REGULATING DECENTRALIZED STABLECOINS: COMPARING MICAR AND THE GENIUS ACT

CHRISTOPHER K. ODINET*
ANDREA TOSATO**

Abstract

Stablecoins have become one of the cornerstones of the digital asset ecosystem, facilitating over $10 trillion in annual transactions. Yet while lawmakers, regulators, and scholars worldwide have focused intensely on *centralized* stablecoins issued by identifiable companies like Tether and Circle, a parallel market of *decentralized* stablecoins has quietly grown to command billions in value, all without comparable scrutiny. These protocols, exemplified by MakerDAO's DAI, operate as autonomous software systems, without identifiable issuers, and with users interacting exclusively with code rather than corporate counterparties. As this shadow infrastructure becomes increasingly integrated into mainstream finance, billions in user value remain exposed to legal uncertainty and without adequate legal protection.

This Essay provides the first comprehensive legal analysis of decentralized stablecoins and, in doing so, reveals a major private law vacuum that distinguishes these tokens from traditional financial instruments. Through our systematic examination of MakerDAO, we demonstrate that the absence of legal personhood leaves users in a complete contractual void, renders title to their holdings uncertain, and largely forecloses viable remedies in tort, criminal, or fiduciary law. Moving beyond critique, we then propose three private ordering solutions, ranging from transparency requirements to decentralized insurance mechanisms to legally incorporated DAOs, that each offer different trade-offs between decentralization and legal certainty.

Finally, we provide the first comparative analysis of how the European Union's Markets in Crypto-Assets Regulation (MiCAR) and the United States' recent GENIUS Act approach decentralized stablecoins. While both frameworks explicitly defer substantive regulation of these protocols to future study, their interim strategies reflect diverging regulatory philosophies. MiCAR employs functional definitions that technically encompass decentralized stablecoins but impose impossible compliance requirements that effectively ban them via liability transfer. The GENIUS Act adopts structural prerequisites that

* Professor of Law & Mosbacher Research Fellow, Texas A&M University.
** Professor of Law, Southern Methodist University. The Authors thank Purabi Kunwar (Texas A&M Law) for her helpful editing and research assistance. All errors belong to the Authors alone.

categorically exclude protocols that lack identifiable issuers, thus leaving them in regulatory limbo. Neither framework successfully resolves the fundamental challenges that these decentralized protocols present: namely, replicating financial functions without financial institutions. By mapping both the private law vacuum and the regulatory landscape, our analysis charts a path toward coherent legal frameworks.

Table of Contents

INTRODUCTION

The stablecoin market has become a cornerstone of the digital asset ecosystem, facilitating over $10 trillion in annual transaction volume and serving as the primary medium of exchange for cryptocurrency traders throughout the world.[1] Yet while lawmakers, regulators and scholars have fixated on *centralized* stablecoins like Tether's USDT and Circle's USDC—both digital assets issued

[1] *See* Jack Caporal, *Which Stablecoins Are the Largest and Most Popular in 2025?*, THE MOTLEY FOOL (July 15, 2025), https://www.fool.com/research/largest-stablecoins/; DUNE & ARTEMIS, THE STATE OF STABLECOINS 2025: SUPPLY, ADOPTION & MARKET TRENDS 12 (Mar. 2025), https://perma.cc/HE67-NWH2

by identifiable companies that maintain reserve assets and offer redemption rights[2]—a parallel market of *decentralized* stablecoins has grown to command billions in value, all without comparable scrutiny.[3] Exemplified by MakerDAO's DAI, decentralized stablecoins are not issued by an identifiable entity with legal personhood.[4] Rather, they are autonomous software systems, commonly referred to as "protocols," composed of interconnected "smart contracts" deployed on distributed ledger networks, such as Ethereum and Solana.[5] Users can interact directly with these protocols to generate tokens that are designed to maintain price parity with a reference asset (*the peg*), typically one token for one US dollar, without reliance on traditional financial intermediaries.[6] This Essay provides the first comprehensive legal analysis of decentralized stablecoins, revealing that these digital assets exist within a veritable legal vacuum that leaves users without contractual counterparties, clouds title to their holdings, and forecloses remedies in tort, criminal, and fiduciary law.[7]

Typically, such a collapse of private law protections would precipitate swift public law intervention. Yet when it comes to decentralized stablecoins, emerging regulatory regimes have largely remained on the sidelines.[8] Both the European Union's Markets in Crypto-Assets Regulation (MiCAR)[9] and the United States' recently enacted GENIUS Act[10] establish comprehensive

---

[2] Centralized stablecoins are issued by corporate entities that hold reserve assets (typically cash, cash equivalents, or government securities) and grant holders contractual redemption rights. *See* Kara Bruce, Christopher K. Odinet & Andrea Tosato, *The Private Law of Stablecoins*, 54 ARIZ. ST. L. J. 1073, 1090 (2022) 5115277 [hereinafter Bruce, Odinet, & Tosato, *Stablecoins*]; Christopher K. Odinet & Andrea Tosato, *Regulating Stablecoins: Comparing MiCAR and the GENIUS Act*, NOTRE DAME L. REV. REFLECTION (forthcoming 2026), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5383158 [herein after Odinet, & Tosato, *Centralized Stablecoins*].

[3] *See* WHARTON BLOCKCHAIN & DIGIT. ASSET PROJECT, DEFI BEYOND THE HYPE: THE EMERGING WORLD OF DECENTRALIZED FINANCE 9–10 (2021), https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf [hereinafter DEFI BEYOND THE HYPE].

[4] Kara Bruce, Christopher K. Odinet, & Andrea Tosato, *Bankrupt Crypto Organizations*, N.C. L. REV. at *8-14 (forthcoming 2026), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5115277 [hereinafter Bruce, Odinet, & Tosato, *Crypto Orgs*].

[5] *See id.*

[6] *Id. See also* Bruce, Odinet, & Tosato, *Stablecoins*, *supra* note 2 at 1084-98.

[7] *See infra* Part I.B.1-4.

[8] *See infra* Part III.

[9] *See* Council Regulation 2023/1114 on Markets in Crypto-Assets, 2023 O.J. (L 150) 4 (EU) [hereinafter MiCAR], https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32023R1114.

[10] Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), S. 1582, 119th Cong. (2025).

frameworks for *centralized* stablecoin issuers[11] while explicitly deferring the substantive regulation of *decentralized* alternatives to future study.[12] MiCAR requires the European Commission to present recommendations for decentralized finance regulation within forty-eight months, while the GENIUS Act mandates Treasury Department studies on "endogenously collateralized payment stablecoins" and the application of service provider definitions to decentralized protocols.[13] To some extent, this regulatory forbearance is understandable given the novel technological and legal questions these protocols present.[14] Yet, this exercise in kicking the can-down-the-road cannot persist indefinitely. As decentralized stablecoins continue accumulating users, building infrastructure dependencies, and integrating into major retail platforms like Coinbase and Robinhood, the urgency of developing appropriate legal frameworks will undoubtedly intensify.[15]

This Essay intervenes at this critical juncture to provide lawmakers, market participants, and legal scholars with the analytical foundation necessary to comprehensively address decentralized stablecoins.[16] Our analysis proceeds in three integrated movements: examining the private law architecture of these protocols,[17] exploring potential private ordering solutions,[18] and comparing the divergent regulatory strategies employed by MiCAR and the GENIUS Act in the interim to manage their exclusion of decentralized protocols.[19]

We begin by undertaking a systematic examination of decentralized stablecoins' private law framework, and we use MakerDAO's DAI as the paradigmatic case study.[20] We map this protocol's technological architecture in detail, explaining how users deposit volatile digital assets into "non-custodial vaults" to generate DAI stablecoins through direct interaction with code, absent any issuing entity.[21] Building on this foundation, we dissect the implications of this structure across four domains. First, we demonstrate that the protocol

---

[11] *See generally* Odinet & Tosato, *Centralized Stablecoins*, *supra* note 2 (comprehensively analyzing the regulatory approaches to this type of stablecoin).

[12] *See infra* Part III.D.

[13] *See infra* Part III.D.

[14] For a discussion of novel insolvency issues, see Bruce, Odinet, & Tosato, *Crypto Orgs*, *supra* note 4, at 32-49.

[15] DUNE & ARTEMIS, *supra* note 1; ARTEMIS ANALYTICS ET AL., STABLECOIN PAYMENTS: FROM THE GROUND UP (May 2025), https://reports.artemisanalytics.com/stablecoins/artemis-stablecoin-payments-from-the-ground-up-2025.pdf.

[16] *See infra* Part III.D and legislative/regulatory timelines for future legal development.

[17] *See infra* Part I.

[18] *See infra* ra Part II.

[19] *See infra* Part III.

[20] *Infra* Part I.

[21] *Infra* Part I.A.

operates in the complete absence of contractual privity.[22] No bilateral or multilateral agreements exist between participants in the system nor with the protocol itself, which lacks legal personhood entirely.[23] This absence forecloses traditional breach of contract claims and eliminates baseline commercial protections like the implied duty of good faith and fair dealing.[24] Second, we identify significant uncertainties regarding users' property rights, particularly concerning assets deposited by wrongdoers and the legal basis for the protocol's automated seizure and auction mechanisms.[25] Third, we show that tort and criminal law provide minimal recourse given the absence of identifiable actors owing duties or possessing the requisite mental states for liability.[26] Fourth and lastly, we explain why fiduciary duty principles cannot coherently apply to the diffuse, pseudonymous, and conflicting relationships that characterize decentralized stablecoin ecosystems.[27]

We then pivot from diagnosis to potential cures by exploring three private ordering mechanisms that could mitigate the vulnerabilities we identified while still preserving the core principles that animate the decentralized stablecoin ecosystem.[28] We begin with the simplest intervention: radical transparency and accurate disclosure.[29] By abandoning their current terminology that misleadingly suggests traditional financial relationships, decentralized protocols could enable better informed consent.[30] We then examine decentralized insurance protocols that provide financial compensation for technical failures, thereby effectively creating synthetic warranties where explicit ones are disclaimed.[31] Finally, we analyze how legally incorporated DAOs with recognized personhood could serve as identifiable issuers and counterparties for "DLT-pragmatists" who seek efficiency gains without accepting complete legal exposure.[32] We admit that each solution involves trade-offs between decentralization ideals on the one hand and legal certainty on the other. Yet, taken together, we think these private ordering solutions demonstrate that the current legal vacuum reflects a choice in design rather than some inherent constraint in the technology itself.

---

[22] *Infra* Part I.A.1.
[23] *Infra* Part I.A.1.
[24] *Infra* Part I.A.1.
[25] *Infra* Part I.A.2.
[26] *Infra* Part I.A.3.
[27] *Infra* Part I.A.4.
[28] *Infra* Part II.
[29] *Infra* Part II.A.
[30] *Infra* Part II.A.
[31] *Infra* Part II.B.
[32] *Infra* Part II.C.

Finally, the Essay shifts to public law.[33] Although MiCAR and the GENIUS Act explicitly defer comprehensive regulation,[34] we analyze the distinct interim strategies they employ to manage the risks of decentralized protocols in the meantime.[35] We identify the "no entity to regulate" dilemma as the fundamental challenge that distinguishes these protocols from traditional financial technology, and then we examine how each regime responds.[36] MiCAR adopts functional definitions that technically encompass decentralized stablecoins while imposing structural requirements that these protocols simply cannot satisfy.[37] In doing so, the European Regulation effectively excludes decentralized stablecoins through compliance scenarios that are impossible and, in the end, transfers any potential regulatory liability to crypto-asset service providers.[38] The GENIUS Act, by contrast, inverts this approach by adopting structural prerequisites that categorically exclude protocols lacking identifiable issuers, thereby leaving this market in jurisdictional limbo.[39] We argue that this divergence between MiCAR and GENIUS reflects competing regulatory philosophies about whether the law should address what stablecoins functionally do or how they are structurally organized.[40] We observe that the study mandates in both laws signal regulatory recognition that decentralized protocols require fundamentally different tools than those developed for traditional financial institutions, yet through delay and path dependence MiCAR and GENIUS risk entrenching these systems to a degree that eventual regulation may prove ineffective.[41]

To develop these arguments, this Essay proceeds as follows. Part I examines the private law architecture of decentralized stablecoins through a comprehensive analysis of MakerDAO's DAI protocol.[42] Part II explores private ordering solutions such as implementing transparency requirements, adopting decentralized insurance, and forming legally recognized DAO entities.[43] Lastly, Part III provides our comparative analysis of MiCAR and the GENIUS Act's approaches to decentralized stablecoin regulation, looking to both what the current frameworks say about these tokens and how they mandate future studies.[44] We conclude by synthesizing our findings and by offering

[33] *Infra* Part III.
[34] *Infra* Part III.D.
[35] *Infra* Part III.
[36] *Infra* Part III.A.
[37] *Infra* Part III.A-B.
[38] *Infra* Part III.A-B.
[39] *Infra* Part III.A-C.
[40] *Infra* Part III.C.
[41] *Infra* Part III.D.
[42] *Infra* Part I.
[43] *Infra* Part II.
[44] *Infra* Part III.

recommendations for addressing the legal vacuum that currently surrounds these increasingly important financial instruments.

I. THE PRIVATE LAW ARCHITECTURE OF DECENTRALIZED STABLECOINS

In this Part, we undertake a comprehensive examination of MakerDAO's DAI. This token serves as the ideal case study to understand decentralized stablecoins as a whole, as it is the oldest, largest, and most technically mature.[45] First, we map MakerDAO's technological architecture and operational mechanics, with the aim of illuminating the key features of decentralized stablecoins as well as highlighting how they differ from their centralized counterparts.[46] Second, building on this technical foundation, we dissect their private law framework.[47] Our analysis reveals that decentralized stablecoins embody a singular trade-off: while they grant holders complete autonomy and disintermediation, they simultaneously provide no identifiable counterparties, create profound uncertainties regarding asset ownership, and leave users with minimal remedies in the face of technical failures, governance attacks, or economic design flaws.[48]

A. The Prototypical Decentralized Stablecoin: MakerDAO

DAI represents the paradigmatic decentralized stablecoin.[49] Launched in 2017, it is the oldest decentralized stablecoin in continuous operation, maintaining its peg throughout periods of both market euphoria and severe crashes.[50] Today, it commands the largest supply among its peers.[51] Crucially, DAI is issued and controlled by MakerDAO, which is not a company but rather

---

[45] See *infra* Part I.A.

[46] See *infra* Part I.A.

[47] See *infra* Part I.B.

[48] See *infra* Part I.B.

[49] *See* DEFI BEYOND THE HYPE, *supra* note 3

[50] For the market capitalization of DAI, see Top Stablecoin Tokens by Market Capitalization, COINMARKETCAP, https://coinmarketcap.com/view/stablecoin/ (last visited Aug. 15, 2025); Zoltán Vardai, Maker DeFi Lending Protocol Rebrands to Sky Ahead of USDS Stablecoin Launch, COINTELEGRAPH (Aug. 27, 2024), https://cointelegraph.com/news/maker-rebrands-sky-launches-usds-sky-token; Ethena's New Stablecoin Revolution, COINRANK (June 27, 2024), https://www.coinrank.io/learn/ethenas-new-stablecoin-revolution/; Liam Miller, Ethena Deep Dive: Understand USDe and ENA Token, NFT EVENING (June 11, 2025), https://nftevening.com/ethena-deep-dive-understand-usde-and-ena-token/.

[51] Lyle Daly, *3 Reasons to Buy DAI.one*, YAHOO FINANCE (Nov. 30, 2025), https://finance.yahoo.com/news/3-reasons-buy-dai-one-100500058.html.

a "protocol"[52] comprising multiple "smart contracts"[53] on the Ethereum network that execute predetermined operations automatically according to deterministic logic.[54] This architecture defines the decentralized stablecoin model: it functions without a single natural or legal person to own or control it.[55]

The MakerDAO protocol operates as an ecosystem populated by distinct groups, each pursuing different economic objectives and responding to different incentives. These participants can be divided into three categories: *Vault Owners* who lock volatile digital assets to generate DAI tokens pegged one-to-one with the US dollar, *Governors* who set the risk parameters of the protocol, and *Maintainers* who perform functions necessary for operational continuity.[56] These groups interact with the MakerDAO smart contracts directly.[57] Additionally, there is a fourth group, *DAI holders*, who acquire tokens through secondary markets without engaging with the protocol itself.[58]

Vault Owners initiate the creation ("minting") of DAIs.[59] This process involves these users interacting with the MakerDAO protocol to create Maker Vaults in which they deposit approved digital assets (such as Ether or Wrapped Bitcoin).[60] Each Vault is distinct and segregated, ensuring that assets from different users are never commingled.[61] Moreover, the Vault is non-custodial, meaning that its creator retains exclusive control over the assets therein via their private keys, subject only to the protocol's immutable code, rather than surrendering control to another person.[62]

Once assets are deposited in a Maker Vault, the MakerDAO protocol permits its owner to generate DAI up to a predetermined percentage of the value of those assets.[63] These ratios vary by asset type and are established through governance.[64] For instance, a user depositing $1,000 worth of Ether

---

[52] *See The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*, MAKERDAO, https://web.archive.org/web/20240415212520/https://makerdao.com/da/whitepaper/ [https://perma.cc/32LZ-BMXM] (last visited Apr 15, 2024) [hereinafter *Maker White Paper*].

[53] *See id.* at 1.

[54] *See id.* at 1.

[55] *See id.* at 1, 7.

[56] *See id.* at 7-12, 19.

[57] *See id.* at 7-12.

[58] *See id.* at 12.

[59] *See id.* at 7.

[60] *See id.* at 7. Technically, the user sends a transaction to the protocol's Vat contract, which records the user's locked balance and permits the corresponding issuance of DAI. Id.

[61] *See id.* at 7.

[62] *See id. at* 7.

[63] *See id.* at 14-15.

[64] *See id.* at 14-15

might be able to generate up to $750 worth of DAI, depending on the specific risk parameters in force at that time.[65]

The rules governing the MakerDAO protocol and the Maker Vaults are determined by Governors.[66] These are individuals or entities who hold MKR tokens, which are transferrable and grant voting rights proportional to holdings.[67] Governors set critical system parameters including which digital assets are approved for deposit into Maker Vaults, the maximum DAI generation ratios for each asset type, and various fees charged to Vault owners.[68] Governors receive compensation from such fees, thereby incentivizing prudent risk management to maintain system solvency and the DAI peg.[69]

To maintain the peg of one DAI to one US Dollar and ensure operational continuity, MakerDAO relies on Maintainers, an umbrella category including several subgroups that contribute to the functioning of the protocol and its stability.[70] At any moment, Vault Owners may reclaim their deposited assets by repaying the generated DAI plus accrued fees.[71] However, throughout the duration of a Vault's existence, if the market value of the deposited assets declines below the safety threshold set by Governors, the protocol automatically seizes and auctions them to a pre-approved groups of buyers known as *Keepers*, who bid using DAI.[72] The proceeds of these auctions are then immediately removed from circulation ("burned"), reducing the total DAI supply to maintain the one-to-one dollar peg and ensure system solvency.[73] In this process, Oracles, another sub-group of Maintainers, play a vital role by supplying the trusted, real-time price feeds the MakerDAO protocol uses to value the Vault assets and trigger the necessary auctions.[74]

---

[65] *See id.* at 14-15.

[66] *See id.* at 14.

[67] *See id.* at 14. The MKR token was launched in 2017 to facilitate decentralized governance. It grants technical powers to vote on variable parameters that are cardinal to the operation of MakerDAO.

[68] *See id.* at 14-15. Governors vote to establish the Liquidation Ratio (the threshold at which assets in vaults are seized and auctioned), the Stability Fee (a variable fee paid by Vault Owners to use the protocol), the Ceilings (the maximum total DAI that can be minted from a specific asset type), and the Liquidation Penalty (a fee charged to users whose Vaults are seized due to the value of the assets therein falling below the liquidation ratio). Id.

[69] *See id.* at 14

[70] *See id.* at 9-11, 19 (detailing the roles of Keepers, Oracles, and DAO Teams).

[71] *See id.* at 7.

[72] Keepers are independent market participants (often automated bots) who profit by arbitraging the difference between the discounted auction price of the seized collateral and its market price. *See id.* at 9.

[73] *See id.* at 8-9. By burning the DAI received from the auction, the protocol effectively covers the shortfall that the original Vault Owner failed to address. *Id.*

[74] *See id.* at 9-11.

As the ultimate safeguard against catastrophic failure, whether from extreme market events or technical attacks, MakerDAO incorporates an Emergency Shutdown mechanism.[75] Upon activation following a vote of Governors, the protocol freezes: vault creation ceases, price feeds lock at final values, and a three-phase settlement process commences.[76] First, Vault Owners withdraw any excess deposited assets not backing outstanding DAI.[77] Second, pending auctions are completed.[78] Third, DAI holders claim proportional shares of the remaining asset portfolio at fixed rates.[79] Critically, if the aggregate value of the assets falls below the total DAI supply, holders receive less than one dollar's worth of assets per token, effectively breaking the peg.[80]

This architecture markedly differentiates decentralized stablecoins from their centralized counterparts. With centralized stablecoins like USDC (Circle) or USDT (Tether), an identifiable issuer mints tokens on demand pursuant to contractual terms, creating mutual rights and obligations between issuer and user.[81] By contrast, MakerDAO merely deploys software with predetermined characteristics on the Ethereum blockchain, enabling users to mint DAI themselves through automated processes without any counterparty involvement.[82] This distinction carries through to asset custody: for centralized stablecoins, users transfer assets to the issuer in return for digital tokens and a contractual redemption right.[83] With decentralized stablecoins, users lock assets in smart contracts while retaining exclusive control through their private keys, subject only to the operational mechanisms of the protocol.[84] The difference is categorical: centralized stablecoins establish synallagmatic relationships between identifiable parties that are legally binding, while decentralized stablecoins function as automated machines made available for public self-service use, operating without legal relationships or recourse to any entity, and under explicit disclaimers that the technology is "unproven," carries "inherent risk," and is provided with "no warranty" against "complete failure."[85]

---

[75] *Id.*, at 19.

[76] *Id.*, at 19-20. By burning the DAI received from the auction, the protocol effectively "pays back" the debt that the original Vault Owner failed to cover, removing that DAI from the total supply. *See id.*

[77] *Id.*, at 19-20.

[78] *Id.*, at 19-20.

[79] *Id.*, at 19-20

[80] *Id.*, at 20.

[81] *See* Odinet & Tosato, *Centralized Stablecoins*, *supra* note2, at *6-11 (analyzing contractual framework of centralized stablecoins).

[82] *See infra* Part II.

[83] *See infra* Part II.

[84] *Id.*, at 7.

[85] *Id.*, at 18.

B. Study and Results

Having mapped MakerDAO's technological architecture, we now turn to examining its private law framework. Our analysis sheds light on the legal landscape of decentralized tokens as a subcategory of stablecoins more broadly. This investigation required assembling documentation dispersed across multiple websites and entities, a fragmentation that itself signals the protocol's decentralized nature.[86] The relevant materials include terms regarding the Dai Foundation's stewardship of intellectual property, separate agreements for various user interfaces, residual documents from the now-dissolved Maker Foundation, and the recent rebranding from MakerDAO to Sky.[87] Most tellingly, no terms of service specifically govern the issuance, holding, or use of DAI itself.[88] The cardinal document is MakerDAO's technical white paper, which is a descriptive explanation of technological mechanics, not a source of legal rights and obligations.[89]

While our analysis necessarily captures a snapshot in time (specifically, July 2025),[90] the private law characteristics we identify transcend this limitation. Four crucial elements become apparent: (1) the absence of a contractual counterparty, (2) uncertainties regarding property rights, (3) tenuous tort and criminal law remedies, and (4) the uncertain application of fiduciary principles.[91] These structural features do not stem from idiosyncratic drafting choices or temporary oversights, rather they are inherent to autonomous protocols operating without legal personhood.[92] For DAI holders, this translates into unique vulnerabilities compared to centralized stablecoin users.[93]

1. The Counterparty Void

From a private law perspective, the most fundamental characteristic of MakerDAO's structure is the complete absence of contractual relationships

[86] *See* generally *supra* Part I.A.

[87] *See Terms of Service*, THE DAI FOUND., https://daifoundation.org/terms-of-service/ (last updated Mar. 8, 2021); *Terms*, MAKER FOUND., https://foundation.app/terms (last updated May 30, 2024); Introducing Sky, SKY, https://sky.money/ (last visited Sept. 7, 2025).

[88] Compare Tether ToS, TETHER, https://tether.to/en/legal/#terms-of-service (last updated Sept. 2, 2022) (establishing contractual terms for USDT), with Maker White Paper, *supra* note 52 (providing only technical descriptions).

[89] *See* Maker White Paper, *supra* note 52.

[90] The protocol's recent rebranding to Sky exemplifies this fluidity. See Vardai, *supra* note 50

[91] *See infra* Part II.B.1-4 and accompanying discussion.

[92] *See* DEFI BEYOND THE HYPE, *supra* note 3, at 9-10; see Bruce, Odinet & Tosato, *Crypto Orgs.*, *supra* note 4.

[93] For comparison, see Bruce, Odinet, & Tosato, *Stablecoins*, *supra* note 2.

within its ecosystem.[94] A contract requires an agreement between two or more persons, yet no such bilateral or multilateral relationships exist when users interact with the MakerDAO protocol.[95] Despite the complex ecosystem involving Vault Owners, DAI Holders, MKR Governors, and various Maintainers, none of these groups enter contractual relationships with each other.[96] Nor do they stipulate binding agreements with the protocol itself, as it possesses no legal personhood and thus lacks the capacity for such agreements.[97] It is simply code executing on the Ethereum blockchain.[98]

This contractual void encompasses every interaction within the protocol. Vault Owners who deposit assets receive no promises from any party; they simply interact with smart contracts that execute predetermined functions.[99] DAI Holders acquire tokens that represent no claim against any issuer and cannot even be used directly to obtain assets from a Maker Vault.[100] Even MKR Governors, who vote on critical system parameters, have no contractual relationship with Vault Owners, let alone DAI holders; they merely participate in a decentralized voting mechanism.[101]

Our analysis reveals that this contractual absence persists despite the protocol's documentation using terminology that superficially implies bilateral relationships.[102] Terms like "collateral," "debt," "Collateralized Debt Positions," and "liquidation" pervade the white paper, suggesting that one party lends DAI pursuant to agreed terms with digital assets serving as security.[103] This language misleadingly signals that users borrow from a lender who holds security interests, which is a fundamental mischaracterization of the actual mechanics.[104] While the vault system may functionally echo secured lending dynamics, no lender exists, no borrower exists, no loan agreement exists, and no security interest in the conventional legal sense exists.

---

[94] *See* Maker White Paper, *supra* note 52, at 1 (describing the Maker Protocol as a "decentralized community").

[95] *See* 1 WILLISTON ON CONTRACTS § 1:1 (4th ed. 2024) (requiring agreement between parties for contract formation).

[96] *Id.*, at 7-12, 19.

[97] *See* Bruce, Odinet, & Tosato, *Crypto Orgs*, *supra* note 4, at a 12.

[98] Carla Reyes, *(Un)Corporate Crypto-Governance*, 88 FORDHAM L. REV. 1875, 1907-08 (2020).

[99] *See* Maker White Paper, *supra* note 52, at 7.

[100] Odinet & Tosato, *Centralized Stablecoins*, *supra* note 2, at 14.

[101] Maker White Paper, *supra* note 52, at 7-6.

[102] *Id.*, at 6-9.

[103] *Id.* (using these terms throughout).

[104] *See Maker Protocol 101*, MAKER PROTOCOL TECH. DOCS 6-7 (Dec. 8, 2020), https://drive.google.com/file/d/1VtGV8Ct2iBO8WjWsjFYLg5DnwlGmetSp/view?pli=1.

The private law implications of this architecture are severe. As we detail below, should the protocol malfunction (whether through technical failures, governance attacks, oracle manipulations, or economic design flaws) users have no contractual recourse.[105] They cannot sue for breach of contract because no agreement exists. They cannot demand damages or specific performance because no party owes them any obligations.[106] This represents not merely weak contractual protection but its categorical absence: a legal lacuna that distinguishes decentralized stablecoins from every traditional financial instrument and even their centralized stablecoin counterparts.[107]

Moreover, the absence of contractual relationships has ramifications that extend beyond the unavailability of remedies. Persons interacting with MakerDAO and DAI holders lack protection against adverse protocol modifications, possess no disclosure rights regarding system risks or governance decisions, and enjoy no procedural safeguards such as notice periods or dispute resolution mechanisms. In a similar vein, the implied duty of good faith and fair dealing which establishes baseline standards of commercial conduct, is entirely absent.[108] This leaves the ecosystem exposed to sharp practices and opportunistic behavior that, while perhaps permissible in the harshest of arm's-length dealings, fundamentally defy the reasonable expectations of participants relying on a stable financial infrastructure.

2. Instability Regarding Ownership, Control, and Property Rights

The absence of contractual relationships creates corresponding complications in property law. For Vault Owners, whatever property rights they held in the deposited digital assets continue unaltered. Since no contractual transfer occurs and the protocol lacks legal personhood, there is no change in the *status quo ante*.[109] Similarly, Vault Owners acquire full ownership of generated DAI consistent with the general principles governing property rights in intangible assets, and subsequent transfers follow the regime established by Article 12 of the Uniform Commercial Code for controllable electronic

---

[105] *See* Maker White Paper, *supra* note 52 , at 18.

[106] *See* RESTATEMENT (SECOND) OF CONTRACTS § 1 (AM. LAW INST. 1981) (defining contract as promise for breach of which law gives remedy).

[107] *See* Odinet & Tosato, *Centralized Stablecoins, supra* note 2, at _.

[108] RESTATEMENT (SECOND) OF CONTRACTS § 205 (AM. L. INST. 1981); see also U.C.C. § 1-304 (imposing the duty of good faith in every contract under the UCC), 201(b)(20) (defining "good faith").

[109] *See* Maker White Paper, *supra* note 52 , at 7 (describing vaults as "non-custodial").

records.[110] This appears straightforward, yet significant uncertainties emerge when fact patterns deviate from the ordinary course.

A particularly complex scenario involves stolen digital assets deposited into Maker Vaults to generate DAI. While the original owner retains proprietary rights in misappropriated assets even within the vault, the status of DAI generated from such assets presents novel questions.[111] Drawing on equity principles, courts might impose a constructive trust, treating the wrongdoer as holding generated DAI for the rightful owner of the stolen assets.[112] The doctrinal foundation would likely rest on knowing receipt (a principle under which a defendant who deals with trust property in a manner inconsistent with the trust is held accountable to the beneficiary).[113] Courts have consistently held that when stolen property generates proceeds (whether through sale, investment, or transformation) original owners may trace their interest into substitute property.[114] The underlying principle is clear: allowing wrongdoers to retain proceeds from stolen property would unjustly enrich them while also incentivizing theft.

However, DAI generation differs fundamentally from traditional conversion scenarios. The wrongdoer does not exchange stolen assets for DAI but uses them as inputs to an algorithmic process that creates new tokens while leaving the original assets intact within the vault.[115] This algorithmic intermediation creates a level of separation between the wrongdoer's actions and resulting DAI, which we see as distinguishing it from direct conversions of tangible property. Further complications arise when wrongdoers combine stolen assets with legitimate holdings in the same vault, as the fractional generation of DAI relative to total asset value would require courts to apply mixed-fund tracing principles to determine proportional entitlements.[116]

---

[110] U.C.C. § 12-102(a)(2) (AM. LAW INST. & UNIF. LAW COMM'N 2022). See Andrea Tosato and Christopher K. Odinet, *Digital Assets and the Property Question*, 78 FLA. L. REV. (forthcoming 2026); available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5151907 [hereinafter Odinet & Tosato, *Property Question*].

[111] *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 58 (AM. LAW INST. 2011).

[112] George P. Costigan, Jr., *The Classification of Trusts as Express, Resulting, and Constructive*, 27 HARV. L. REV. 437, 449 (1914).

[113] John D. McCamus, Restitutionary Remedies in Three-Party Cases: A Comparative Perspective, 14 FIU L. Rev. 65, 70 (2020);

[114] *See* United States v. Henshaw, 388 F.3d 738, 741 (10th Cir. 2004); Commodity Futures Trading Comm'n v. Walsh, 712 F.3d 735, 748 (2d Cir. 2013).

[115] *See* Maker White Paper, *supra* note 52, at 7-8.

[116] *See* Austin W. Scott, The Right to Follow Money Wrongfully Mingled with Other Money, 27 HARV. L. REV. 125, 128-30 (1913).

Most critically, the practical utility of any constructive trust remedy faces severe limitations from Article 12's qualified purchaser rule.[117] Once DAI enters circulation, acquirers who obtain tokens in good faith, for value, and without notice of competing claims take free of any constructive trust.[118] Given the rapid velocity of digital asset markets, where tokens change hands multiple times daily across global exchanges, this protection would shield virtually all subsequent holders except the original wrongdoer.[119]

Uncertainty also pervades MakerDAO's core stabilization mechanism. When the protocol automatically seizes vault assets due to price movements and auctions them to Keepers, the legal basis for this transfer is beset with uncertainties. Assets move from vault to auction to Keeper, yet technological movement alone is not sufficient for a transfer of ownership. Property law requires either consent for voluntary dispositions or legal authorization for involuntary dispossession.[120] Here, neither appears to be present. Vault Owners never sign agreements authorizing seizure; they merely deposit assets into smart contracts with predetermined functions.[121] While one might argue that using the protocol constitutes implicit consent to its mechanics, this theory encounters serious obstacles. First, consent typically requires a counterparty capable of receiving it,[122] yet the protocol lacks legal personhood.[123] Second, if the vault owner lacks capacity to consent (due to minority, mental incapacity, or duress) or if the seizure results from technical malfunction rather than legitimate triggers, property law principles operate to make the transaction void or voidable.[124]

These uncertainties directly affect Keepers who acquire assets at auction, creating multiple layers of legal risk. As explained above, their ability to acquire good title is uncertain given the absence of valid consent from Vault Owners. Moreover, Keepers may not be covered by the qualified purchaser rule under

---

[117] U.C.C. § 12-102(a)(2) (defining "qualifying purchaser"). *See* Tosato & Odinet, *Property Question*, *supra* note 110, at *42-51 (providing an extensive analysis of the genesis and current state of the Article 12 qualifying purchaser rule)

[118] *See id.*

[119] See DUNE & ARTEMIS, *supra* note 1, at 12 (documenting high transaction volumes in DeFi markets).

[120] *See generally* Kurtz, Hovenkamp, Brown, Odinet, and Lindsey's Cases and Materials on American Property Law (8th ed 2026) (discussing both voluntary and involuntary transfers of property rights).

[121] *See supra* Part I.A.

[122] *See, e.g.*, Cal. Civ. Code §§ 1550, 1565. *See also* Restatement Second of Contracts §§ 3, 18.

[123] *See supra* Part I.B.

[124] *See, e.g.*, Emile v. Regal Remodelers, L.L.C., 23-174 380 So. 3d 696, 703-05 (La. App. 5 Cir. 1/31/24).

Article 12, as the governing provision requires a voluntary transaction.[125] The statutory framework assumes bilateral exchanges that simply do not exist in this context.[126] Keepers bid in an automated auction conducted by an ownerless protocol, rather than entering into an agreement with the Vault Owner.[127] Even if courts were to recognize Keepers as purchasers, the "good faith" and "without knowledge" of competing claims requirements of the qualified purchaser rule could pose significant hurdles.[128] For example, a Keeper who acquires assets during a known oracle manipulation or while governance debates a potential bug could fail the good faith test entirely. Thus, while subsequent purchasers from Keepers might qualify as qualified purchasers under Article 12, Keepers themselves remain exposed to claims from Vault Owners for participating in potentially invalid transfers.

Ultimately, while property law principles apply to decentralized stablecoins in theory, the protocols' technological architecture renders their application uncertain, shrouding in doubt basic questions about title, validity of transfers, and the resolution of competing claims. These ambiguities may be tolerated when market function smoothly, but they foreshadow chaos in bankruptcy proceedings where property rights must be definitively established, priorities determined, and assets distributed as guided by property law.

3. Inadequate Remedies in Tort and Criminal Law

With contractual claims foreclosed, DAI users must look to tort or criminal law for recourse. These avenues, however, prove equally inhospitable given MakerDAO's decentralized and autonomous architecture. While actions against external attackers who hack vaults or exploit the protocol present no conceptual difficulties (though significant practical challenges in identifying perpetrators), losses from internal malfunctions, design flaws, or economic failures encounter a more fundamental problem: there may be no person to sue or prosecute.[129]

Negligence claims face an immediate barrier in establishing duty of care.[130] Plaintiffs would need to convince courts that a diffuse, pseudonymous, ever-changing group of global actors—Governors voting on risk parameters, Maintainers contributing code, Oracles providing price feeds—owe specific

---

[125] *See* U.C.C. § 12-102(2), 104 (Am. L. Inst. & Unif. L. Comm'n. 2022).

[126] *Id.*

[127] *See supra* Part I.A.

[128] U.C.C. § 12-102(a)(2).

[129] *See* Reyes, *supra* note 98, at 1907-08 n.235 (discussing lack of existing law imposing duties on software developers).

[130] RESTATEMENT (SECOND) OF TORTS § 282 (AM. LAW INST. 1965).

legal duties to every anonymous protocol user.[131] Courts have traditionally rejected such expansive duties between parties lacking direct relationships, particularly for open-source projects where software licenses explicitly disclaim liability.[132] Even if duty were established, proving breach would require demonstrating that specific governance votes or code contributions fell below a "reasonable DAO participant" standard: a standard that no court has yet articulated and that would require unprecedented technical expertise to apply.[133] Perhaps most decisively, the economic loss doctrine, which bars negligence recovery for pure financial losses absent physical injury or property damage, would likely preclude many if not most claims.[134]

Conversion claims prove equally unsuitable albeit for different reasons.[135] This tort requires intentional exercise of dominion over another's property without consent.[136] When the protocol automatically seizes and auctions vault assets due to price movements (whether from legitimate oracle feeds or software bugs), no human exercises the requisite volitional act.[137] The user's initial decision to deposit assets into smart contracts, combined with the protocol's automated nature and explicit warnings about liquidation risks, likely precludes any finding of wrongful intent.[138]

Fraudulent misrepresentation claims founder on the extensive risk disclosures throughout MakerDAO's documentation.[139] While the protocol's marketing materials describe DAI as "stable," the white paper warns users of "inherent risk," potential "complete failure," and that the technology is "unproven" with "no warranty."[140] Courts would likely find reliance on stability claims unjustifiable given these explicit disclaimers, particularly for users sophisticated enough to navigate the complex vault creation process.[141]

Criminal law offers a theoretically potent but practically constrained avenue for recourse. In principle, the legal analysis regarding external attacks is

---

[131] *See* Maker White Paper, *supra* note 52, at 9-11, 14, 19.

[132] *See* Reyes, *supra* note 98, at 1907-08.

[133] RESTATEMENT (SECOND) OF TORTS § 285 cmt. d (requiring the standard of a "reasonable man under the circumstances").

[134] *See* Christopher K. Odinet, Modernizing Mortgage Law, 100 N.C. L. REV. 89, 141-42 (2021) (explaining economic loss doctrine's limitation on tort claims for financial losses).

[135] RESTATEMENT (SECOND) OF TORTS § 222A.

[136] *Id.*

[137] *See* Maker White Paper, *supra* note 52, at 8-9 (describing automated liquidation process).

[138] *Id.* at 18 (warning of liquidation risks).

[139] RESTATEMENT (SECOND) OF TORTS § 525 (requiring justifiable reliance for fraud claims).

[140] *See* Maker White Paper, *supra* note 52, at 18.

[141] *See id.*, at 7-9 (detailing complex vault creation mechanics).

straightforward: malicious actors who exploit code vulnerabilities to siphon assets from Maker Vaults commit identifiable crimes, ranging from computer fraud to grand larceny.[142] Should a hacker discover a reentrancy vulnerability or manipulate an oracle to drain value from the protocol, the criminal nature of the act is not in doubt. However, the effectiveness of this protection is severely blunted by the operational realities of the ecosystem. Victims and prosecutors alike often face the insurmountable challenge of deanonymizing sophisticated actors who operate through obfuscated network channels, often from jurisdictions that lack extradition treaties or robust cybercrime enforcement mechanisms.[143] Consequently, while the law formally criminalizes such theft, it rarely provides a mechanism for actual recovery or retribution.[144]

A far more complex question arises regarding the potential criminal liability of the protocol's own architects, such as Governors and Maintainers, for losses stemming from their governance decisions or code contributions. Generally, establishing liability here encounters a profound *mens rea* barrier.[145] Unless prosecutors can prove that a Governor voted for a parameter change or a developer pushed code with the specific intent to defraud users (a "rug pull"), mere negligence or poor economic design fails to meet the threshold for criminal intent.[146] It should also be noted that, historically, software developers (particularly in non-custodial contexts) have also been viewed as neutral toolmakers, insulated from liability for how their code is used or how it performs.[147]

However, this shield of neutrality is showing signs of fracture. Recent enforcement actions, most notably the 2024 prosecution of the Samourai Wallet founders, suggest U.S. authorities are increasingly willing to actively target software creators.[148] In that case, prosecutors successfully argued that

---

[142] *See* 18 U.S.C. § 1030 (computer fraud). See, e.g., N.Y. Penal Law § 155.42 (grand larceny in the first degree),

[143] *See* United States v. Storm & Semenov, No. 1:23-cr-00430 (S.D.N.Y. filed Aug. 23, 2023) (illustrating challenges in prosecuting pseudonymous protocol developers).

[144] *See id.*

[145] Mens rea, BLACK'S LAW DICTIONARY (11th ed. 2019).

[146] *See* MODEL PENAL CODE § 2.02 (AM. LAW INST. 1985) (requiring purposeful, knowing, reckless, or negligent mental state).

[147] *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984) (establishing that manufacturers of technologies capable of "substantial noninfringing uses" are not liable for the infringing acts of users); Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1139–41 (9th Cir. 1999) (holding that source code is protected speech under the First Amendment). *See also* Bryan Casey & Mark A. Lemley, *You Might Be a Robot*, 105 Cornell L. Rev. 287, 333 (2020) (noting that software developers have historically been insulated from liability)

[148] *See* Press Release, U.S. Att'y's Off., S.D.N.Y., Founders of Samourai Wallet Cryptocurrency Mixing Service Charged with Money Laundering and Unlicensed Money Transmitting Offenses (Apr. 24, 2024).

developers could be criminally liable for operating an unlicensed money transmitting business, explicitly rejecting the defense that non-custodial software merely empowered users to manage their own funds.[149] While the Samourai facts involved active marketing to illicit actors and centralized coordination servers (both of which are features that make it distinguishable from a protocol like MakerDAO), the underlying legal theory is perilous. The theory suggests that control over the process, even without their taking custody of assets, may suffice for criminal liability. This, in turn, could potentially expose Governors who set risk parameters or Maintainers who operate critical infrastructure to prosecution if the protocol is later deemed to facilitate illicit activity.[150]

Overall, it appears that tort and criminal law, like contract and property law before them, provide minimal practical protection for DAI users experiencing losses.[151]

4. Fiduciary Liability

Beyond the confines of contract, tort, and criminal law, a final potential avenue of recourse for Vault Owners and DAI holders lies in fiduciary principles. In the event of losses stemming from adverse governance decisions or technical failures, aggrieved parties might allege that the protocol's Governors and Maintainers breached fiduciary duties owed to them.

The theory that distributed ledger technology (DLT) software developers should be treated as fiduciaries was first comprehensively articulated by Angela Walch.[152] She argued that despite their "decentralized" reputation, public blockchain networks like Bitcoin and Ethereum (and by extension protocols such as MakerDAO) are controlled by identifiable "core developers" who exercise significant power over these systems.[153]

---

[149] *See* Indictment at 6–8, United States v. Rodriguez, No. 1:24-cr-00244 (S.D.N.Y. Apr. 24, 2024) (alleging that defendants "executed" transactions by operating a centralized server that coordinated the CoinJoin mixing process)

[150] *See id.*, at 13 (noting that defendants "maintained control" over the software infrastructure).

[151] *See supra* Parts I.B.1-3.

[152] Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains* in Philipp Hacker and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019)

[153] *Id.* at 58.

Drawing on Tamar Frankel's influential work,[154] Walch contended that these developers resemble traditional fiduciaries because they offer socially desirable expert services requiring specialized technical knowledge, exercise control over property and power entrusted to them, create vulnerability to misuse among those who rely on their decisions, and operate in contexts where users lack adequate self-protection mechanisms or market safeguards.[155] She therefore normatively argued that this power should carry corresponding duties of care and loyalty, thereby ensuring accountability for the stewards of these novel systems.[156]

Recent litigation has tested this theory. In *Tulip Trading v Van der Laan* ("*Tulip Trading*"),[157] the English Court of Appeal held that while fiduciary duties for DLT software developers are not established under current law, their existence was an arguable proposition, raising a serious issue to be tried.[158] Lord Justice Birss stated:

> There is … a realistic argument along the following lines. … developers have undertaken a role which involves making discretionary decisions and exercising power for and on behalf of other people, in relation to property owned by those other people. That property has been entrusted into the care of the developers. The developers therefore are fiduciaries[159]

Notwithstanding this judicial openness and setting aside the comparative law distinctions regarding the precise content of fiduciary duties across common law jurisdictions,[160] we believe imposing such duties on MakerDAO's Governors and Maintainers faces formidable doctrinal obstacles. This is particularly evident for DAI Holders who acquire tokens in secondary markets. These users never interact with the protocol, deposit no assets into its care, and delegate authority to Governors and Maintainers indirectly at best, if

---

[154] *See generally* TAMAR FRANKEL, FIDUCIARY LAW (2011) (extensively discussing fiduciary law).

[155] *Id. at* 64-65, drawing on Tamar Frankel, *Fiduciary Law* (Oxford University Press 2011), 6.

[156] *Id.* at 69.

[157] *Tulip Trading Ltd. v. Van der Laan* [2022] EWHC 667 (Ch), [2022] 2 All E.R. (Comm) 624; *Tulip Trading Ltd. v. Van der Laan* [2023] EWCA Civ 83, [2023] 4 W.L.R. 16 (Eng.). For an insightful analysis of these cases, see Peter Hunn, Mathew Kimber and Sarah Worthington, Developers of Software Code as Fiduciaries: Whatever Next for Cryptoassets and Bitcoin? (December 04, 2024). Available at SSRN: https://ssrn.com/abstract=5060411 or http://dx.doi.org/10.2139/ssrn.5060411

[158] *Tulip Trading Ltd. v. Van der Laan* [2023] EWCA Civ 83, at 86-91.

[159] *Id.*, at 86, but contrast *Tulip Trading v Van der Laan* [2022] EWHC 667 (Ch) at 73.

[160] Even among common law jurisdictions there are differences in how fiduciary relationships are theorized and the precise elements required for their establishment.

at all. Their relationship with the protocol is entirely remote and impersonal. Recognizing a fiduciary bond on this basis would stretch the doctrine beyond its breaking point, as the core requirement of a direct entrustment relationship is visibly absent.[161]

The analysis is more complex for Vault Owners, who deposit digital assets into the protocol's smart contracts. As a threshold matter, Maintainers clearly fail to satisfy fiduciary requirements: Keepers merely purchase assets at auction, Oracles provide automated price feeds, and Developers contribute code without any meaningful interaction with Vault Owners. The Vault Owner-Governor relationship, by contrast, might superficially resemble a fiduciary bond, given the latter's power to affect the assets deposited by the former into the protocol. Yet a systematic analysis reveals distinctions that, to our mind, preclude such a characterization.

Considering the first element of Walch's framework, Governors arguably *provide socially desirable services through specialized knowledge*, setting complex risk parameters to maintain DAI's peg and MakerDAO's solvency.[162] This could be viewed as analogous to investment advisory relationships and thus fiduciary in nature. But we see this parallel as being superficial. Governors operate impersonally within a decentralized system, setting general rules for protocol operation rather than providing individualized services to specific clients.[163] As their name suggests, they govern rather than provide the type of personalized professional engagement that characterizes traditional fiduciary relationships.[164]

Regarding the second element, *entrustment*, Vault Owners indeed deposit valuable digital assets into smart contracts, and Governors possess the power to trigger involuntary liquidations through parameter changes. Functionally, depositing assets into a Vault might be viewed as granting Governors the authority to determine when the assets should be sold. However, a critical distinction exists between the power to affect another's property and the power to act on their behalf. Fiduciary relationships require delegation of autonomous decision-making power, which is absent here. Vault Owners do not appoint Governors as agents, rather, they opt into a pre-existing governance structure. Governors cannot access vault assets directly; their power is a protocol feature, not user-entrusted authority.

The final two elements, *vulnerability* and the *lack of self-help remedies*, are also missing. Vault Owners are arguably exposed to Governor misconduct

---

[161] *See* Hunn et al., *supra* note 157 at, 15-16 (arriving at a similar conclusion in the context of public blockchain networks).

[162] *See id.*

[163] *See* Hunn et al., *supra* note 157 , at 15-16.

[164] *Id.* at 1901.

through incompetent risk assessments or conflicts of interest. But this vulnerability stems from protocol design, not entrustment. Furthermore, protocol documents explicitly place all technical risk on users. Users receive notice that they are interacting with experimental software on a strict caveat emptor basis. Moreover, the Governance Security Module imposes a twenty-four-hour delay between Governors' governance decisions and their execution, thereby reducing Vault Owners' vulnerability to a considerable extent.[165] It should not be overlooked that Vault Owners can close positions before adverse changes take effect. Thus, while volatility may increase exit costs, this reflects market economics rather than artificial barriers. The system thus replaces relational trust with algorithmic trust fortified by temporal safeguards (all aspects which users accept when entering the protocol).

Even accepting arguendo that Governors owe fiduciary duties to Vault Owners, applying traditional fiduciary principles would prove doctrinally incoherent and practically unworkable.

If Governors were deemed agents of Vault Owners, they would owe duties of performance in accordance with the express and implied terms of their arrangement, including a duty to act with care, competence, and diligence.[166] Yet construing these obligations would encounter insurmountable obstacles. No contract exists between pseudonymous Vault Owners and equally pseudonymous Governors to define the scope of such duties.[167] Even if courts were to imply a contractual relationship (itself a remarkable stretch given the absence of any direct interaction between these parties), the extensive disclaimers throughout MakerDAO's documentation would likely exclude any meaningful duty of care, as participants assume all risks.[168]

The duty of loyalty presents even greater conceptual difficulties. The orthodox view requires fiduciaries to subordinate their interests to those of their principals. Specifically, this entails the prophylactic duties to refrain from acquiring material benefits from third parties, acting as or on behalf of an adverse party, competing with the principal, or using the principal's property for personal gain.[169] Yet, applying this schema to MakerDAO is structurally problematic. Governors have no visibility into Vault Owners' identities, positions, or what constitutes their best interest. Furthermore, they vote collectively based on MKR token holdings, not as individualized agents serving specific principals. This collective decision-making mechanism diffuses

---

[165] For details, see *Maker Protocol 101*, *supra* note 104.

[166] *See* RESTATEMENT (THIRD) OF AGENCY §§ 8.07–8.08 (AM. LAW INST. 2006).

[167] *See supra* Part I.B.

[168] *See supra* Part I.B.

[169] *See* RESTATEMENT (THIRD) OF AGENCY §§ 8.01-8.06 (AM. LAW INST. 2006).

individual responsibility, thus making it difficult to attribute specific breaches to specific actors.

Even if individual responsibility could be isolated, the "multiple principals" problem remains fatal. Fiduciaries owe duties to each principal individually, yet different Vault Owners possess inherently conflicting economic interests. Some benefit from higher stability fees, others from lower. Some prefer conservative liquidation ratios, others aggressive parameters, Governors would face irreconcilable duty conflicts. Traditional fiduciary law offers only one solution to such conflicts: the fiduciary must cease acting.[170] Applied here, this would paralyze governance and precipitate system collapse.

Finally, even if courts somehow navigated these doctrinal impossibilities, traditional remedies would prove hollow. The primary remedy for breach of loyalty is disgorgement of ill-gotten profits.[171] Yet Governors receive no distinct transactional profits traceable to specific governance decisions affecting Vault assets. While stability fees flow to MKR holders collectively, these represent system-wide revenue from all vaults, not illicit profits extracted from a breach against a specific Vault Owner. Similarly, while MKR tokens may appreciate from sound governance, this general market appreciation cannot be causally linked to the specific losses of liquidated users. Without an illicit profit to disgorge, this remedy risks producing an empty judgment. Conversely, while plaintiffs might seek compensatory damages for market depreciation or liquidation losses,[172] recovering these "real" losses would require re-establishing the very causal links and duties of care that, as discussed above, are precluded by the absence of a contract as well as the economic loss doctrine.

II. POSSIBLE PRIVATE ORDERING SOLUTIONS

In Part I, we mapped the mechanics of decentralized stablecoins, revealing how their structural characteristics engender a state of unique private law fragility for stablecoin holders. In this Part II, we explore a menu of private ordering mechanisms that could address these vulnerabilities. Our purpose here is twofold. First, we demonstrate that it is possible to construct decentralized stablecoins that do not sacrifice core functionality yet that materially mitigate legal vulnerabilities within established principles of contract, property, and corporate law. Second, we explain ways that decentralized stablecoins can

[170] *See* RESTATEMENT (THIRD) OF AGENCY § 8.01 cmt. b.
[171] RESTATEMENT (THIRD) OF AGENCY § 8.01 cmt. d.
[172] RESTATEMENT (THIRD) OF AGENCY § 8.01 cmt. d.

compete not only on their technical innovation but also on their ability to offer quality legal frameworks.

To be sure, we recognize that voluntary adoption of these solutions faces significant headwinds. The architectures of extant decentralized stablecoins reflect both an intentional decision of developers to minimize their liability and a philosophical commitment to disintermediation.[173] Yet three market forces may soon catalyze change. Institutional participants and sophisticated retail users are increasingly prioritizing legal clarity, even within decentralized systems. Simultaneously, new protocols may challenge incumbents like MakerDAO by offering users more robust legal frameworks. Most significantly, impending regulatory intervention (which we examine in Part III) creates incentives for proactive reforms that preserve autonomy while addressing vulnerabilities.

A. Transparency and Accurate Disclosure Requirements

The simplest private ordering solution requires neither structural changes nor financial cost but rather a commitment to linguistic precision and radical honesty. Throughout the decentralized stablecoin ecosystem, protocols rely heavily on skeuomorphic terminology that creates false expectations of legal relationships.[174] MakerDAO's pervasive use of words like "collateral," "debt," "liquidation," and "Collateralized Debt Positions" exemplifies this problem. These terms fundamentally mischaracterize the legal reality, suggesting the existence of bilateral lending arrangements where, in fact, there are none.[175] This semantic misrepresentation, whether intentional, negligent or innocent, engenders cognitive dissonance between user expectations and actual risks, potentially attracting participants unprepared for the absence of legal recourse.[176]

To remedy this, protocol documentation should state unequivocally that users have no contractual counterparty, no entity to sue, no recourse beyond insurance coverage, and bear all economic and governance risks.[177] Rather than burying warnings in technical white papers, these disclosures should appear

---

[173] *See* Bruce, Odinet & Tosato, *Crypto Orgs*, *supra* note 4 , at *15-20) (discussing the ideological and economic incentives driving DLT networks).

[174] *See supra* Part I.B.1 (analyzing misleading terminology).

[175] Maker White Paper, *supra* note 52, at 6-9; Maker Protocol 101, *supra* note 104, at 6, 8.

[176] *See supra* Part I.B.1.

[177] Compare Maker White Paper, *supra* note 52, at 18 (warnings buried in technical details), with prominent risk disclosures in traditional financial products. See, e.g., 12 CFR 1024.6 (home loan information booklet); Tex. Fin. Code ch. 348. (required contract content and headings for motor vehicle installment sales agreements); Tex. Fin. Code ch. 393. (required fee schedule and alternatives information for payday and vehicle title loans).

prominently wherever users interact with the protocol: on websites, in wallet interfaces, and especially during the minting process.[178] The language should be plain, not technical: "No company backs this stablecoin. No one owes you anything. If the system fails, you alone bear the loss."[179]

Decentralized stablecoin developers should also retreat from simplistic metaphors and flawed analogies with traditional financial instruments in favor of descriptive accuracy. Protocols should adopt terminology that describes technological mechanics, without implying legal rights. For example, MakerDAO should use "locked assets," instead of "collateral" (which implies a security interest); "generated DAIs," as opposed to "debt" (which implies the existence of an obligation to someone); and, "automatic sales" should replace "liquidation" (which hints to either a margin call or a judicial process).[180] Such changes would preserve technical accuracy while eliminating the false comfort of familiar financial concepts. Protocols could even require users to complete comprehension tests to ensure that they understand the risks inherent to decentralized stablecoins.[181]

While transparency cannot create legal rights from nothing, it does serve a critical market function by allowing the possibility for users to make more informed decisions about risk.[182] Those seeking complete decentralization could proceed with full knowledge, while risk-averse actors might choose centralized alternatives or else to purchase insurance.[183] This solution would cost nothing to implement and compromises no philosophical principles, yet could prevent countless users from discovering too late that their "collateralized debt position" creates neither collateral rights nor debt obligations (merely exposure to autonomous code executing without recourse).[184]

B. Decentralized Insurance

Although linguistic precision and radical candor are valuable, they cannot fill the private law void that envelops decentralized stablecoins. To provide substantive remedies, developers could look to decentralized insurance.

---

[178] *See supra* Part I.A.

[179] Cf. Maker White Paper, *supra* note 52, at 18 (using technical language like "inherent risk" and "no warranty").

[180] *See supra* Part I.B.1

[181] Cf. SEC Rule 17a-4(j), 17 C.F.R. § 240.17a-4(j) (requiring broker-dealers to verify customer understanding of complex products).

[182] *See* Basic Inc. v. Levinson, 485 U.S. 224, 231-32 (1988) (establishing materiality standard for investment decisions).

[183] *See supra* Part II.A.

[184] *See supra* Parts I.B.1-4.

This mechanism would offer financial compensation for a range of possible failures while preserving core architectural principles, albeit at the price of increased operational complexity and direct financial cost. Decentralized insurance emerged as a direct market response to smart contract failures, offering financial protection without compromising the philosophical commitment to disintermediation.[185] Projects like Nexus Mutual, launched in 2019 as the first discretionary mutual for Ethereum risks, enable users to purchase coverage through pseudonymous transactions, with claims assessed by token-holder governance and payouts executed automatically through smart contracts.[186] By 2025, these protocols have expanded beyond simple smart contract coverage to address risks specific to stablecoins, with InsurAce offering protection against depegging events.[187]

This mechanism could mitigate several vulnerabilities inherent to decentralized stablecoins, without relying on intermediaries.[188] It would function as a synthetic warranty: where stablecoin protocols explicitly disclaim all liability for technical failures, users could purchase substitute protection from third-party insurance protocols. Coverage could protect against smart contract bugs causing unintended liquidations, oracle manipulations triggering erroneous asset seizures, and governance attacks exploiting protocol mechanics.[189] Users would purchase policies denominated in either a stablecoin or another digital asset, with premiums calculated based on historical failure rates and current risk parameters, thereby creating a functional substitute for contractual recourse: direct financial compensation for verifiable technical failures.[190]

Yet this solution is functionally constrained. Decentralized insurance is generally limited to events that are either objectively verifiable (parametric insurance) or subject to the consensus of claims assessors (discretionary coverage).[191] It is ill-suited to cover losses from legitimate governance decisions that prove detrimental, economic design flaws, protocol abandonment, or user error.[192] These risks stem from subjective human judgment and create

---

[185] *See* Core Contracts, ETHERISC, https://docs.etherisc.com/gif/core-contracts (describing parametric coverage via smart contracts).

[186] NEXUS MUTUAL, https://nexusmutual.io/ (last visited Sept. 7, 2025); Decentralized Insurance, MKT. RSCH., https://www.marketresearch.com/Global-Industry-Analysts-v1039/Decentralized-Insurance-41255273/ (last visited Sept. 7, 2025).

[187] Stablecoin De-Peg Cover, INSURACE PROTOCOL, https://docs.insurace.io/landing-page/documentation/cover-products/stablecoin-de-peg-cover (last visited Sept. 7, 2025).

[188] *See supra* Part I.B.1-4 (identifying MakerDAO vulnerabilities).

[189] *See* Gina Alsdorf & Jason Berkun, Is Blockchain the Next Big Thing for Insurance Companies?, REUTERS (Oct. 9, 2024).

[190] *See* Maker Protocol 101, *supra* note 186 and accompanying sources.

[191] *See* Alsdorf & Berkun, *supra* note 189.

[192] Maker White Paper, *supra* note 52, at 16-17 (acknowledging "black swan" risks).

intractable moral hazard problems.[193] Premium costs also reflect the experimental nature of these decentralized insurance protocols; coverage for a $10,000 position might cost $200-500 annually, making coverage economically viable only for larger positions or risk-averse users.[194]

Consequently, the most promising evolution lies in integration. Rather than requiring users to navigate separate insurance protocols, decentralized stablecoins could incorporate coverage options directly into their interfaces, perhaps even automating protection based on user-defined risk thresholds.[195] Such changes could transform decentralized insurance from an extrinsic hedging product into an intrinsic component of decentralized stablecoin architecture, providing meaningful protection while preserving the disintermediation that defines these systems.[196]

C. Corporate DAOs for DLT-Pragmatists

While decentralized insurance provides a mechanism for financial compensation, it ultimately leaves the private law void unresolved. To cure this structural defect requires a profound architectural concession: protocols must abandon complete decentralization and establish legal persons as identifiable issuers and counterparties. We recognize that this approach would likely be anathema to ideological purists who prize disintermediation and autonomy above all else. Nevertheless, we offer that the market for decentralized stablecoins is not monolithic.[197] A growing constituency, which we term "DLT-Pragmatists," seeks to escape the friction of traditional finance and the opacity of centralized stablecoins without accepting the abject legal exposures of pure decentralization.

For DLT-pragmatists, a decentralized autonomous organization (DAO) with legal personhood could offer an optimal compromise. Such DAOs occupy a middle ground: they preserve the automated operations and distributed governance that distinguish decentralized protocols from traditional financial institutions, while providing the identifiable counterparties, enforceable rights, and accessible remedies absent from pure protocols like MakerDAO. This approach would retain many of the structural characteristics that attract users to

---

[193] *Id.*

[194] *See* Crypto Insurance Gap Reveals $3.31 Trillion Market Opportunity, RISK & INSURANCE (June 17, 2025) (discussing insurance pricing challenges).

[195] *See supra* Part I.A.

[196] *See supra* note 186.

[197] *See* Bruce, Odinet & Tosato, *Crypto Orgs*, *supra* note 4 , at 15-20.

decentralized systems while restoring the legal relationships and recourse mechanisms necessary for a robust private law framework.[198]

Such entities would leverage emerging legal frameworks in Wyoming, Tennessee, and other jurisdictions that grant DAOs limited liability protection, recognize smart contracts as capable of creating binding agreements between parties, and allow for tokenized governance.[199] Such a legally incorporated DAO could issue stablecoins through "contractware"—embedding terms directly in token metadata or implementing programmable electronic instruments that execute contractual provisions automatically.[200] Thus, users would enter into binding contracts with the issuing DAO through their protocol interactions, thus establishing bilateral legal relationships currently absent from decentralized stablecoins.[201]

This structure would systematically address the private law voids identified in Part I.[202] First, the issuing DAO would cure the counterparty deficiency by serving as a liable entity for both contractual and tort claims. Now, token holders could sue for breach when systems do not perform as agreed or seek damages when negligent operations cause losses. Beyond these basic remedies, the DAO's legal personhood could support fiduciary duties to token holders and thereby create accountability mechanisms that are impossible under current architectures.[203] Second, the structure under consideration would resolve the property transfer ambiguities that plague autonomous protocols. Possessing the capacity to legally control or own deposited assets, the DAO could execute valid transfers and convey clear title to purchasers at auction. This would eliminate the uncertainty surrounding current liquidation mechanisms in which assets move from smart contracts to acquirers without any legal person authorizing the transfer. Moreover, this formal status would clarify the application of Article 12's qualified purchaser rules by establishing precisely when the DAO takes free of competing claims and when purchasers from the DAO receive protected status.[204] Third, this approach could enhance procedural

---

[198] *See* Jason Grant Allen, Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language, in SMART LEGAL CONTRACTS: COMPUTABLE LAW IN THEORY AND PRACTICE 23 (Jason Grant Allen & Peter Hunn eds., 2022).

[199] WYO. STAT. ANN. § 17-31-101 et seq. (2024); TENN. CODE ANN. § 48-250-101 et seq. (2024).

[200] Allen, *supra* note 198, at 23-25.

[201] *See supra* Part I.B.1 (identifying counterparty void).

[202] *See supra* Parts I.B.1-4.

[203] *See* WYO. STAT. ANN. § 17-31-106 (allowing DAO operating agreements to specify member rights and duties).

[204] Cf. U.C.C. § 8-503 (Property Interest of Entitlement Holder in Financial Asset Held by Securities Intermediary).

justice: dispute resolution could occur through predetermined arbitration mechanisms, offering meaningful recourse without costly litigation.[205]

However, the legal certainty provided by this structure would introduce operational burdens. Legal personhood for the issuing DAO would trigger regulatory obligations, including tax liabilities,[206] registered agent requirements, and potentially KYC/AML compliance (all precisely the institutional overhead many users seek to avoid).[207] The viability of this solution, therefore, would depend on calibration: introducing sufficient legal structure to provide meaningful protection without triggering the full regulatory apparatus that would eliminate the efficiency advantages of the decentralized model.

III. Regulatory Interventions and Comparative Analysis

While private ordering mechanisms offer promising pathways for risk mitigation, their adoption remains voluntary and, to date, largely theoretical. Consequently, the heavy lifting of consumer protection and systemic risk management has fallen to the state. As noted at the outset, both the European Union and the United States have recently advanced comprehensive frameworks (MiCAR and the GENIUS Act) designed to bring stablecoins within the regulatory perimeter. Yet, these interventions focus primarily on *centralized* issuers. Regulating *decentralized* stablecoins presents a fundamental paradox: the very features that engender private law vulnerability (the absence of issuers, autonomous operation, and pseudonymous governance) also blunt the effectiveness of traditional regulatory tools. In this Part III, we examine how these emerging legal regimes grapple with such hurdles. In doing so, we reveal a divergence in strategy that ranges from indirect exclusion to calculated ambiguity.

A. The "No Entity to Regulate" Problem

The regulatory challenges posed by decentralized stablecoins mirror the private law difficulties identified above. Namely, protocols like MakerDAO operate without legal personhood, leaving regulators with no entity to license, supervise, or sanction.[208] This creates a fundamental mismatch between traditional financial regulation (which is premised on identifiable institutions with management, physical offices, and traditional assets) and autonomous

[205] *See* 9 U.S.C. § 2 (enforcing arbitration agreements).

[206] *See* 26 U.S.C. § 7701(a)(3) (defining "corporation" for tax purposes to include associations).

[207] *See* 31 U.S.C. § 5312 (defining financial institutions subject to AML requirements).

[208] *See supra* Part I.B.1.

smart contracts executing on global, permissionless networks.[209] Although billions in value flow through the software itself, there is quite literally no one to regulate.[210]

Regulators confronting this void face three theoretical options, each problematic. They could first target software developers and maintainers themselves by imposing requirements on smart contract design or criminalizing non-compliant code deployment. And while it is true that developers are theoretically identifiable, recent U.S. enforcement actions against Tornado Cash developers and Uniswap Labs illustrate the practical and constitutional challenges of regulating the creation of computer code.[211] Issues abound relative to freedom of expression and innovation.[212]

Second, regulators could restrict users directly through mechanisms like holding limits, tax penalties, or outright prohibitions on interacting with decentralized protocols. This approach, while certainly enforceable against identified users, risks driving activity into more obscure channels or offshore jurisdictions, which could in turn potentially exacerbate rather than mitigate systemic risks.[213]

Third, and most practically, regulators could focus on the interfaces between decentralized protocols and traditional finance; namely, the exchanges, wallet providers, and other intermediaries that enable most users to access these systems.[214] By leveraging existing regulatory relationships with identifiable entities, governments can indirectly constrain the adoption of decentralized stablecoin without having to directly regulate autonomous code.[215] This strategy has been used before, as seen through the successful pressure campaign that led major exchanges to delist privacy-enhancing cryptocurrencies, thus demonstrating how intermediary regulation can effectively limit mainstream access to problematic protocols.[216]

---

[209] *See* Reyes, *supra* note 98, at 1875-76.

[210] Maker White Paper, *supra* note 52, at 1 (describing MakerDAO as "decentralized community").

[211] *United States v. Storm & Semenov*, No. 1:23-cr-00430 (S.D.N.Y. filed Aug. 23, 2023); *In re Universal Navigation Inc. d/b/a Uniswap Labs*, CFTC Docket No. 24-25 (Sept. 4, 2024).

[212] *See id.*

[213] *See* BANK FOR INT'L SETTLEMENTS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 18 (2023).

[214] *See infra* Part III.B.

[215] *See* 31 C.F.R. § 1010.100 (defining money service businesses). See also Christopher K. Odinet, *Consumer Bitcredit and Fintech Lending*, 69 ALA. L. REV. 781, 813 (2018) and Christopher K. Odinet, *Predatory Fintech and the Politics of Banking*, 106 IOWA L. REV. 1739, 1768 (2021) (both discussing the regulation of fintech intermediaries).

[216] *See, e.g.*, *Binance Delists Privacy Coins in European Markets*, BINANCE (June 2023) (removing Monero, Zcash due to regulatory pressure).

As explained in the subparts that follow, both MiCAR and the GENIUS Act ultimately adopt variations of this third approach, though they do so with markedly different implementations.

B. Transferring Risk to Market Intermediaries

MiCAR provides a prime example of regulatory strategy that is focused on intermediaries. Indeed, the law explicitly excludes protocols with "no identifiable issuer" from its core regulatory requirements, while at the same time imposing comprehensive obligations on crypto-asset service providers (CASPs) that offer such assets.[217] When CASPs list decentralized stablecoins, they must draft and publish white papers describing the asset's characteristics and risks, perform enhanced due diligence, and assume full liability for the accuracy of their representations.[218] These provisions effectively make CASPs quasi-issuers for assets they cannot control.[219]

This approach creates a calculated risk transfer. In essence, CASPs must decide whether listing decentralized stablecoins justifies potential liability for autonomous protocol failures.[220] The regulation's ingenuity lies in leveraging market incentives rather than imposing direct prohibitions. By making intermediaries potentially liable for protocol malfunctions, oracle failures, or governance attacks beyond their ability to control or even influence, MiCAR may achieve *de facto* exclusion of decentralized stablecoins from EU markets without explicitly banning them.[221]

MiCAR's application to stablecoins reveals particular tensions. The regulation defines "E-Money Tokens" (EMTs) as crypto-assets that maintain a stable value by referencing official currencies (which is a functional definition that clearly encompasses MakerDAO's DAI stablecoin).[222] Yet the rules for EMTs presuppose centralized issuers who obtain regulatory approval, grant direct redemption rights, and maintain segregated reserves.[223] To our mind, this creates an impossible compliance scenario: DAI functionally qualifies as an

---

[217] MiCAR, *supra* note 9, recital 22.

[218] *Id.* arts. 4(3), 6.

[219] *Id.*

[220] *See* Matthias Lehmann, *MiCAR- Gold Standard or Regulatory Poison for the Crypto Industry?* 4 (EBI Working Paper Series No. 160, 2024).

[221] *See* MiCAR & Unidentifiable Issuers of Crypto Assets, AXIS ADVISORY (Sept. 10, 2023).

[222] MiCAR, *supra* note 9, art. 3(1)(7).

[223] *Id.* arts. 48(1), 51.

EMT but structurally cannot satisfy EMT requirements.[224] The result is regulatory limbo. CASPs cannot list an asset that meets EMT definitions without EMT compliance, yet, at the same time, no entity exists to furnish such compliance.[225]

The GENIUS Act takes a fundamentally different approach through exclusion by definition.[226] By requiring "payment stablecoins" to have an identifiable "issuer" obligated to convert tokens at fixed rates, the Act categorically excludes protocols like MakerDAO from its regulatory perimeter.[227] The legislation reinforces this exclusion by explicitly carving out "distributed ledger protocols," "self-custodial software interfaces," and "liquidity pools" from the definition of "digital asset service provider."[228] Yet crucially, the Act remains silent on whether regulated service providers may list or facilitate trading in decentralized stablecoins that fall outside its definitions.[229]

The GENIUS Act's silence creates different uncertainties compared to MiCAR. While the Act doesn't prohibit service providers from offering decentralized stablecoins, neither does it provide safe harbors or pathways for compliance. This ambiguity leaves U.S. intermediaries in limbo (technically permitted to list DAI but potentially exposed to enforcement under other authorities or future regulatory clarification).[230] The Act's mandate for Treasury studies on "endogenously collateralized payment stablecoins" and DeFi applications suggests regulators recognize this gap but have deferred substantive decisions.[231]

Early market responses reflect the different risks created by these two laws. No major EU-based CASP has listed significant decentralized stablecoins under MiCAR, thereby suggesting the liability framework effectively excludes these assets.[232] Meanwhile, U.S. exchanges continue offering DAI and similar tokens and thus operating in the GENIUS Act's regulatory void while awaiting further guidance.[233] Both approaches use intermediaries as control points, but

---

[224] Compare *id.*, with Maker White Paper, *supra* note 52 (lacking issuer capable of compliance).

[225] *See* Lehmann, *supra* note 220 , at 4.

[226] GENIUS Act, *supra* note 10, § 2(22)(A)(ii).

[227] *Id.*

[228] *Id.* § 2(7)(B).

[229] *See id.* (lacking provisions addressing decentralized stablecoins).

[230] *See* 31 U.S.C. § 5312 (Bank Secrecy Act authorities).

[231] GENIUS Act, *supra* note 10, §§ 9(e)(1)(E), 14.

[232] Interim MiCAR Register - Other Crypto-Assets, ESMA (Dec. 2024).

[233] *See* Top Stablecoin Tokens by Market Capitalization, *supra* note 50 (showing DAI trading on U.S. exchanges).

MiCAR's active allocation of liability may prove more immediately effective than the GENIUS Act's ambiguity.

C. Functional vs. Structural Regulatory Requirements

We see the fundamental tension between MiCAR and the GENIUS Act as reflecting competing regulatory philosophies: specifically, whether the law address what stablecoins functionally do or how they are structurally organized.[234] This distinction is critical for decentralized stablecoins, which behave functionally like their centralized counterparts (both maintain dollar pegs, facilitate payments, serve as trading collateral, etc), while structurally they operate through autonomous protocols rather than corporate issuers.[235]

MiCAR adopts a primarily functional approach, defining E-Money Tokens by their economic purpose: maintaining stable value by referencing official currencies.[236] This definition captures DAI, which purports to maintain dollar parity through its stabilization mechanisms.[237] Yet MiCAR's regulatory requirements assume structural characteristics that decentralized protocols simply cannot possess: namely, issuers to seek authorization, management to supervise operations, reserves to segregate, and legal entities to sanction when things go wrong.[238] Thus, the regulation creates a category that functionally includes decentralized stablecoins while structurally excluding them from compliance, which is a contradiction that effectively bars these assets from regulated markets.[239]

On the other hand, the GENIUS Act inverts this approach through structural prerequisites.[240] By defining payment stablecoins as requiring an "issuer" with redemption obligations, the Act categorically excludes decentralized protocols regardless of their functional characteristics.[241] DAI may maintain stability with the dollar, facilitate billions in payments, and serve identical economic functions to USDC, yet it falls outside the regulatory scope simply because no entity issues or redeems it.[242] In our view, while this structural filter indeed provides clarity (in other words, protocols either have issuers or

---

[234] Cf. MiCAR, *supra* note 9, art. 3(1)(7) with GENIUS Act, *supra* note 10, § 2(22)(A)(ii).
[235] See *supra* Part I.A.
[236] MiCAR, *supra* note 9, art. 3(1)(7).
[237] Maker White Paper, *supra* note 52, at 8-9.
[238] MiCAR, *supra* note 9, arts. 48, 51.
[239] See *supra* Part III.B.
[240] GENIUS Act, *supra* note 10, § 2(22)(A)(ii).
[241] *Id.*
[242] Cf. Maker White Paper, *supra* note 52.

they don't), it potentially creates regulatory gaps where functionally similar products receive disparate treatment.[243]

These approaches produce opposite problems. MiCAR's functional definitions risk capturing technologies that cannot comply with its structural requirements, thereby creating compliance scenarios that are impossible and may indeed stifle innovation.[244] In turn, the GENIUS Act's structural boundaries risk regulatory arbitrage such that protocols deliberately adopt decentralized structures to escape oversight while performing identical economic functions.[245] Neither framework successfully reconciles the challenge that decentralized stablecoins present, which is the emergence of technologies deliberately designed to replicate financial functions but without financial institutions to orchestrate them.[246]

The solution to this problem may require abandoning binary categorizations altogether in favor of more graduated approaches that match regulatory intensity to actual risks, rather than merely mapping regulatory treatment to organizational forms.[247] As discussed below, both MiCAR and the GENUIS Act mandate future study, thus suggesting that lawmakers recognize these tensions but lack ready solutions.[248]

D. Future Regulatory Development and Study Mandates

Both laws acknowledge their incomplete treatment of decentralized stablecoins through explicit mandates for future study, which we see as signaling that current approaches represent provisional responses rather than final solutions.[249] MiCAR requires the European Commission to present comprehensive recommendations for decentralized finance regulation within forty-eight months, while the GENIUS Act mandates that the Treasury Department study the oddly phrased "endogenously collateralized payment stablecoins" and DeFi applications of service provider definitions.[250] These parallel deferrals reveal a shared recognition that decentralized protocols require

---

[243] *See* Christopher J. Waller, *Reflections on a Maturing Stablecoin Market*, BD. OF GOVERNORS OF THE FED. RESERVE SYS. (Feb. 12, 2025).

[244] *See* Lehmann, *supra* note 220, at 5-6.

[245] *See* FIN. STABILITY BD., REGULATION, SUPERVISION AND OVERSIGHT OF "GLOBAL STABLECOIN" ARRANGEMENTS 12 (2021).

[246] *See supra* Part I.B.1.

[247] *See* Gary Gensler, Chair, SEC, Statement on Financial Innovation (Dec. 3, 2024) (advocating technology-neutral, risk-based regulation).

[248] MiCAR, *supra* note 9, art. 146; GENIUS Act, *supra* note 10, § 14.

[249] MiCAR, *supra* note 9, art. 146; GENIUS Act, *supra* note 10, §§ 9(e)(1)(E), 14.

[250] *Id.*

fundamentally different regulatory tools than those developed for traditional financial institutions.[251]

From our vantage, the scope of each study mandate suggests regulators are grappling with threshold questions about whether and how to regulate autonomous code. The GENIUS Act's focus on "endogenously collateralized" tokens (assumedly those backed solely by other digital assets from the same originator) directly targets protocols like MakerDAO, since DAI is backed by crypto assets locked in vaults rather than external reserves.[252] Meanwhile, MiCAR's broader DeFi mandate encompasses not just stablecoins but also the entire ecosystem of decentralized exchanges, lending protocols, and yield aggregators that increasingly rely on stablecoins as assets for settlement.[253]

By establishing frameworks for centralized actors while studying decentralized alternatives, lawmakers have in essence created temporary safe harbors that may prove difficult to unwind.[254] As DAI and similar tokens continue circulating during periods of study, and thereby accumulating users and building infrastructure dependencies, regulators may face mounting pressure to give regulatory cover to existing protocols or else risk market disruption.[255] The longer studies extend, the more entrenched decentralized stablecoins become, which has the potential to constrain future regulatory options through simple path dependence.[256] On the other hand, delay may prove prudent given the technological and legal complexities involved. Regulation that is premature risks stifling beneficial innovation or driving development to less transparent jurisdictions.[257]

CONCLUSION

Our study of MakerDAO's legal architecture and the comparative analysis of regulatory responses that followed reveals that decentralized stablecoins operate in a comprehensive legal vacuum that neither private ordering nor current regulation adequately fills. The future studies mandated by both MiCAR and the GENIUS Act must confront fundamental questions: Can code itself be regulated without criminalizing software development? Should

---

[251] *See supra* Part III.A.

[252] GENIUS Act, *supra* note 10, § 14; Maker White Paper, *supra* note 52, at 7-9.

[253] MiCAR, *supra* note 9, art. 146; DUNE & ARTEMIS, *supra* note 1, at 12 (providing DeFi transaction volumes).

[254] *See* Clayton M. Christensen, THE INNOVATOR'S DILEMMA 98-99 (1997)

[255] *See supra* Introduction (noting over $10 billion in decentralized stablecoin market capitalization).

[256] *See* Oona A. Hathaway, *Path Dependence in the Law*, 86 IOWA L. REV. 601, 603-04 (2001).

[257] *See* FIN. STABILITY BD., *supra* note 245, at 3-4.

functional equivalence drive regulatory parity regardless of structure? How can consumer protection exist without identifiable protectors? Until regulators answer these questions, users of decentralized stablecoins remain in the legal void our analysis has identified: bearing risks that neither private law nor public regulation adequately addresses.