A Landscape on the Neutrality and Indipendence of Decentralized Autonomous Organizations (DAOs) from Government Influence: Insights from Multiple Case Studies

Francesco Santoro
Department of Mathematics, Computer Science and Physics, University of Udine, Udine, Italy

* Corresponding author. Email: francescosantoro76@gmail.com (F.S.)
Manuscript received January 30, 2025; accepted March 18, 2025; published June 23, 2025.
DOI: 10.18178/IJBTA. 2025.3.1.62-75

Abstract: The interaction between Decentralized Autonomous Organizations (DAOs) and regulatory frameworks has become a pivotal issue in the realm of blockchain and decentralized governance. DAOs, defined by distributed decision-making, smart contract-based rules, and operational autonomy, seek to minimize centralized control and external interference. However, high-profile cases reveal the significant challenges DAOs face in maintaining neutrality and independence under increasing regulatory scrutiny. This study conducts a multi-case analysis to explore how DAOs navigate legal and geopolitical pressures, highlighting both their structural strengths and vulnerabilities. For example, centralized entities faced direct targeting of leadership, while pseudonymous governance within DAOs complicated enforcement yet did not guarantee immunity, as shown in certain cases. Similarly, other cases exemplify how DAOs can maintain operational functionality amid sanctions but also exposes individual liabilities. The findings emphasize the need for legal frameworks tailored to DAOs' unique structures and capabilities, enabling them to balance autonomy with compliance. By examining the resilience of decentralized governance and its ethical and operational implications, this study provides insights into how DAOs can sustain neutrality and accountability in a regulated global environment.

Keywords: decentralized autonomous organizations, Decentralized Autonomous Organizations (DAOs), Neutrality and independence, Governmental influence, Blockchain governance

1. Introduction

The rise of Decentralized Autonomous Organizations (DAOs) represents a profound shift in governance, employing blockchain technology to support decentralized, transparent, and autonomous operations. DAOs rely on smart contracts to encode decision-making rules, removing centralized authority and distributing control among stakeholders who vote with tokens. This model promises greater efficiency, global inclusivity, and neutrality than traditional organizations. Yet as DAOs gain influence, they face complex regulatory landscapes designed for centralized entities, raising questions about sustaining autonomy under mounting scrutiny. At the core of the DAO model lies a tension between independence and compliance.

While decentralization extends beyond conventional jurisdictional boundaries, governments have shown they can still exert control—whether through targeting individual contributors, restricting financial intermediaries, or reinterpreting existing laws. High-profile cases illustrate the vulnerability of both centralized and decentralized structures. Huawei and Telegram, for instance, encountered severe disruptions when governments-imposed restrictions. Huawei's reliance on U.S.-based partners left it exposed to geopolitical pressures, while Telegram's centralized leadership structure led to the personal arrest of its founder. These examples highlight how external forces can compromise the independence of traditional organizations. DAOs, by contrast, distribute authority, making it harder for regulators to pinpoint targets. The Tornado Cash case shows how immutable smart contracts can maintain operations despite sanctions. However, individuals involved in DAOs remain subject to legal repercussions, as seen when contributors to Tornado Cash faced prosecution. Similarly, the Ooki DAO case underscored that decentralization alone does not ensure immunity; regulators classified it as an unincorporated association, potentially holding token holders liable. The recent Lido DAO ruling further complicates this landscape. In November 2024, a U.S. District Court classified Lido DAO as a general partnership under California law, treating token holders as co-owners with potential liability. Prominent venture capital firms involved in Lido DAO were deemed general partners, marking a crucial departure from the assumption that decentralization inherently shields participants from legal risk. This decision may deter DAO participation or push them to adopt formal legal structures, such as LLCs, for liability protection. While jurisdictions like Wyoming and the Marshall Islands have created DAO-friendly frameworks, their adoption remains uneven. The Lido DAO ruling highlights the broader tension between innovation and regulation. Although decentralization provides resilience against the vulnerabilities faced by traditional organizations, it is no cure-all. Involving venture capital firms in governance can blur the line between decentralization and centralized influence, potentially triggering conventional liability frameworks. As DAOs evolve, they must engage with regulators to ensure viability in shifting legal environments. This study analyzes key cases—Huawei's and Telegram's centralized vulnerabilities, Tornado Cash's operational resilience, Ooki DAO's participant liabilities, and the Lido DAO ruling—to explore how decentralization intersects with regulation and liability. By examining these examples, it offers insights into how DAOs might balance autonomy with compliance. While DAOs can redefine governance, their sustainability depends on harmonizing decentralized structures with evolving legal standards. Emerging DAO-friendly jurisdictions provide models for achieving this balance, but recent rulings suggest much work remains to resolve legal ambiguities and risks. Ultimately, this research sheds light on how DAOs can navigate the intersection of technology, law, and geopolitics, arguing that sustainable success depends on finding equilibrium between innovation and accountability.

2. The Huawei-Google Ban: Exposing the Fragility of Centralized Tech Models and Highlighting the DAO Alternative

The U.S. government's 2019 decision to add Huawei to the Department of Commerce's Entity List served as a stark reminder of how centralized corporate structures remain vulnerable to political pressures and regulatory interventions [1]. By effectively barring U.S. companies, including Google, from conducting business with Huawei, this move underscored that entities subjected to a singular national jurisdiction can be swiftly influenced—or even crippled—by government policy. Such circumstances illustrate that when commercial operations rely on traditional corporate hierarchies and close ties to individual governments, they risk being treated as extensions of state power. However, if Huawei had been structured as a Decentralized Autonomous Organization (DAO) with governance mechanisms detached from direct governmental control, it would have been significantly harder for the U.S. to accuse it of serving as an

instrument of Chinese influence. In other words, the credibility and autonomy afforded by a DAO could have mitigated these vulnerabilities and defused accusations stemming from geopolitical tensions. The Huawei-Google ban was justified on the basis of national security concerns, reflecting one of the more substantial escalations in the U.S.-China trade conflict [1]. This intervention not only disrupted Huawei's global operations but also rattled the international technology landscape, exposing the fragility of interdependent supply chains and partnerships in a world increasingly fragmented along geopolitical line [2]. As the world's second-largest smartphone manufacturer at the time, Huawei had relied heavily on Google's Android ecosystem—encompassing the operating system, app marketplace, and essential services—for its devices [3]. This interdependence allowed Huawei to dominate markets where affordability and versatility were key consumer priorities. Yet, the subsequent ban effectively cut Huawei off from Google's services, incapacitating its smartphone division in critical markets and forcing the firm to accelerate the development of HarmonyOS. While this pivot demonstrated Huawei's technological resilience, it also underscored the immense cost and complexity of rebuilding a complete ecosystem from the ground up in direct competition with entrenched market leaders like Google and Apple [4]. The U.S. actions against Huawei fit into a broader strategy aimed at curbing China's rising influence in global technology. As a leader in 5G, Huawei represented a focal point of China's ambitions to shape future telecommunications standards. U.S. officials expressed fears that Huawei's equipment could be leveraged for espionage by the Chinese government, a claim Huawei has consistently denied [2]. These suspicions prompted not only a U.S. ban but also attempts to convince allies to exclude Huawei from their 5G infrastructure. As a result, the tech landscape became further fragmented, compelling businesses to navigate conflicting regulatory terrains and geopolitical allegiances [1]. Crucially, the Huawei-Google scenario highlights the risks inherent in relying on centralized corporate models. Huawei's dependence on a few key partnerships, particularly with Google, made it acutely vulnerable to unilateral regulatory decisions [3]. In stark contrast, DAOs present a structural alternative precisely because their governance systems are decentralized and distributed among diverse stakeholders rather than concentrated in a single, easily targeted entity. DAOs leverage blockchain-based smart contracts to automate decision-making and management processes, minimizing reliance on national legal frameworks and traditional corporate hierarchies [5]. If Huawei had operated as a DAO—where governance tokens, community votes, and distributed consensus shaped strategic decisions—no single country's government could swiftly sever critical partnerships or impede its core services with one policy directive. Indeed, such an arrangement would have made it far more difficult to argue that the organization was merely an extension of any particular nation's political interests [6]. Nonetheless, embracing a DAO structure is not a panacea. While decentralization can provide a measure of autonomy from governmental intervention, DAOs remain exposed to broader regulatory and infrastructural dependencies. For instance, a DAO engaged in international trade may still need access to centralized payment systems, shipping networks, or cloud service providers—all of which can be subjected to government mandates [7]. Similarly, DAOs cannot fully escape legal scrutiny: jurisdictions enforcing strict regulations may target the developers, core contributors, or even users if they believe the DAO's activities circumvent national policies [6]. Thus, while a DAO's governance is detached from direct state control, its peripheral services may still be influenced by existing legal and economic frameworks. The Huawei-Google case also underscores the profound ripple effects that geopolitical tensions can have on innovation ecosystems. The ban pressured Huawei to seek new relationships with alternative suppliers and to invest heavily in proprietary technologies, such as its Kirin chipsets, to minimize dependence on U.S. components [4]. In doing so, it catalyzed unforeseen forms of innovation. A DAO-based model could diffuse the impact of such disruptions by distributing governance and operational responsibilities across a global network of participants. This diversity could reduce reliance on any single region, supplier, or regulatory environment,

thus providing a more neutral, resilient foundation for technological growth [5]. Additionally, the case illuminates the role of trust in global commerce. Huawei's reputation was severely strained by allegations of state espionage, regardless of their veracity [2]. This erosion of trust, coupled with the withdrawal of Google services, prompted many consumers and governments to reassess their engagement with Huawei's products. By contrast, DAOs may bolster trust through transparent governance and immutable blockchain records. Decisions, resource allocations, and strategic roadmaps can all be publicly audited, ensuring that no hidden agendas can easily shape outcomes behind closed doors. Such transparency might have mitigated the reputational damage Huawei faced, as international stakeholders could verify processes rather than relying solely on national narratives [6]. Still, transitioning entire industries—especially critical infrastructures like telecommunications—to a DAO framework remains challenging. Regulatory environments may attempt to rein in DAOs if they view them as circumventing security protocols or economic oversight [7]. Moreover, the cultural and technical leap from centralized corporations to decentralized collectives involves a steep learning curve for both industry players and policymakers. The technological maturity, legal acceptance, and operational norms necessary for DAOs to be fully effective in this context will require concerted effort and adaptation [5]. In essence, the Huawei-Google conflict serves as both a warning and a call to consider new organizational forms. It underscores how vulnerable centralized corporations are to geopolitical pressures and how important it is to anticipate external shocks. DAOs, with their decentralized governance and detached relationship to government control, offer a blueprint for building more resilient, trust-enhancing ecosystems that can operate across fragmented global landscapes without being easily co-opted by political interests. While they are no silver bullet, DAOs present a compelling alternative governance model capable of mitigating many of the vulnerabilities revealed by the Huawei-Google ban. By examining this case, we gain valuable insights into how a DAO-driven future might foster neutrality, innovative growth, and greater resistance to the shifting winds of international policy.

3. The Telegram Case: Lessons in Governance and the Role of Decentralization

The arrest of Telegram's co-founder and CEO, Pavel Durov, on August 24, 2024, at Le Bourget Airport in Paris marked a pivotal moment in the ongoing discourse on technology governance and platform responsibility. French authorities charged Durov with complicity in distributing child sexual exploitation material and drug trafficking, attributing these infractions to Telegram's inadequate content moderation systems [8]. This event underscores the inherent vulnerabilities of centralized platforms and raises critical questions about the efficacy of centralized leadership in managing platforms at a global scale. This paper explores how the adoption of Decentralized Autonomous Organizations could mitigate such risks, using Telegram's case as a focal point. By examining DAOs' governance structure, this discussion highlights the potential for decentralized systems to distribute accountability, reduce legal exposure, and increase resilience against enforcement actions. The paper also addresses the challenges of transitioning to decentralized models, including operational complexity, regulatory compliance, and achieving community consensus. Telegram, a centralized platform established in 2013, operates under the direct leadership of Pavel Durov, making the organization highly susceptible to regulatory actions targeting its executives. Durov's arrest exemplifies the concentration of accountability in centralized governance structures. With decision-making authority concentrated in a single individual, the legal vulnerabilities of platforms like Telegram are amplified [8]. Centralized governance inherently ties platform operations to the leadership's ability to comply with regulatory standards. In the case of Telegram, this governance model exposed its founder to direct enforcement measures for perceived lapses in content moderation, as French authorities cited these deficiencies as enabling criminal activities [9]. The implications of Durov's arrest extend beyond individual accountability, drawing attention to the systemic risks faced by centralized organizations. These

risks include regulatory scrutiny, potential market destabilization, and damage to the platform's reputation [10]. In contrast to centralized models, DAOs distribute decision-making authority across a decentralized network of participants, reducing the reliance on individual leaders. A DAO operates through smart contracts deployed on blockchain networks, enabling automated and transparent governance processes [11]. This model allows stakeholders to collectively make decisions, mitigating the legal and regulatory risks associated with centralized authority. Had Telegram adopted a DAO-like governance structure, the risks associated with centralized accountability could have been significantly mitigated. For example, a DAO could handle content moderation through decentralized mechanisms, such as community voting or automated systems powered by artificial intelligence. This approach would distribute responsibility across a network of pseudonymous participants, making it more challenging for regulatory authorities to target specific individuals for enforcement actions [11]. A decentralized content moderation system could incorporate stakeholder-driven proposals to address regulatory concerns. By leveraging blockchain technology, these systems could enforce compliance through pre-programmed rules while maintaining the platform's neutrality. The legal risks faced by Telegram, including Durov's arrest, might have been reduced under such a governance framework. The decentralized nature of DAOs disperses control and liability, ensuring that no single entity or individual bears disproportionate responsibility for operational shortcomings. While DAOs present an attractive alternative for mitigating centralized vulnerabilities, transitioning to such a model involves significant challenges. Establishing consensus among a diverse network of participants is complex, particularly when addressing sensitive issues like content moderation. Additionally, DAOs face operational hurdles, such as designing effective governance structures that balance transparency, efficiency, and compliance [11]. Regulatory compliance is another critical issue for DAOs. Despite their decentralized nature, DAOs remain subject to some extent to legal frameworks, as demonstrated by cases like Ooki DAO, where regulators pursued actions against participants for non-compliance with financial laws. Ensuring that decentralized governance mechanisms align with international legal standards is essential to avoid similar outcomes [11]. Following Durov's arrest, the broader Telegram ecosystem began exploring decentralized governance models. In November 2024, the TON Foundation, associated with Telegram, launched the Society DAO to introduce decentralization into its operational framework [10]. This initiative reflects a growing recognition of the advantages of decentralization in reducing regulatory risks and increasing resilience. The DAO's governance model aims to distribute decision-making authority among stakeholders, empowering the community to participate in operational decisions. This approach minimizes the concentration of accountability while enhancing platform resilience against legal challenges. However, the success of such initiatives depends on the ability to balance decentralization with effective governance, ensuring that the platform remains functional, compliant, and secure. The case of Telegram underscores the limitations of centralized governance in managing global platforms. It highlights the potential of decentralized models, such as DAOs, to address these limitations by distributing accountability and reducing legal exposure. However, implementing decentralized governance requires careful planning to navigate the complexities of operational management and regulatory compliance. As technology platforms continue to evolve, the tension between centralized control and decentralized governance will remain a critical issue. The lessons learned from Telegram's experience offer valuable insights into the potential benefits and challenges of adopting decentralized systems. DAOs represent a forward-looking approach to governance, providing a framework for balancing operational resilience, regulatory compliance, and user autonomy. Pavel Durov's arrest serves as a cautionary tale about the vulnerabilities of centralized governance in the face of regulatory scrutiny. It underscores the need for alternative governance models, such as DAOs, which distribute authority and accountability across a decentralized network [10]. While DAOs offer significant advantages in mitigating

legal risks, their implementation requires thoughtful design and alignment with legal standards. For Telegram, adopting a DAO governance model could provide a path to greater resilience and compliance while preserving platform neutrality. As the digital landscape evolves, the balance between centralization and decentralization will define the future of technology governance. Telegram's exploration of decentralized solutions through the Society DAO represents a step in this direction, offering a potential blueprint for navigating the challenges of governance in the digital age.

4. Ooki DAO: Redefining Liability and Legal Boundaries in Decentralized Governance

The legal complexities surrounding Decentralized Autonomous Organizations have become a focal point in the evolving governance of blockchain-based entities. A particularly impactful case in this context is Commodity Futures Trading Commission (CFTC) v. Ooki DAO, which examined how decentralized governance intersects with traditional regulatory structures. In 2022 the CFTC charged Ooki DAO, the successor to bZeroX, LLC, with offering leveraged and margined retail commodity transactions without proper registration—actions typically reserved for licensed Futures Commission Merchants (FCMs) [12]. By framing Ooki DAO as an unincorporated association, the CFTC extended liability to its governance token holders, arguing that their participation in voting on DAO proposals constituted involvement in operational decision-making [13]. This stance introduced a significant precedent for DAO participants, highlighting the legal risks of even minimal engagement in decentralized governance. The court's ruling in favor of the CFTC marked a pivotal moment, holding Ooki DAO liable for violating U.S. financial regulations and imposing a penalty of $643,542. Additionally, the court mandated the cessation of the DAO's trading activities and the shutdown of its website to prevent further violations [14]. Beyond financial penalties, the court's decision introduced an innovative legal mechanism for serving notice to decentralized organizations. By utilizing Ooki DAO's online forums and chat platforms to communicate legal proceedings, the case demonstrated how traditional legal frameworks are adapting to the decentralized, pseudonymous nature of blockchain governance structures [15]. This approach represents a shift in regulatory tactics, reflecting a broader effort to hold DAOs accountable despite their structural resistance to centralized oversight. Critics have raised concerns about the broader ramifications of this precedent. By treating DAOs as unincorporated associations, courts potentially expose all participants to joint liability, a move that could discourage innovation and deter engagement in decentralized projects. For example, CFTC Commissioner Summer K. Mersinger criticized the decision, arguing that it could stifle participation in Web3 governance models and create unnecessary barriers to innovation in the Decentralized Finance (DeFi) ecosystem [16]. This risk is particularly pronounced in jurisdictions like the United States, where broad interpretations of partnership laws make it possible to assign liability to passive participants. Such interpretations could lead to a chilling effect on DAO activity, as developers, token holders, and investors weigh the risks of potential legal repercussions [17]. The Ooki DAO case also underscores the importance of legal incorporation for DAOs to mitigate liability risks. Jurisdictions like Wyoming and the Marshall Islands have taken proactive steps to provide DAOs with formal legal status. In Wyoming, DAOs can register as Limited Liability Companies (LLCs) under the Wyoming DAO Supplement, which limits participant liability and offers a clear governance structure. Similarly, the Marshall Islands has introduced legislation allowing DAOs to register as legal entities, ensuring compliance with international legal standards while preserving their decentralized nature [18]. These frameworks provide a model for other jurisdictions to follow, enabling DAOs to operate within regulatory boundaries without compromising their innovative potential. Despite the significant regulatory implications, the Ooki DAO case has spurred broader discussions about the future of decentralized governance. Proponents of regulation argue that establishing clear legal frameworks can foster a stable and secure environment for DAOs, encouraging innovation while protecting participants and investors. For

example, incorporating DAOs as recognized legal entities not only shields participants from unexpected liabilities but also enhances trust and legitimacy within the blockchain ecosystem. Conversely, critics contend that over-regulation risks stifling the innovative potential of blockchain technology, which thrives on the principles of autonomy and decentralization. They emphasize the need for nuanced regulatory approaches that balance the autonomy of DAOs with the requirements of financial compliance [14]. The implications of the Ooki DAO case extend beyond the immediate legal context, influencing the broader regulatory landscape for DAOs and DeFi [19]. The case illustrates the challenges of aligning decentralized innovations with existing legal norms, particularly when governance structures are dispersed across global participants. Without clear legal standards, DAOs risk operating in a gray area where accountability and liability remain ambiguous, leaving participants exposed to regulatory penalties and litigation. However, the case also highlights the potential for DAOs to navigate these challenges through proactive engagement with regulators and by adopting governance models that align with established legal frameworks [16]. Moreover, the Ooki DAO ruling serves as a cautionary tale for other DAOs, emphasizing the necessity of robust governance mechanisms and legal compliance. Cases like this have prompted some DAOs to explore incorporating as legal entities in blockchain-friendly jurisdictions, such as Switzerland and Singapore, which offer regulatory clarity and support for decentralized initiatives. By adopting these measures, DAOs can strike a balance between innovation and accountability, paving the way for sustainable growth in the blockchain sector. In the long term, the Ooki DAO case may serve as a catalyst for the development of global standards for DAO governance, ensuring that decentralized organizations can operate effectively while adhering to legal and regulatory norms [7 , 18]. In conclusion, the Ooki DAO case represents a critical juncture in the evolution of decentralized governance. It underscores the importance of aligning DAO operations with existing legal frameworks to mitigate risks for participants and foster a stable regulatory environment. As the blockchain ecosystem continues to expand, the lessons learned from this case will likely shape the future of DAO governance, offering insights into how decentralized organizations can navigate the complex intersection of innovation, regulation, and accountability.

5. Tornado Cash: Decentralized Privacy Under Regulatory Scrutiny

Cryptocurrency mixers such as Tornado Cash are pivotal in the discussion of blockchain privacy and regulation. Tornado Cash operates by enabling users to obfuscate the origin and destination of their cryptocurrency transactions, thereby achieving a level of anonymity that is otherwise unattainable on transparent blockchain networks like Ethereum. By pooling user deposits and allowing withdrawals to unrelated addresses, it eliminates transactional links, preserving privacy for users concerned about surveillance, profiling, or financial crime risks. However, these same features have rendered Tornado Cash an attractive tool for illicit activities, including money laundering, ransomware payments, and the financing of terrorism. This dual functionality has made Tornado Cash a centerpiece in debates over the balance between privacy rights and the need for regulatory compliance [20]. The legal and regulatory challenges surrounding Tornado Cash reached a peak on August 8, 2022, when the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned the platform under Executive Order 13694. The platform was accused of facilitating the laundering of over $7 billion in virtual currency, with connections to funds stolen by the North Korean Lazarus Group in multiple high-profile cyberattacks. What distinguished these sanctions was their unprecedented targeting of a decentralized protocol—a set of immutable smart contracts deployed on the Ethereum blockchain—rather than a centralized entity. Tornado Cash's design, intended to be censorship-resistant, posed significant obstacles for regulators aiming to restrict its use. Even with the sanctions, the platform remained operational, illustrating the robustness and independence of decentralized blockchain infrastructures [6, 27]. The sanctions had immediate and far-reaching

consequences for Tornado Cash and its ecosystem. The platform's governance token, TORN, saw its market capitalization plummet by 60% within days of the announcement, reflecting investor skepticism about its future viability. User activity also dropped sharply, with transaction volumes falling by over 70%, and the diversity of user addresses engaging with Tornado Cash significantly diminished. This decline posed challenges to the platform's core functionality, as the privacy Tornado Cash offers depends on the size and diversity of its anonymity pools. Smaller transaction pools, especially in high-value categories like the 100 ETH pool, experienced reduced effectiveness in maintaining privacy guarantees [20].

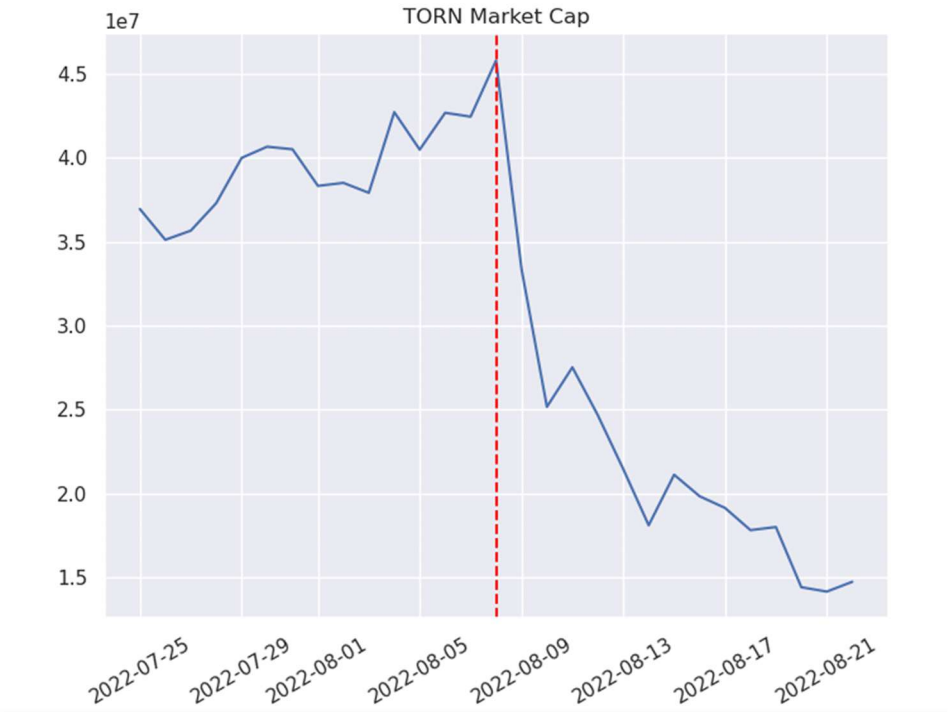

Fig. 1. Value of TORN tokens around sanction announcement.

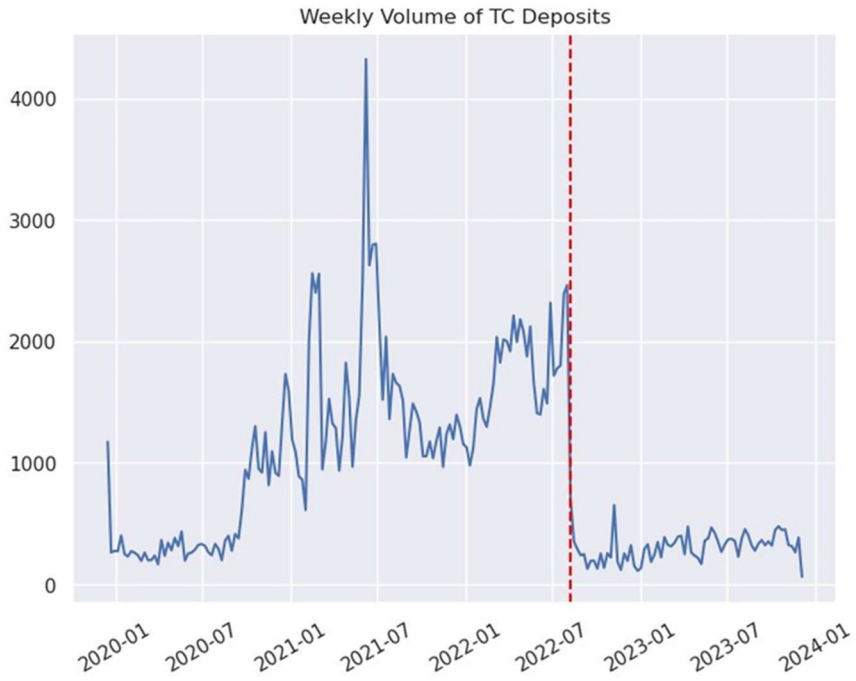

Fig. 2. Weekly deposit volume around sanction announcement.

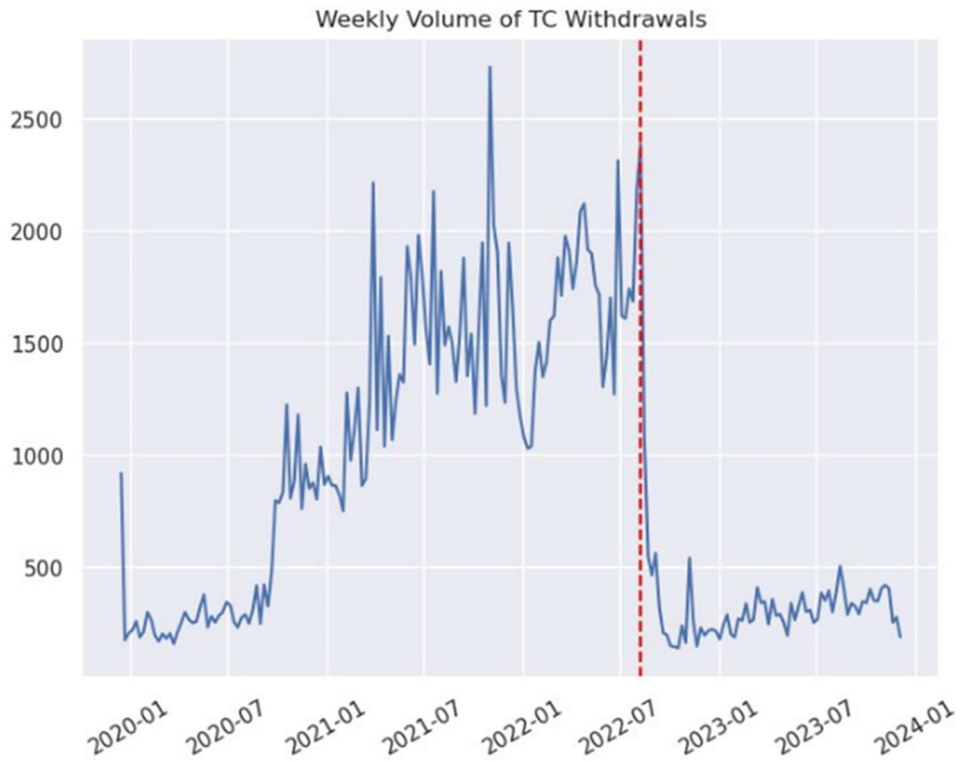

Fig. 3. Weekly withdrawal volume around sanction announcement.

Legal repercussions extended to Tornado Cash's developers, highlighting the risks faced by contributors to decentralized projects. Alexey Pertsev, one of the platform's creators, was arrested in the Netherlands and sentenced to 64 months in prison in 2024 for his role in facilitating money laundering. Similarly, Roman Storm and Roman Semenov, developers associated with Tornado Cash, faced legal scrutiny in the United States [21]. These actions underscored a critical tension in the regulation of decentralized platforms: while developers often have no direct control over how their code is used, they are increasingly being held accountable for its misuse. These cases revealed a broader regulatory strategy targeting individuals in addition to the technology itself, raising concerns within the blockchain community about the legal liabilities of open-source development [22]. Despite these challenges, Tornado Cash demonstrated significant resilience, a testament to its decentralized nature. By mid-2023, transaction volumes began recovering, particularly in smaller-value pools, where anonymity guarantees could still be maintained. This rebound suggested that Tornado Cash continued to fulfill its role as a privacy tool for certain user segments. However, the sanctions also revealed vulnerabilities in Ethereum's broader ecosystem. Validators and block builders on the Ethereum network played a critical role in processing Tornado Cash transactions. Over time, the processing of these transactions became increasingly concentrated among a few non-compliant builders, such as Titan Builder, exposing fragilities in Ethereum's censorship resistance and decentralization. While some builders actively excluded Tornado Cash transactions to comply with sanctions, others continued processing them, creating a dependence on a narrow group of actors to maintain Tornado Cash's functionality [20]. The case of Tornado Cash serves as a natural experiment in assessing the effectiveness of regulatory interventions in decentralized systems. While the sanctions temporarily disrupted its operations and diminished its user base, they did not succeed in entirely neutralizing the platform. Tornado Cash remained operational, highlighting the limitations of traditional regulatory frameworks in addressing the challenges posed by autonomous, immutable code. At the same time, the sanctions drew attention to the ethical responsibilities of the blockchain community in

maintaining tools that can be misused. As regulators, developers, and users grapple with these complexities, the Tornado Cash case provides critical lessons for the future of decentralized finance, emphasizing the need for nuanced approaches to balance privacy, security, and compliance [6, 27].

6. The Lido DAO Case: Legal Precedents and Decentralized Governance Challenges

The legal complexities surrounding Decentralized Autonomous Organizations took a pivotal turn with a recent ruling in the U.S. District Court for the Northern District of California. On November 18, 2024, Judge Vince Chhabria classified Lido DAO as a general partnership under California law, setting a precedent with far-reaching implications for DAO participants and the broader Decentralized Finance (DeFi) ecosystem. This decision underscores the ongoing tension between innovative decentralized structures and traditional legal frameworks, particularly concerning liability and regulatory compliance [23]. The case emerged from a class-action lawsuit filed by Andrew Samuels, an investor in Lido DAO's native token (LDO), who alleged that the tokens were unregistered securities. Samuels contended that Lido DAO should have registered these tokens with the U.S. Securities and Exchange Commission (SEC) and sought damages for financial losses incurred due to the token's declining value [22]. The court ruled that Lido DAO's governance model, characterized by token holders collectively making decisions and earning staking rewards, aligns with California's definition of a general partnership: "the association of two or more persons to carry on as co-owners a business for profit" [24]. As a result, all participants, including venture capital firms such as Paradigm Operations, Andreessen Horowitz, and Dragonfly Digital Management, were deemed general partners, exposing them to potential personal liability for the DAO's actions [25]. These ruling challenges the foundational assumption that DAOs, as decentralized entities, inherently shield participants from legal and financial liability. While DAOs operate without centralized leadership and rely on blockchain technology for governance, this decision highlights that decentralization alone does not exempt participants from traditional legal definitions and responsibilities. The classification of Lido DAO as a general partnership raises concerns for token holders, particularly institutional investors, as they may face liabilities disproportionate to their level of involvement in governance activities. For instance, active participation in voting or contributing to operational decisions could now be construed as sufficient to incur liability, as seen in other high-profile DAO cases like Ooki DAO [26]. The broader implications of this decision extend beyond Lido DAO, posing significant risks to the DeFi sector. Venture capital firms and individual token holders must now consider the possibility that their involvement in DAOs could expose them to personal liability, even without explicit intent to form a legal partnership. This may discourage institutional and retail participation in DAO governance, stifling innovation within the space. Furthermore, the ruling underscores the need for DAOs to adopt formal legal structures, such as Limited Liability Companies (LLCs) or other entity types, to protect their participants. Jurisdictions like Wyoming and the Marshall Islands, which provide legal recognition for DAOs, offer frameworks that mitigate such risks while preserving the decentralized ethos of these organizations [22]. From a regulatory perspective, the Lido DAO case highlights the complexities of applying existing legal frameworks to decentralized structures. Judge Chhabria's ruling builds on prior cases, such as the CFTC v. Ooki DAO decision, where the participation of token holders in governance was deemed sufficient to establish liability under partnership laws. These cases collectively signal an evolving regulatory landscape in which governments seek to hold DAOs accountable, irrespective of their decentralized nature. The ruling also reinforces the role of regulators in addressing ambiguities within the legal status of DAOs, emphasizing the need for tailored frameworks that balance innovation with accountability [24]. Notably, the ruling raises ethical and practical considerations for DAOs. Decentralized governance models were originally conceived as an alternative to centralized organizations, promising autonomy, transparency, and shared decision-making. However, as DAOs face increasing regulatory scrutiny,

they must reassess how to maintain these principles while addressing liability concerns. The involvement of prominent venture capital firms in Lido DAO's governance also calls into question the true extent of decentralization within certain DAOs, as these entities often hold disproportionate influence over decisions. This dynamic may inadvertently weaken the DAO's claims of operating as a fully decentralized entity, further complicating its legal status and liability exposure [25]. The Lido DAO ruling underscores a critical juncture in the evolution of decentralized governance. While the decision highlights vulnerabilities in current DAO frameworks, it also presents an opportunity for the ecosystem to evolve. Legal experts suggest that DAOs can mitigate these risks by adopting formalized structures that balance decentralization with legal protections, such as DAO-specific legal entities. Additionally, this case calls on regulators to develop coherent guidelines that account for the unique characteristics of DAOs, ensuring a level playing field for decentralized and traditional organizations alike [26]. By exposing the vulnerabilities inherent in decentralized governance, the Lido DAO case challenges the DeFi sector to confront the realities of regulatory compliance and liability. It not only reaffirms the need for clarity in DAO legal frameworks but also emphasizes the importance of engaging with regulators proactively. Achieving a sustainable balance between decentralization and accountability is essential for DAOs to realize their potential as innovative governance models in a highly regulated global landscape.

7. Conclusion

The rise of Decentralized Autonomous Organizations heralds a transformative era in governance, characterised by distributed decision-making, operational autonomy, and the ability to function independently of traditional institutional frameworks. This study has explored through several key cases the tensions DAOs face as they navigate an increasingly regulated global environment, demonstrating their potential to act as neutral entities even under intense governmental pressures. Through the analysis of key cases such as Tornado Cash, Ooki DAO, and their comparisons with centralized organisations like Huawei and Telegram, this research underscores both the promise and the vulnerabilities inherent to decentralized governance. Central to DAOs' resilience is their decentralised architecture, which allows them to distribute authority across a network of stakeholders. This structural advantage enables DAOs to bypass many of the vulnerabilities associated with centralised organisations. For example, Tornado Cash maintained operational functionality despite facing significant sanctions, illustrating how decentralisation can offer a measure of insulation from external interference. However, the sanctions also revealed a critical trade-off: while the DAO's code proved resilient, the individuals behind it—developers, contributors, and token holders—became focal points for enforcement actions. This duality underscores a recurring theme in the evolution of DAOs: while decentralisation can mitigate systemic vulnerabilities, it cannot wholly shield individuals from the realities of regulatory scrutiny. The experiences of centralised entities like Huawei and Telegram provide a stark contrast. Huawei's reliance on its partnership with Google made it acutely vulnerable to geopolitical actions, as evidenced by the U.S. government's severance of critical business ties. Similarly, Telegram's centralised leadership exposed its executives to direct legal actions, culminating in the arrest of its founder, Pavel Durov. These cases highlight the inherent fragility of centralised systems when navigating conflicting regulatory and political landscapes. DAOs, by distributing decision-making authority and operational control, represent an alternative model that fundamentally disrupts the concentration of risk. However, the Ooki DAO and Lido DAO cases demonstrate that even decentralised governance structures are not immune to evolving regulatory tactics, as the participation of token holders in governance was interpreted as grounds for legal liability. One of the key insights of this research is the necessity for DAOs to proactively engage with legal and regulatory frameworks rather than positioning themselves as inherently outside their reach. The emergence of DAO-friendly jurisdictions such as Wyoming

and the Marshall Islands offers valuable lessons. These jurisdictions have created legal frameworks that provide DAOs with formal incorporation options, such as Limited Liability Company (LLC) status, which limits liability for participants while preserving operational legitimacy. Such proactive measures allow DAOs to maintain their decentralised ethos while addressing accountability and compliance requirements. However, these frameworks must be carefully tailored to ensure they do not inadvertently undermine the decentralisation that is central to the DAO model. Ethical considerations also loom large in this discourse. The Tornado Cash case, for example, raises questions about the balance between privacy and accountability. While Tornado Cash provided an invaluable tool for user anonymity, it also became a vehicle for illicit activities, such as money laundering and ransomware payments. This dual-use challenge underscores the need for DAOs to integrate ethical oversight into their governance models. Community-driven governance, powered by transparent mechanisms and decentralised consensus, can play a critical role in addressing these ethical challenges while ensuring compliance with societal and legal norms. As DAOs continue to mature, their sustainability and scalability will depend on their ability to balance the competing demands of autonomy, compliance, and innovation. This requires a multi-faceted approach: legal clarity must be paired with technological advancements that strengthen governance structures. Innovations such as automated compliance mechanisms, smart contracts for pseudonymous accountability, and AI-driven decision-making systems can enhance DAOs' capacity to navigate complex regulatory landscapes. At the same time, DAOs must remain adaptive, evolving their governance structures to address emerging challenges without compromising their core principles of decentralisation and operational neutrality. The findings of this study reveal that while DAOs possess significant potential to redefine governance, their success is contingent on their capacity to harmonise decentralisation with regulatory and ethical considerations. The long-term viability of DAOs requires a deep commitment to engaging with global regulatory systems and fostering trust among participants and stakeholders. This engagement is not simply a defensive measure but a strategic opportunity to shape the future of decentralised governance. By proactively addressing regulatory ambiguities and ethical dilemmas, DAOs can position themselves as models of transparency, resilience, and innovation. Looking forward, the lessons from Tornado Cash, Ooki DAO, and other cases analysed in this study highlight a clear pathway for DAOs to thrive. First, they must leverage their decentralised architecture to foster inclusivity and reduce vulnerabilities associated with traditional governance models. Second, they must adopt proactive approaches to compliance, working collaboratively with regulators and policymakers to establish clear and sustainable operational standards. Finally, DAOs must continually refine their governance mechanisms to address ethical and legal challenges, ensuring their contributions to society are both innovative and accountable. In conclusion, DAOs represent a new frontier in organisational governance, offering a blueprint for entities that prioritise neutrality, resilience, and inclusivity. However, realising this potential requires a delicate balancing act: the need to remain true to the principles of decentralisation while addressing the demands of an increasingly interconnected and regulated global landscape. As this study demonstrates, the path forward for DAOs is not without challenges, but the opportunities they offer are transformative. By addressing these challenges with foresight and adaptability, DAOs can establish themselves as sustainable, ethical, and innovative governance models, paving the way for a future where decentralisation is not just an ideal but a practical reality in global systems of governance.

Conflict of Interest

The author declares no conflict of interest.

Acknowledgment

I would like to thank Prof. Massimo Franceschet for his guidance and support throughout the development of this work.

References

[1] Amadeo, R. (2019, May 20). Google reportedly ends business with Huawei, will cut it off from play store. [Online]. Available: https://www.arstechnica.com/gadgets/2019/05/google-reportedly-ends-business-with-huawei-will-cut-it-off-from-play-store/

[2] L. Kuo and S. Siddiqui. (2019, May 16). Huawei hits back over Trump's national emergency on telecoms 'threat.'* The Guardian. [Online]. Available: https://www.theguardian.com/us-news/2019/may/15/donald-trump-national-emergency-telecoms-threats-huawei

[3] The Verge. (2019, May 20). Huawei responds to Android ban with service and security guarantees, but its future is unclear. [Online]. Available: https://www.theverge.com/2019/5/20/18632234/huawei-android-ban-response-google-security-updates

[4] A. Satariano, R. Zhong, and D. Wakabayashi. (2019, May 20). U.S. tech suppliers, including Google, restrict dealings with Huawei after Trump order. [Online]. Available: https://www.nytimes.com/2019/05/20/technology/google-android-huawei.html

[5] Stanford Journal of Blockchain Law and Policy. (2021, June 30). The rise of Decentralized Autonomous Organizations: Opportunities and Challenges. [Online]. Available: https://stanford-jblp.pubpub.org/pub/rise-of-daos

[6] MIT Computational Law Report. (2023). Aligning decentralized autonomous organization' to precedents in cybernetics. [Online]. Available: https://law.mit.edu/pub/dao-precedents-cybernetics

[7] Reuters. (2024, June 10). Digital assets and DAOs: New theories of liability. [Online]. Available: https://www.reuters.com/legal/legalindustry/digital-assets-daos-new-theories-liability-2024-06-10

[8] Wikipedia. (2024). Arrest and indictment of Pavel Durov. [Online]. Available: https://en.wikipedia.org/wiki/Arrest_and_indictment_of_Pavel_Durov

[9] Everything we know about the arrest of Telegram's founder. (2024). [Online]. Available: https://nymag.com/intelligencer/article/why-was-telegram-ceo-pavel-durov-arrested-in-france.html

[10] Financial Times. (2024). Telegram finances propped up by crypto gains as founder fights charges. [Online]. Available: https://www.ft.com/content/a48acdae-6a6c-4073-894f-89ef5cf8b185

[11] The tale of telegram governance: When the rule of thumb fails. (2020). [Online]. Available: https://law.yale.edu/sites/default/files/area/center/justice/document/telegram-governance-publish.pdf

[12] Commodity Futures Trading Commission (CFTC). (2022). CFTC imposes $250,000 penalty against bZeroX, LLC and its founders and charges successor Ooki DAO for offering illegal, off-exchange digital-asset trading, registration violations, and failing to comply with the bank secrecy act. [Online]. Available: https://www.cftc.gov

[13] CoinDesk. (2023). CFTC wins lawsuit against crypto derivatives operator Ooki DAO. [Online]. Available: https://www.coindesk.com

[14] Cointelegraph. (2023). Ooki DAO to shut down after 'precedent-setting' court battle with CFTC. [Online]. Available: https://cointelegraph.com

[15] Blockchain legal resource. (2023). CFTC wins default judgment against Ooki DAO. [Online]. Available: https://www.blockchainlegalresource.com

[16] A. Drylewski, S. D. Levi, and D. Michael. (2024). Digital assets and DAOs: New theories of liability. [Online]. Available: https://www.reuters.com/legal/legalindustry/digital-assets-daos-new-theories-liability-2024-06-10

[17] R. Gonzalez, "The impact of DAOs on corporate law: An analysis of DAO frameworks and potential legal implications," 2023.

[18] M. Cartwright, "Internationalising state power through the internet: Google, Huawei and geopolitical struggle," *Internet Policy Review*, vol. 9, no. 3, pp. 1–18, 2020.

[19] Blockworks. (2023). Ooki DAO loses to CFTC after refusal to contest case. [Online]. Available: https://www.blockworks.co

[20] A. Brownworth *et al.* (2024). Regulating decentralized systems: Evidence from sanctions on Tornado Cash [Online]. Available: https://doi.org/10.59576/sr.1112

[21] Cryptonews.net. (2024). Tornado Cash developer Alexey Pertsev found guilty of money laundering. [Online]. Available: https://cryptonews.net/news/legal/2002024

[22] BeInCrypto. (2024, November 19). Lido DAO members exposed to liability, california court rules. [Online]. Available: https://www.beincrypto.com/lido-dao-governance-under-fire/

[23] Cointelegraph. (2024, November 18). California judge rules DAO members liable under partnership laws. [Online]. Available: https://cointelegraph.com/news/california-judge-rules-dao-members-liable-under-partnership-laws
[24] Decrypt. (2024, November 18). California court rules Lido DAO members can be held liable under partnership laws. [Online]. Available: https://decrypt.co/292275/california-court-rules-lido-dao-members-can-be-held-liable-under-partnership-laws
[25] Reuters. (2024, December 2). In blow to crypto collectives, judge rules venture backers must face claims. [Online]. Available: https://www.reuters.com/legal/government/column-blow-crypto-collectives-judge-rules-venture-backers-must-face-claims-2024-12-02/
[26] CryptoSlate. (2024, November 19). US court rules DAOs can face legal liability under partnership law. [Online]. Available: https://cryptoslate.com/us-court-rules-daos-can-face-legal-liability-under-partnership-law
[27] BankInfoSecurity. (2024). Tornado cash developer sentenced to 5 years in prison. [Online]. Available: https://www.bankinfosecurity.com/tornado-cash-developer-sentenced-to-5-years-in-prison-a-22427
[28] United States Department of the Treasury. (2022). Treasury sanctions notorious virtual currency mixer Tornado Cash. [Online]. Available: https://home.treasury.gov/news/press-releases/jy0983