International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2025 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Digital Directors, Real Risks: Unpacking Vicarious Liability in Virtual Corporations

Laksh Gera[a] Ananya Rai[b]

[a]Institute of Law, Nirma University, Ahmedabad, India [b]Institute of Law, Nirma University, Ahmedabad, India

Received 05 November 2025; Accepted 05 December 2025; Published 09 December 2025

The rapid rise of digital-first enterprises, including Decentralised Autonomous Organisations (DAOs), smart contracts, and algorithm-driven governance, has fundamentally disrupted traditional notions of corporate accountability. This article critically examines the doctrine of vicarious liability under the Companies Act 2013 in light of these technological transformations. It analyses whether established concepts such as "officers in default," shadow directors, and corporate criminal liability can be meaningfully extended to virtual corporations where decision-making is decentralised, automated, or anonymous. The paper explores the potential liability of developers, token holders, and blockchain platforms, drawing parallels with emerging international jurisprudence and regulatory trends. It further highlights the challenges faced by courts in attributing intent, control, and responsibility in code-driven environments. The study argues that without doctrinal adaptation and legislative clarity, virtual corporate forms risk becoming liability-free zones, undermining the very purpose of vicarious liability. Ultimately, the article advocates a purposive reinterpretation of company law to balance innovation with accountability in the evolving digital economy.

Keywords: *digital directors, vicarious liability, company, criminal liablity.*

INTRODUCTION: SETTING THE DIGITAL STAGE

In an era where emails are drafted by artificial intelligence, contracts are executed through automated code, and virtual avatars can represent individuals in corporate meetings, it is fair to pause and ask a fundamental question: Who is really accountable? As businesses increasingly rely on digital systems and algorithmic decision-making, traditional notions of corporate responsibility are being quietly, but significantly, challenged. The issue is no longer limited to identifying wrongdoing, but rather to determining whether responsibility can be meaningfully attributed at all.

Under the Companies Act 2013[1], the principle of vicarious liability has long provided courts with a framework to hold companies accountable for the acts of their directors, managers, and other key personnel. This structure assumes a clear chain of command and identifiable human actors. However, with the rise of Decentralised Autonomous Organisations (DAOs), AI-driven operations, and token-based governance models, that clarity is steadily eroding. Decision-making is increasingly decentralised, automated, and in many cases carried out by anonymous participants rather than identifiable corporate officers.

This paper seeks to explore how the doctrine of vicarious liability fits into this rapidly evolving digital landscape. It traces the development of the doctrine under Indian company law and examines whether existing legal principles can be extended to regulate modern, technology-driven business entities. In doing so, it highlights the growing complexity faced by courts when confronted with the question of whether legal responsibility can be attributed to autonomous systems or lines of code.

VICARIOUS LIABILITY: THE CLASSICAL VERSION

In simple terms, vicarious liability refers to the legal principle under which one person may be held responsible for the wrongful acts of another. In the context of company law, this generally means that a company can be made liable for the actions of its employees or agents, so long as those actions were carried out in the course of their employment. The rationale behind this

[1] Companies Act 2013

principle is straightforward: when a company benefits from the acts performed on its behalf, it should also bear the consequences if those acts result in legal wrongdoing.

- Section 2(60) of the Act defines 'officers who are in default' to include directors, key managerial personnel, and even those individuals in accordance with whose directions or instructions the Board is accustomed to act.[2]
- Provisions such as Sections 66 and 447 make it clear that liability for fraudulent conduct may arise even where a person has not directly carried out the wrongful act themselves.[3]
- The concept of corporate criminal liability is also built on the idea that a company acts through its 'mind and will,' which is ordinarily attributed to its directors, thereby allowing the company itself to be held culpable.

However, these statutory provisions operate on the assumption of a clear and identifiable hierarchy, one where authority flows from a superior to a subordinate through defined commands. This assumption becomes problematic in the context of Decentralised Autonomous Organisations, where decisions emerge from decentralised voting mechanisms and automated code rather than from identifiable individuals. In such a framework, determining who truly exercises control or can be said to be "in charge" is far from straightforward.

ENTER THE ALGORITHM: VIRTUAL CORPORATIONS AND THEIR DIRECTORS

DAOs and other digital-first business models are fundamentally reshaping conventional ideas of corporate governance. Unlike traditional companies, DAOs do not operate through a centralised leadership structure. Instead, governance is carried out through smart contracts and voting mechanisms controlled by token holders. Even routine corporate functions, such as executing contracts or managing payments, are often automated through code.

Consider a DAO that manages virtual property in the metaverse and deploys a smart contract to govern lease agreements. If that contract fails to account for applicable local regulations and results in a legal violation, the question immediately arises: who bears responsibility?

[2] Companies Act 2013, s 2(60)
[3] Companies Act 2013, s 66, 47

In a conventional corporate setup, accountability would typically rest with identifiable individuals such as the Chief Executive Officer, compliance officers, or legal advisors. In a DAO, however, these roles are either absent or dispersed among anonymous contributors. The decentralised and automated nature of such organisations makes the application of traditional principles of vicarious liability deeply problematic, as the established assumptions of control and hierarchy no longer hold.

DEVELOPERS AS SHADOW DIRECTORS: CODE IS LAW, BUT WHO CONTROLS IT?

Attention must then turn to the developers, the individuals who design and deploy the code that governs the functioning of these virtual organisations. While developers are rarely designated as directors in any formal sense, their influence over the DAO's operations can be substantial. By creating or modifying smart contracts that dictate how the organisation functions, developers often exercise a degree of control comparable to that of corporate decision-makers.

This brings into focus the legal concept of a 'shadow director.' Under Sections 2(59) and 2(60) of the Companies Act 2013,[4] a person in accordance with whose directions or instructions the Board is accustomed to act may be regarded as a de facto or shadow director. Where developers routinely amend core contracts or embed decisive operational choices into immutable code, courts may reasonably view them as exercising such influence.

Developers frequently counter this by arguing that once deployed on the blockchain, the code operates autonomously and beyond their control. While this argument may hold technical merit, legal analysis tends to focus on intent, foreseeability, and control. If a developer was aware of a potential legal risk and possessed the ability to prevent or rectify it, liability may still arise despite claims of technical autonomy.

TOKEN HOLDERS: DIRECTORS BY DEMOCRACY?

In traditional corporate structures, shareholders generally participate in decision-making only on limited and significant matters. DAOs, by contrast, enable token holders to vote on a wide

[4] Companies Act 2013, ss 2(59)-2(60)

range of operational issues, including hiring decisions, protocol upgrades, and the allocation of funds. Such extensive involvement begins to blur the line between ownership and management.

Indian company law may offer a basis for extending liability in such circumstances. Under Section 2(60) of the Companies Act,[5] individuals whose instructions are routinely followed, or who participate in the day-to-day management of the company, may be classified as 'officers in default.' For instance, if token holders of a DAO engaged in peer-to-peer lending collectively vote to introduce a lending mechanism that violates local regulations, the question arises whether they can be held liable, at least in a collective sense.

While Indian courts have not yet addressed this issue directly, international developments offer some guidance. In *CFTC v Ooki DAO* (2023), a United States court held that token holders who actively participated in governance could be treated as "persons" for legal accountability. Although not binding in India, the case signals a broader global shift towards recognising decentralised participants as legally responsible actors, a trajectory Indian courts may eventually follow.

SMART CONTRACTS AS EMPLOYEES? NAVIGATING THE GREY ZONE

In conventional business structures, decision-making and execution are carried out by identifiable human actors. When something goes wrong, liability is traced back through this chain to the person responsible. Smart contracts complicate this model. These self-executing pieces of code perform predefined functions automatically, without any further human intervention, once deployed.

Consider a DAO operating in the decentralised finance (DeFi) space that deploys a lending smart contract. Due to a minor coding error, users are charged excess interest. There is no malicious intent and no external interference, only flawed code. The question then becomes: who is to be held accountable?

One approach that has gained attention is the idea of treating smart contracts as agents, or even quasi-employees, of the organisation. After all, they perform tasks on behalf of the entity. Under

[5] Companies Act 2013, s 2(60)

traditional principles of agency law, when an agent acts within the scope of its authority, liability attaches to the principal. If smart contracts are viewed through this lens, firms could be held responsible for the consequences of their automated actions, even where the harm is accidental.

While Indian law has not yet tested this theory directly, the Companies Act, 2013 provides possible entry points. Sections 2(38) and 2(60)[6] may be invoked to examine the role of developers or deployment teams, particularly where inadequate supervision, auditing, or testing results in malfunction or regulatory breach. In such cases, liability may arise not because the code erred, but because human oversight failed.

Comparative jurisprudence also offers guidance. In *Various Claimants v Barclays Bank* (UK, 2020), the court examined whether a relationship was 'akin to employment' rather than formally contractual. Applying this reasoning, if a smart contract is integral to a company's operations and performs functions that would otherwise be carried out by human employees, the analogy to agency or employment becomes legally persuasive.

In India, although statutory law has yet to fully grapple with AI-driven or algorithmic decision-making, regulatory signals suggest an evolving approach. The Ministry of Electronics and Information Technology's 2023 AI framework introduced system classifications, transparency obligations, and potential liability for harmful outcomes. Should such principles be formally legislated, businesses and DAOs alike may face accountability for automated decisions, especially where there is a failure to audit, monitor, or control digital systems.

While the legal position remains unsettled, the practical risks are undeniable. Organisations can no longer afford to treat code as a neutral or consequence-free tool; responsibility does not disappear merely because decisions are automated.

PLATFORM LIABILITY: WHEN INFRASTRUCTURE BECOMES ACCOUNTABLE

Behind every DAO and decentralised application lies a critical but often overlooked layer, the blockchain platform on which it operates. Networks such as Ethereum, Solana, Avalanche, and

[6] Companies Act 2013, ss 2(38), 2(60)

Binance Smart Chain are frequently characterised as neutral infrastructure. Yet this characterisation understates their functional role.

These platforms do far more than merely "host" applications. They validate transactions, execute smart contracts, and provide the protocol-level architecture upon which decentralised ecosystems depend. In practical terms, they are not passive landlords but active facilitators. When things go wrong, the question naturally arises: can platforms be held vicariously liable for activities conducted on their networks?

International regulatory bodies are increasingly answering in the affirmative. The Financial Action Task Force (FATF) has classified entities that enable the exchange, transfer, or custody of virtual assets as Virtual Asset Service Providers (VASPs). Once categorised as such, platforms are subject to anti-money laundering and counter-terrorist financing obligations similar to those imposed on traditional financial institutions. This reflects a growing recognition that platforms are not merely neutral conduits; their design choices and enforcement mechanisms can either prevent or enable misconduct.

The analogy is instructive. In the physical world, a property owner who knowingly permits illegal activity on their premises may face legal consequences for complicity or negligence. A similar logic is beginning to emerge in the digital realm. If a blockchain platform facilitates a DAO that engages in fraud, money laundering, or the dissemination of malicious software, regulatory authorities are increasingly unwilling to accept claims of complete non-involvement.

As decentralised systems become more embedded in real-world finance and governance, platforms may be expected to take on greater compliance responsibilities. These could include vetting smart contracts before deployment, monitoring suspicious activity, and even freezing transactions when legally required. Some networks have already taken tentative steps in this direction. Ethereum's layer-two solutions and emerging compliance layers allow for limited intervention, while Binance Smart Chain has introduced measures to flag or restrict illicit tokens and wallets. Although these mechanisms remain imperfect, they signal a broader shift in regulatory expectations.

This evolution, however, presents a fundamental tension. Excessive regulation risks undermining the decentralised ethos that defines blockchain technology. Yet from a legal standpoint, the trajectory is clear: platforms are increasingly viewed as gatekeepers, and gatekeepers carry duties.

The precise contours of platform liability remain unsettled, but one conclusion is unavoidable. In the emerging framework of decentralised corporate activity, infrastructure can no longer remain invisible. As regulators and courts turn their attention to the foundation layer, platforms may find that responsibility travels upward and that being 'just the infrastructure' is no longer a sufficient defence.

THE STRUGGLES IN THE COURTROOM: WHEN JUDGES MEET CODE

Having examined how vicarious liability might apply to DAOs, developers, token holders, and platforms, attention must now turn to those tasked with resolving these questions in practice - the judiciary. Courts are traditionally equipped to assess human intention, documentary evidence, and corporate decision-making processes. Increasingly, however, they are being asked to determine whether an error in a smart contract constitutes negligence, or whether collective voting by thousands of anonymous token holders can give rise to legal responsibility.

This presents an unfamiliar challenge. Judges trained to interpret statutes and precedents must now grapple with decentralised systems, automated execution, and lines of code written in programming languages such as Solidity. While this may seem far removed from conventional adjudication, courts have shown a willingness to adapt.

A notable example is the United States decision in *CFTC v Ooki DAO* (2023), where a DAO was treated as an unincorporated association capable of being sued, and governance token holders were held potentially liable where they played an active role in decision-making. Although no comparable Indian precedent exists as yet, Indian courts have historically demonstrated flexibility in responding to novel legal issues, whether through expansive environmental jurisprudence or the recognition of the right to privacy in *Puttaswamy v Union of India*[7].

[7] *Justice K.S. Puttaswamy (Retd) v Union of India* 2019 (1) SCC 1

The more immediate difficulty, however, lies in procedure. How does one serve notice on a DAO? Who represents it in court? Where there is no registered office, no board, and no formal management, the traditional tools of litigation begin to falter. Until procedural law evolves to reflect digital realities, courts may find themselves struggling to identify responsible actors within decentralised systems.

REGULATORY FOG: THE LAW LAGS BEHIND

India's existing regulatory framework has yet to meaningfully engage with the rise of DAOs and decentralised governance. The Companies Act 2013 is premised on conventional corporate structures - boards, directors, shareholders, and annual general meetings. DAOs, by contrast, operate through governance proposals and token-based voting mechanisms, rendering many of these assumptions obsolete.

There are no provisions recognising non-human decision-makers or addressing liability arising from automated execution via smart contracts. Even the Information Technology Act 2000[8], which governs cyber activities, does not contemplate decentralised or algorithm-driven governance structures.

Some guidance may be drawn from the Digital Personal Data Protection Act 2023[9], which introduces accountability for entities using automated systems to process data. While not directly applicable to DAOs, the underlying principle that automation does not eliminate responsibility could inform future legislative or judicial approaches. For now, however, such extensions remain speculative.

Regulatory bodies such as the Reserve Bank of India and SEBI have addressed certain aspects of crypto assets and exchanges, but have remained largely silent on the legal status and governance of DAOs. Whether DAOs are to be treated as companies, partnerships, trusts, or something entirely novel remains unresolved. This regulatory ambiguity complicates compliance and renders enforcement particularly challenging.

[8] Information Technology Act 2000
[9] Digital Personal Data Protection Act 2023

THE RISK OF EVADING RESPONSIBILITY: A STRUCTURAL LOOPHOLE

In the absence of clear legal frameworks, DAOs risk becoming vehicles for evading accountability. With no formally appointed directors, no physical presence, and no identifiable chain of command, responsibility can easily dissolve into decentralised ambiguity. When wrongdoing occurs, the response is often a collective shrug: 'It was the DAO.' Such outcomes undermine the very purpose of vicarious liability, which exists to ensure that harms caused in the course of business do not escape legal scrutiny. If entities can simply restructure as DAOs and shield themselves behind anonymous governance mechanisms, both regulators and affected parties are left without effective remedies. This concern is not merely theoretical. The 2016 DAO hack demonstrated how vulnerabilities in smart contract code could result in massive financial losses without any clear avenue for legal accountability. The code functioned as written, and the absence of a recognised legal entity left regulators with little room to act.

Vicarious liability is not punitive in nature; it is grounded in the principle of responsibility. Unless the law adapts to address decentralised business models, that principle risks being hollowed out.

THE WAY FORWARD: BRIDGING LAW AND TECHNOLOGY

Looking ahead, several possible paths emerge. One option is to formally recognise DAOs as legal entities, akin to limited liability partnerships or registered trusts. Jurisdictions such as Wyoming in the United States have already taken steps in this direction by allowing DAOs to register as limited liability companies. A similar approach in India could provide legal certainty without stifling innovation.

Another reform could involve expanding the interpretation of "officer in default" under the Companies Act. Where developers or token holders exercise sustained control over decision-making or code deployment, courts could adopt a purposive approach that focuses on actual influence rather than formal titles.

Regulatory intervention will also be crucial. Authorities such as SEBI or the Ministry of Corporate Affairs could issue guidelines classifying decentralised entities, prescribing disclosure

obligations, and clarifying responsibility for code-based operations. Such measures would help bring DAOs operating in Indian markets within a visible compliance framework.

Finally, legal education must evolve alongside technological change. Future lawyers and judges will need at least a working understanding of blockchain systems, smart contracts, and decentralised governance. As digital evidence increasingly finds its way into courtrooms, the ability to interpret technological processes will become as essential as statutory interpretation. The intersection of law and code is no longer a distant possibility; it is already here. The challenge lies in ensuring that legal accountability keeps pace with technological innovation, rather than being left behind by it.

CONCLUSION: GHOSTS IN THE (CORPORATE) MACHINE

For centuries, the doctrine of vicarious liability has provided a reliable framework for attributing responsibility within corporate structures. By linking liability to the acts of directors, agents, and employees, the law has ensured that wrongdoing carried out in the course of business does not escape accountability. However, the emergence of virtual corporations, smart contracts, and decentralised governance models has placed this doctrine in unfamiliar territory.

The central question is no longer merely *who committed the act*, but *who can be said to be responsible* when decision-making is automated, dispersed, or embedded in code. In systems where there is no clear driver at the wheel, traditional assumptions about control and intent begin to falter. This paper has argued that the answer does not lie in discarding vicarious liability altogether, but in reimagining its application for an algorithm-driven age. Through legislative reform, purposive judicial interpretation, and clearer regulatory expectations for platforms and participants, the law can adapt to these new forms of enterprise without sacrificing its core principles.

After all, the harm caused by a malfunctioning smart contract or a reckless DAO is very real. The fact that the decision was executed by code rather than by human hands does not diminish its consequences. If the law is to remain effective and credible, it must evolve to confront these digital realities. The corporate form may be changing, but responsibility cannot be allowed to disappear into the machine.