of the burden of proof functions, in this context, as a technical-procedural instrument for mitigating evidentiary uncertainty, allocating to the technically qualified agent - and therefore the party better positioned to produce evidence of its diligence - the burden of demonstrating that its conduct complied with applicable standards of care.

At the third and final level are residual intermediaries: exchanges that list tokens, access platforms to the ecosystem, and auxiliary service providers. They should be subject to subsidiary liability, conditioned on demonstrating that their omissive conduct, reflected in noncompliance with duties of verification, monitoring, or information, causally contributed to the production of the harm, in close functional analogy with the civil-liability regime of internet application providers, as disciplined by the Brazilian Internet Civil Framework (Law No. 12,965/2014), which subordinates the provider's liability to prior notification and subsequent inertia in removing harmful content.

The parallel extends to the doctrinal treatment already afforded to cryptoasset exchanges, in which the imposition of compliance and information duties is recognized, the breach of which may give rise to the indirect liability of the intermediary.⁸³ Subsidiarity here does not imply immunity, but rather a gradation of the reparatory obligation compatible with the peripheral position of these agents in the value chain and with the degree to which their causal contribution to the harmful event can be determined. As Faleiros Júnior observes, exchanges that act as intermediaries in the custody and trading of cryptoassets "assume responsibility for hosting the systems" through which the operations are performed, in a position functionally analogous to that of application providers.⁸⁴

B. Duties of Governance and Due Diligence

The second pillar of the proposed model consists of imposing specific duties of governance and due diligence on qualified participants in the tokenized value chain. Breach of these duties, independently of proof of fault in the classical subjective sense, should ground the imputation of

⁸² Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019), at 224.

⁸³ Silveira, work cited in the manuscript (2018); Massimo Bartoletti, Stefano Lande, Andrea Loddo & Livio Pompianu, *Cryptocurrency Scams: Analysis and Perspectives*, 9 *IEEE Access* (2021).

⁸⁴ José Luiz de Moura Faleiros Júnior, *Responsabilidade civil e criptoconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos*, 13(37) *Revista Fórum de Direito Civil* 11 (Sept./Dec. 2024), at 22.

liability. Due diligence, as defined by Faleiros Júnior, consists of an audit carried out with the objective of preventing liabilities and optimizing business management.⁸⁵ In the context of agribusiness tokenization, this due diligence is not limited to traditional financial analysis but encompasses verification of the technological robustness of the stablecoin used, the adequacy of the smart contract to the specificities of the agricultural operation, and assessment of depeg risks.⁸⁶

The practical consequence of breach of these duties is the configuration of a presumption of causation in favor of the victim: once it is shown that the agent breached a specific duty of governance and that the harm relates to the sphere of risk covered by that duty, causation is presumed, leaving the agent to demonstrate the absence of nexus.⁸⁷

C. Accountability as an Autonomous Imputation Criterion

The third pillar of the model - the duty of accountability as an autonomous imputation criterion - complements the previous two and gives the set its most relevant dimension. Accountability operates as a basis for liability when, although it is not possible to demonstrate a direct causal nexus between the agent's conduct and the harm, it is proven that the agent held a position of influence over the value chain and breached duties of rendering accounts, transparency, or governance. It is therefore liability based on the position occupied in the chain of risk, and not on the individual action considered in isolation.

The theoretical foundation of this pillar rests on the distinction between liability and accountability developed by Comandé in the context of artificial intelligence: while liability presupposes a causal nexus between conduct and harm, accountability is grounded in the position of decision-making power and in the obligation to justify choices before those affected.⁸⁸ Faleiros Júnior transposes this distinction to the cryptoeconomy, identifying accountability as an autonomous vector of corporate governance in data-rich markets, one that imposes transparency

⁸⁵ José Luiz de Moura Faleiros Júnior, *Responsabilidade civil e o mercado de criptoativos*, in *Temas Atuais de Direito Digital* (São Paulo, 2023), at 20.

⁸⁶ Demir Murat Aksoy & Zümrüt Ecevit Sati, *Tokenization of Real World Assets: An Agricultural Token System Implementation Based on Blockchain Architecture*, 2(1) *The Journal of Applied Engineering and Agriculture Sciences* 24 (2025); Marco Schletz, Darius Nassiry & Myung-Kyoon Lee, *Blockchain and Tokenized Securities: The Potential for Green Finance*, ADBI Working Paper No. 1079 (Asian Development Bank Institute 2020).

⁸⁷ Mafalda Miranda Barbosa, *Do Nexo de Causalidade ao Nexo de Imputação: Contributo para a Compreensão da Natureza Binária e Personalística do Requisito Causal ao Nível da Responsabilidade Civil Extracontratual* (Principia 2013).

⁸⁸ Giovanni Comandé, *Intelligenza Artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giuridica dell'Economia*, vol. 1 (Antonio Nuzzo & Gustavo Olivieri eds., Il Mulino 2019), at 171; Katrin Schuler, Ann Sofie Cloots & Fabian Schär, *On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 10(2) *Journal of Financial Regulation* 213 (2024).

and rendering of accounts as duties detached from proof of fault.⁸⁹

In the proposed model, accountability operates on two planes. On the *ex ante* plane, it imposes duties of proactive transparency: the stablecoin issuer must regularly disclose the composition of its reserves; the smart contract developer must provide understandable technical documentation; and the DeFi protocol operator must make public the governance parameters and liquidation criteria. On the *ex post* plane, accountability imposes a duty to respond: once harm occurs, the agent that occupied a position of influence in the value chain must render accounts of the measures adopted to prevent the result, the information it had available, and the reasons for its decisions.

Any breach of this duty to respond constitutes, by itself, a basis for imputing liability, independently of proof of fault or direct causal nexus. The most relevant objection to this pillar is that it would represent an unjustified expansion of civil liability, subverting the principle that the obligation to repair requires at least a causal nexus between conduct and harm.

The response is twofold. First, the duty of accountability does not dispense with the existence of harm; it merely relaxes the requirement of direct causal nexus, replacing it with the demonstration of a position of influence and breach of the duty to render accounts. Second, this relaxation is justified by the structurally opaque nature of the tokenized economy, in which requiring direct causal nexus is, in practice, equivalent to denying justice to the victim. Accountability does not replace causation as a requirement of civil liability; it complements it, operating as an auxiliary criterion when direct causation is indemonstrable for structural reasons, and not because there is no material relationship between the conduct and the harm.

D. Articulation of the Pillars, Objections, and Limits of the Model

The three proposed pillars do not operate in isolation, but in dynamic articulation. Layered proportional liability defines who answers and to what extent; the duties of governance and due diligence define why the agent answers (the basis of imputation); and accountability defines when the agent answers even in the absence of a demonstrated direct causal nexus. The articulation of the three pillars allows, in theory, the resolution of the imputation gaps identified in the preceding sections: fragmentation is addressed by layering;⁹⁰ distributed causation is addressed by governance duties (which create a presumption of causation); and information asymmetry is addressed by accountability.

⁸⁹ José Luiz de Moura Faleiros Júnior, *Accountability e devida diligência como vetores da governança corporativa nos mercados ricos em dados*, 26(1) *Revista Semestral de Direito Empresarial* 183 (June 2020), at 189.

⁹⁰ Dirk A. Zetsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018).

The model, however, presents limits that must be made explicit. First, it depends on at least some agents in the chain being identifiable, a condition that may not exist in genuinely decentralized DeFi protocols, in which all participants operate under pseudonyms on public networks without centralized governance. In that hypothesis, the proposed model attenuates the imputation gap but does not eliminate it. Second, application of the model presupposes a jurisdictional and regulatory apparatus capable of dealing with the transnationality of the transactions, which requires international cooperation and mechanisms for recognizing foreign decisions that remain incipient within the tokenized economy.⁹¹ Third, the effectiveness of the model depends on the victim's ability to access the justice system and to bear the costs of litigating technically complex claims, a challenge that especially affects small rural producers.

CONCLUSION

The investigation carried out in this study demonstrated that the use of stablecoins as financing instruments, especially in Brazilian agribusiness, produces civil-liability imputation gaps that do not find an adequate response in traditional dogmatic assumptions. The initial hypothesis was confirmed: the operational decentralization promoted by stablecoins generates structural fragmentation of the poles of liability, with harmful effects on investors, rural producers, and the stability of sectoral markets.⁹²

The proposed model does not purport to exhaust the matter, but to offer an interpretive framework capable of guiding the application of law and the construction of future regulatory frameworks. Its limits were made explicit: dependence on the minimum identifiability of agents, the need for international jurisdictional cooperation, and access-to-justice challenges for vulnerable victims. The tokenization of agribusiness is an irreversible phenomenon, with potential to broaden access to credit and reduce intermediation costs; its sustainable viability, however, depends on the construction of a protective legal framework that reconciles technological innovation with legal certainty.⁹³

⁹¹ Agata Ferreira, *The Curious Case of Stablecoins - Balancing Risks and Rewards?*, 24(4) *Journal of International Economic Law* 755 (2021); Steven L. Schwarcz, *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022).

⁹² Bank for International Settlements, *Stablecoins: Risks, Potential and Regulation*, BIS Working Papers No. 1114 (2023); Financial Stability Board, *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report* (July 2023).

⁹³ Marco Schletz, Darius Nassiry & Myung-Kyoon Lee, *Blockchain and Tokenized Securities: The Potential for Green Finance*, ADBI Working Paper No. 1079 (Asian Development Bank Institute 2020); Christian Catalini, Alonso de Gortari & Nihar Shah, *Some Simple Economics of Stablecoins*, 14 *Annual Review of Financial Economics* 117 (2022).

Civil liability, as a living legal institute in permanent reconstruction, has adaptive capacity to confront the challenges of the tokenized economy. The condition for doing so is that doctrine and case law accept the need for specific normative criteria, without losing sight of the ethical and functional foundations that justify the duty to repair: corrective justice, the equitable distribution of risks, and the protection of the vulnerable in the economic chain.

The three pillars proposed in this study constitute a contribution in that direction, with the expectation that doctrinal debate will refine them, test them, and eventually incorporate them into judicial practice.⁹⁴

The ultimate conclusion of this study is that civil liability possesses, in its foundations, the dogmatic resources necessary to confront the challenges of the tokenized economy. The notion of sphere of risk, duties of care in legal traffic, the theory of activity risk, and the construction of duties of accountability offer a theoretical basis for the interpretive reconstruction of the assumptions of imputation. What is required is the willingness to accept that causation may be distributed without being indemonstrable, that fault may be collective without being anonymous, and that liability may be proportional without being ineffective.

In that spirit, the three pillars proposed here constitute a first step - necessarily provisional and subject to revision - in constructing a dogmatic framework commensurate with the complexity that the tokenized economy presents to law.

REFERENCES

- Aksoy, Demir Murat & Zümür Ecevit Satı, Tokenization of Real World Assets: An Agricultural Token System Implementation Based on Blockchain Architecture, 2(1) *The Journal of Applied Engineering and Agriculture Sciences* 24 (2025).
- Antonopoulos, Andreas M., *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly Media 2015).
- Argelich Comelles, Cristina, Smart Contracts o Code is Law: Soluciones Legales para la Robotización Contractual, *InDret*, no. 2 (2020).
- Bank for International Settlements, *Stablecoins: Risks, Potential and Regulation*, BIS Working Papers No. 1114 (2023).
- Barbosa, Mafalda Miranda, Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova, 1 *Revista de Direito da Responsabilidade* 206 (2019).
- Bartoletti, Massimo, Stefano Lande, Andrea Loddo & Livio Pompianu, *Cryptocurrency Scams: Analysis and Perspectives*, 9 *IEEE Access*

⁹⁴ Mafalda Miranda Barbosa, *Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova*, 1 *Revista de Direito da Responsabilidade* 206 (2019); José Luiz de Moura Faleiros Júnior, *Responsabilidade civil e criptoeconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos*, 13(37) *Revista Fórum de Direito Civil* 11 (Sept./Dec. 2024).

- (2021).
- Bonnet, Joris, Blockchain et finance décentralisée (Ph.D. dissertation, Université de Paris, École doctorale 101, 2024).
- Caetano, M. X., D. R. dos Santos & C. Arrigoni, Criptomonedas: seus desafios de regulamentação e os impactos a instituições financeiras centralizadas, 9(3) International Journal of Professional Business Review 1 (2024).
- Capponi, Agostino, Garud Iyengar & Jay Sethuraman, Decentralized Finance: Protocols, Risks, and Governance, Foundations and Trends in Finance (2023).
- Catalini, Christian, Alonso de Gortari & Nihar Shah, Some Simple Economics of Stablecoins, 14 Annual Review of Financial Economics 117 (2022).
- Chen, Yan, Lin William Cong & Jianwei Xia, Blockchain Disruption and Smart Contracts, 35(4) The Review of Financial Studies 1495 (2022).
- Comandé, Giovanni, Intelligenza Artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità, in *Analisi giuridica dell'Economia*, vol. 1 (Antonio Nuzzo & Gustavo Olivieri eds., Il Mulino 2019).
- Conrado, Paulo Cesar, ed., Criptoativos, tokenização, blockchain e metaverso (Thomson Reuters Brasil 2022).
- Cortez, Nathan, Regulating Disruptive Innovation, 29 Berkeley Technology Law Journal 175 (2014).
- Costa, Isac Silveira da, O futuro é infungível: tokenização, non-fungible tokens (NFTs) e novos desafios na aplicação do conceito de valor mobiliário, Revista de Direito das Sociedades e dos Valores Mobiliários, special vol., 283 (Dec. 2021).
- Divino, Stênio Geraldo Lopes, Smart contracts: conceitos, limitações, aplicabilidade e desafios, 4(6) RJLB 2771 (2018).
- Dotta Neto, Milton, Responsabilidade Civil das Agências de Rating (Lumen Juris 2016).
- European Central Bank, The Expansion of Functions and Uses of Stablecoins, Financial Stability Review (Nov. 2021).
- Faleiros Júnior, José Luiz de Moura, Accountability e devida diligência como vetores da governança corporativa nos mercados ricos em dados, 26(1) Revista Semestral de Direito Empresarial 183 (June 2020).
- Faleiros Júnior, José Luiz de Moura, Responsabilidade civil e criptoeconomia: a atuação das corretoras (exchanges) e sua responsabilização por ilícitos cibernéticos, 13(37) Revista Fórum de Direito Civil 11 (Sept./Dec. 2024).
- Faleiros Júnior, José Luiz de Moura, Responsabilidade civil e o mercado de criptoativos, in *Temas Atuais de Direito Digital* (São Paulo, 2023).
- Ferreira, Agata, The Curious Case of Stablecoins - Balancing Risks and Rewards?, 24(4) Journal of International Economic Law 755 (2021).
- Financial Stability Board, Regulation, Supervision and Oversight of

- Crypto-Asset Activities and Markets: Final Report (July 2023).
- Frada, Manuel A. Carneiro da, *A Responsabilidade Civil das Agências de Notação do Risco (Rating): Ensaio de Construção Dogmático-Crítica* (Almedina 2018).
- Gorton, Gary B. & Jeffery Zhang, *Taming Wildcat Stablecoins*, 90(3) *University of Chicago Law Review* 909 (2023).
- Helguera, Carlos de Cores, *Criptoactivos y circulación jurídica*, in *Tutela Jurídica do Corpo Eletrônico* (Cristiano Colombo, Wilson Engelmann & José Luiz de Moura Faleiros Júnior coords., Foco 2022).
- Krause, David, *Algorithmic Stablecoins: Mechanisms, Risks, and Lessons from the Fall of TerraUSD* (Marquette University 2024).
- Lei No. 14.478, de 21 de dezembro de 2022, *Diário Oficial da União [D.O.U.]* (Braz.).
- Moreira, Cintia, Malu Delgado & Rodrigo Santos, *Repensando a Tecnologia Blockchain* (São Paulo, 2023).
- Regulation (EU) 2023/1114 of the European Parliament and of the Council of May 31, 2023 on markets in crypto-assets (MiCA).
- Rosenvald, Nelson & Felipe Braga Netto, *Responsabilidade Civil: Teoria Geral* (Foco 2024).
- Schär, Fabian, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, 103(2) *Federal Reserve Bank of St. Louis Review* 153 (2021).
- Schletz, Marco, Darius Nassiry & Myung-Kyoon Lee, *Blockchain and Tokenized Securities: The Potential for Green Finance*, ADBI Working Paper No. 1079 (Asian Development Bank Institute 2020).
- Schuler, Katrin, Ann Sofie Cloots & Fabian Schär, *On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 10(2) *Journal of Financial Regulation* 213 (2024).
- Schwarcz, Steven L., *Regulating Global Stablecoins: A Model-Law Strategy*, 75 *Vanderbilt Law Review* 1729 (2022).
- Uhdre, Dayana de Carvalho, *Blockchain, Tokens e Criptomoedas: Análise Jurídica* (Almedina 2021).
- Uhdre, Dayana de Carvalho, *Tokenização, consumo de intangíveis e responsabilização*, in *Estudos de Direito Digital* (São Paulo, 2023).
- Wright, Aaron, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4(2) *Stanford Journal of Blockchain Law & Policy* (2020).
- Zetzsche, Dirk A., Douglas W. Arner & Ross P. Buckley, *Decentralized Finance (DeFi)*, 6(2) *Journal of Financial Regulation* (Sept. 2020).
- Zetzsche, Dirk A., Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018(4) *University of Illinois Law Review* 1361 (2018).

* * *

Victor Hugo Gimenez Gonçalves

Master's student in Law, concentration area in Law in Economic and Social Relations, research line in Business Law in the Brazilian and International Economic Order, Milton Campos Law School, Nova Lima/MG, Brazil.

Email: vh2g.or@gmail.com

ORCID iD: <https://orcid.org/0000-0002-4794-9761>

 10.59224/bjlti.v4i1.175-206
ISSN: 2965-1549