

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Automated Decision Making in Corporate Governance: Minority Shareholder Oppression in Smart Contract Voting Systems

MOHIT KHARB* AND PARTHA PRATIM MITRA**

ABSTRACT

The rise of digital technologies has transformed corporate governance, introducing tools such as smart contracts to automate decision making in shareholder voting. These systems promise efficiency, transparency, and reduced human error, yet their adoption raises significant concerns for minority shareholders, who may find themselves particularly vulnerable to oppression in a digital voting environment. Unlike traditional voting mechanisms, smart-contract-based systems are coded with predefined rules that execute automatically, leaving little room for human oversight or intervention. While this automation can prevent certain forms of manipulation, it may also entrench existing power imbalances, allowing majority shareholders to design rules or triggers that systematically disadvantage minority interests. The technical intricacy of smart contracts may further mask important governance choices, making it difficult for shareholders with less technological expertise to monitor or contest unfair practices. This paper examines the relationship between minority shareholder rights and automated decision making, addressing the practical and legal dimensions of corporate voting powered by smart contracts. It considers risks such as the absence of recourse, the opacity of coded rules, and the unforeseen effects of algorithmic rigidity. By drawing attention to these difficulties, this paper seeks to inform regulators, corporate boards, and shareholders of the need for safeguards that ensure equity, accountability, and inclusivity in the governance of businesses adopting digital voting technologies. Ultimately, although smart contracts have the potential to transform corporate governance, caution is required to prevent automation from escalating the oppression of minority shareholders.

Keywords: *Automated corporate governance, smart contract voting, minority shareholder oppression, blockchain, corporate accountability.*

* Author is an LLM student at Vivekananda Global University, Jaipur, Rajasthan, India.

** Author is a Professor and Dean, Faculty of Law, Vivekananda Global University, Jaipur, Rajasthan, India.

I. INTRODUCTION

The rapid digitalization of corporate governance has transformed traditional mechanisms of shareholder participation and decision making. In recent years, blockchain technology and smart contracts have been increasingly integrated into corporate voting systems to enhance transparency, efficiency, and automation in governance processes.¹ These technologies promise to reduce transaction costs, eliminate intermediaries, and ensure tamper-resistant records of shareholder votes.²

Automated decision making (ADM) in corporate governance refers to the use of algorithmic systems to execute, monitor, and enforce corporate decisions without continuous human intervention.³ Smart contracts, self-executing code deployed on blockchain networks, enable automated voting outcomes once predefined conditions are met.⁴ While such systems offer significant advantages in terms of speed and reliability, they raise complex legal and governance concerns, particularly regarding minority shareholder rights.⁵

Minority shareholder oppression has long been a central issue in corporate law. Traditional corporate structures often concentrate power in majority shareholders or controlling management, thereby creating risks of exclusion, unfair prejudice, and abuse of voting power against minority stakeholders.⁶ Corporate law has historically responded through doctrines such as fiduciary duties, derivative actions, and oppression remedies to safeguard minority interests.⁷

The transition from conventional voting mechanisms to smart-contract-based systems does not eliminate these structural power imbalances. Instead, it may encode them into immutable digital frameworks that are resistant to modification once deployed.⁸ When governance rules are translated into code, the interpretation of shareholder rights becomes dependent on technical design choices, potentially limiting judicial flexibility and equitable remedies.⁹

Smart contract voting systems are increasingly utilized in decentralized autonomous organizations (DAOs) and blockchain-enabled corporations. These systems automatically execute voting outcomes once quorum and majority thresholds are met, without discretionary

¹ Don Tapscott & Alex Tapscott, *BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD* (2016).

² Nick Szabo, *FORMALIZING AND SECURING RELATIONSHIPS ON PUBLIC NETWORKS*, 2(9) *First Monday* (1997).

³ Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 *REGUL. & GOVERNANCE* 505 (2018).

⁴ Vitalik Buterin, *A NEXT-GENERATION SMART CONTRACT AND DECENTRALIZED APPLICATION PLATFORM* (Ethereum White Paper, 2014).

⁵ Primavera De Filippi & Aaron Wright, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE* (2018).

⁶ Frank H. Easterbrook & Daniel R. Fischel, *THE ECONOMIC STRUCTURE OF CORPORATE LAW* (1991).

⁷ David Kershaw, *COMPANY LAW IN CONTEXT: TEXT AND MATERIALS* (2d ed. 2012).

⁸ Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 *DUKE L.J.* 313 (2017).

⁹ Lawrence Lessig, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

human oversight.¹⁰ Although automation can reduce fraud and manipulation, it may also amplify majority dominance by rigidly enforcing numerical outcomes without considering contextual fairness.¹¹

Minority shareholders in smart contract voting environments face unique risks. First, algorithmic rigidity may prevent the suspension or review of oppressive resolutions before execution, thereby limiting the opportunity for injunctive relief.¹² Second, coding errors or vulnerabilities may disproportionately affect minority stakeholders who lack technical expertise or influence over the contract's design.¹³

The concept of "code as law" highlights how technological architecture can regulate behaviour as effectively as legal rules.¹⁴ In blockchain governance, smart contracts effectively replace or supplement corporate bylaws, embedding decision-making logic directly into software protocols.¹⁵ This transformation raises concerns about accountability, transparency, and access to remedies for minority shareholders when automated decisions produce unjust outcomes.¹⁶

Furthermore, automated governance systems may reduce opportunities for deliberation and negotiation among shareholders. Traditional corporate meetings allow for discussion, persuasion, and compromise before final voting decisions are made.¹⁷ In contrast, smart contract voting often relies on token-weighted voting mechanisms that emphasize quantitative control rather than qualitative deliberation.¹⁸

Token-weighted voting structures, common in blockchain governance, allocate decision-making power in proportion to token ownership. While this mirrors the "one share, one vote" principle in corporate law, it may exacerbate wealth concentration and marginalize minority voices.¹⁹ The automation of such mechanisms through smart contracts can entrench these inequalities by removing opportunities for judicial or managerial discretion.²⁰

¹⁰ Samer Hassan & Primavera De Filippi, *Decentralized Autonomous Organization*, 10(2) INTERNET POL'Y REV. (2021).

¹¹ Dirk A. Zetsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The Rise of Decentralized Autonomous Organizations*, 6 J. FIN. REG. 257 (2020).

¹² De Filippi & Wright, *supra* note 5.

¹³ Nicola Atzei, Massimo Bartoletti & Tiziana Cimoli, *A Survey of Attacks on Ethereum Smart Contracts*, in PRINCIPLES OF SECURITY AND TRUST 164 (2017).

¹⁴ Lessig, *supra* note 9.

¹⁵ Kevin Werbach, *THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST* (2018).

¹⁶ Yeung, *supra* note 3.

¹⁷ Kershaw, *supra* note 7.

¹⁸ Hassan & De Filippi, *supra* note 10.

¹⁹ Zetsche et al., *supra* note 11.

²⁰ Easterbrook & Fischel, *supra* note 6.

Additionally, algorithmic bias and design asymmetries may further disadvantage minority shareholders. The individuals who draft and deploy smart contracts, often developers or controlling stakeholders, may encode governance rules that subtly favour majority interests.²¹ Once deployed, the immutability of blockchain systems makes it difficult to amend or rectify these embedded biases without consensus from dominant stakeholders.²²

Corporate governance theory emphasizes the importance of balancing efficiency with fairness. While automation enhances efficiency by reducing delays and human error, it may undermine equitable treatment if minority shareholders lack effective participation or redress mechanisms.²³ The absence of interpretative flexibility in automated systems contrasts sharply with traditional judicial oversight, where courts can evaluate the substance and fairness of corporate actions.²⁴

Another dimension of concern involves regulatory uncertainty. Existing corporate laws were designed for centralized entities with identifiable directors and management structures.²⁵ Smart-contract-based governance challenges these frameworks by decentralizing authority and diffusing responsibility among code developers, token holders, and platform operators.²⁶ This fragmentation complicates the attribution of liability in cases of minority oppression.

Moreover, decentralized governance models often operate across jurisdictions, raising questions about applicable law and enforcement mechanisms.²⁷ Minority shareholders may face significant barriers in pursuing legal remedies against anonymous or globally dispersed majority stakeholders.²⁸ This cross-border dimension further weakens traditional protective doctrines in corporate law.

The intersection of automated decision making and minority shareholder protection thus presents a critical area of contemporary legal inquiry. While blockchain governance promises transparency and procedural fairness through open ledgers and immutable records, transparency alone does not guarantee substantive justice.²⁹ A system may be transparent yet still produce outcomes that are oppressive or discriminatory toward minority stakeholders.³⁰

²¹ Atzei et al., *supra* note 13.

²² Buterin, *supra* note 4.

²³ Easterbrook & Fischel, *supra* note 6.

²⁴ Kershaw, *supra* note 7.

²⁵ Zetzsche et al., *supra* note 11.

²⁶ Werbach, *supra* note 15.

²⁷ De Filippi & Wright, *supra* note 5.

²⁸ Hassan & De Filippi, *supra* note 10.

²⁹ Yeung, *supra* note 3.

³⁰ Lessig, *supra* note 9.

Therefore, scholarly analysis must assess whether existing corporate law doctrines, such as unfair prejudice remedies and fiduciary duties, are adaptable to smart contract environments. It is necessary to examine whether algorithmic governance can incorporate safeguards such as dispute resolution triggers, pause functions, or override mechanisms to prevent oppressive outcomes.³¹

II. AUTOMATED DECISION-MAKING (ADM) FRAMEWORKS

Automated decision-making (ADM) frameworks have emerged as a critical component of modern governance, particularly in domains where algorithmic systems influence legal, economic, and social outcomes.³² Such frameworks refer to structured processes wherein decisions are made wholly or partially by algorithms without continuous human intervention, often relying on data analytics, machine learning, and artificial intelligence tools.³³ The growing reliance on ADM systems has raised concerns about accountability, transparency, and fairness, especially when these systems operate in sensitive sectors such as finance, criminal justice, and public administration.³⁴ At the conceptual level, an effective ADM framework is built upon core principles including transparency, explainability, accountability, and non-discrimination.³⁵ Transparency ensures that stakeholders understand how decisions are derived, while explainability provides meaningful justifications for outcomes generated by algorithms.³⁶ Accountability mechanisms assign responsibility to developers, deployers, and regulators for the consequences of automated decisions.³⁷ Furthermore, non-discrimination requires that ADM systems avoid biases that may lead to unequal treatment of individuals based on protected characteristics.³⁸

In the Indian context, the adoption of ADM systems has been increasing across sectors such as fintech, e-governance, and digital platforms, necessitating a robust regulatory and ethical framework. India's legal ecosystem, particularly through the Digital Personal Data Protection

³¹ Werbach & Cornell, *supra* note 8.

³² See generally Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'*, 38 AI MAG. 50 (2017).

³³ *Id.*

³⁴ Frank Pasquale, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015).

³⁵ Finale Doshi-Velez & Been Kim, *Towards a Rigorous Science of Interpretable Machine Learning* (2017), <https://arxiv.org/abs/1702.08608>.

³⁶ Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76 (2017).

³⁷ Michael Veale & Lilian Edwards, *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*, 34 COMPUTER L. & SEC. REV. 398 (2018).

³⁸ Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

Act and sectoral guidelines, has begun to acknowledge the implications of algorithmic decision-making.³⁹

However, the absence of a comprehensive statutory framework specifically addressing ADM raises concerns regarding oversight and redressal mechanisms. Globally, jurisdictions such as the European Union have taken significant steps to regulate ADM through instruments like the General Data Protection Regulation (GDPR), which introduces safeguards such as the "right to explanation" and restrictions on solely automated decisions.⁴⁰ These regulatory measures emphasize the importance of human oversight and informed consent in automated processes.⁴¹ Similarly, the United States adopts a sector-specific approach, focusing on algorithmic accountability through guidelines and enforcement actions rather than a unified legislative framework.⁴² An effective ADM framework also incorporates procedural safeguards to mitigate risks associated with automation. These safeguards include algorithmic audits, impact assessments, and continuous monitoring to ensure system integrity and fairness.⁴³ Algorithmic impact assessments, in particular, serve as proactive tools to evaluate potential risks before deployment.⁴⁴ Moreover, independent audits enhance trust by verifying that systems operate in accordance with legal and ethical standards.⁴⁵

Another critical dimension of ADM frameworks is data governance, as the quality and integrity of data directly influence the outcomes of automated systems.⁴⁶ Bias in training data can lead to discriminatory outcomes, thereby undermining the legitimacy of automated decisions.⁴⁷ Consequently, robust data protection measures and ethical data practices are essential to ensure fairness and reliability in ADM processes.⁴⁸ The integration of human oversight remains a key requirement in ADM frameworks to prevent over-reliance on automated systems. Human-in-the-loop models enable intervention in critical decision-making processes, thereby enhancing

³⁹ The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁴⁰ Paul Voigt & Axel von dem Bussche, *THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE* (2017).

⁴¹ Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18 (2017).

⁴² Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

⁴³ Inioluwa Deborah Raji et al., *Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing*, in PROCEEDINGS OF THE 2020 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 33 (2020).

⁴⁴ Dillon Reisman et al., *ALGORITHMIC IMPACT ASSESSMENTS: A PRACTICAL FRAMEWORK FOR PUBLIC AGENCY ACCOUNTABILITY* (AI Now Inst. 2018).

⁴⁵ Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017).

⁴⁶ Luciano Floridi et al., *AI4People: An Ethical Framework for a Good AI Society*, 28 MINDS & MACHINES 689 (2018).

⁴⁷ Cathy O'Neil, *WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY* (2016).

⁴⁸ Brent Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, 3 BIG DATA & SOC'Y 1 (2016).

accountability and reducing the risk of erroneous outcomes.⁴⁹ Such hybrid approaches strike a balance between efficiency and ethical considerations, ensuring that automation does not compromise fundamental rights.⁵⁰

In addition to legal and technical considerations, ADM frameworks must also address ethical challenges associated with algorithmic governance. Ethical guidelines emphasize fairness, inclusivity, and respect for human dignity in automated decision-making processes.⁵¹ These principles are increasingly being incorporated into policy frameworks and corporate governance structures to promote responsible AI deployment.⁵² In conclusion, the development of a comprehensive ADM framework requires a multidisciplinary approach that integrates legal, technical, and ethical perspectives. While global jurisdictions have made significant progress in regulating automated decision-making, India still faces challenges in establishing a cohesive and enforceable framework. Future efforts should focus on strengthening regulatory mechanisms, enhancing transparency, and ensuring that automated systems operate in a manner consistent with constitutional and human rights principles.

III. SMART CONTRACT VOTING

Smart contract voting is an emerging application of blockchain technology that seeks to enhance the transparency, security, and efficiency of electoral and organizational decision-making processes. Smart contracts are self-executing digital agreements deployed on blockchain networks, where predefined rules are automatically enforced without the need for intermediaries. In voting systems, smart contracts can be programmed to register eligible voters, record votes, verify voter authenticity, and automatically calculate and publish election results.⁵³ The integration of smart contracts into voting mechanisms offers several advantages over conventional electronic and paper-based voting systems. First, blockchain-based smart contracts provide immutability, ensuring that once a vote is recorded, it cannot be altered or deleted. This feature significantly reduces the risk of electoral fraud and unauthorized manipulation of voting records.⁵⁴ Second, smart contracts enable real-time vote counting and

⁴⁹ Saleema Amershi et al., *Power to the People: The Role of Humans in Interactive Machine Learning*, 35 AI MAG. 105 (2014).

⁵⁰ Iyad Rahwan, *Society-in-the-Loop: Programming the Algorithmic Social Contract*, 20 ETHICS & INFO. TECH. 5 (2018).

⁵¹ Anna Jobin, Marcello Ienca & Effy Vayena, *The Global Landscape of AI Ethics Guidelines*, 1 NATURE MACH. INTELLIGENCE 389 (2019).

⁵² Corinne Cath et al., *Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach*, 24 SCI. & ENG'G ETHICS 505 (2018).

⁵³ Nick Szabo, *THE IDEA OF SMART CONTRACTS* (1997).

⁵⁴ Satoshi Nakamoto, *BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM* (2008), <https://bitcoin.org/bitcoin.pdf>.

result generation, thereby minimizing administrative costs and delays associated with manual vote tabulation. Furthermore, the decentralized nature of blockchain networks eliminates dependence on a single authority, enhancing trust among participants and reducing the possibility of centralized control or corruption.⁵⁵

Another significant benefit of smart contract voting is transparency. All voting transactions can be securely recorded on a distributed ledger, allowing authorized stakeholders to verify the integrity of the election process. At the same time, cryptographic techniques can be incorporated to protect voter anonymity and confidentiality, thereby balancing transparency with privacy requirements.⁵⁶ These characteristics make smart contract voting particularly attractive for corporate governance, shareholder voting, public elections, and decentralized autonomous organizations (DAOs). Despite these advantages, several challenges remain. Technical vulnerabilities in smart contract code may expose voting systems to cyberattacks or unintended outcomes. Additionally, issues related to digital literacy, internet accessibility, and scalability may limit widespread adoption. Legal and regulatory uncertainties also persist, particularly regarding the recognition of blockchain-based voting records and the allocation of liability in cases of system malfunction.⁵⁷

As governments and institutions continue to explore digital governance mechanisms, smart contract voting has the potential to transform democratic participation by providing a secure, transparent, and efficient alternative to traditional voting methods. However, its successful implementation requires robust technological safeguards, clear legal frameworks, and comprehensive oversight mechanisms to ensure public trust and electoral integrity. The absence of a comprehensive statutory framework specifically addressing automated decision-making thus raises concerns regarding oversight and redressal mechanisms, and the safeguards developed in instruments such as the GDPR, including the "right to explanation" and restrictions on solely automated decisions,⁵⁸ remain equally relevant to the deployment of smart-contract-based voting mechanisms, emphasizing transparency, accountability, and human oversight.

IV. MINORITY RIGHTS AND OPPRESSION

Minority rights are an essential aspect of human rights protection and democratic governance. They aim to safeguard individuals and groups who differ from the majority on the basis of

⁵⁵ Zibin Zheng et al., *Blockchain Challenges and Opportunities: A Survey*, 14 INT'L J. WEB & GRID SERVS. 352 (2018).

⁵⁶ Dylan Yaga et al., BLOCKCHAIN TECHNOLOGY OVERVIEW (NIST Internal Rep. 8202, 2019).

⁵⁷ Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 6(1) J. GOVERNANCE & REG. 45 (2017).

⁵⁸ Voigt & von dem Bussche, *supra* note 40.

religion, ethnicity, language, culture, or other characteristics. International instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) recognize the need to protect minorities from discrimination and ensure equal treatment.⁵⁹ Despite these protections, minority groups often face oppression in the form of social exclusion, economic disadvantage, political marginalization, and cultural discrimination. Such practices limit their opportunities and participation in society, thereby undermining the principles of equality and justice. The protection of minority rights therefore requires not only legal recognition but also effective measures to promote inclusion and prevent discrimination.⁶⁰

In the digital age, concerns regarding minority rights have expanded to automated decision-making (ADM) systems. Algorithms used in employment, credit assessment, and public services may unintentionally reinforce existing biases, leading to discriminatory outcomes for vulnerable communities. Transparency and accountability in technological systems have therefore become important aspects of minority rights protection. However, the absence of a comprehensive statutory framework specifically addressing ADM raises concerns regarding oversight and redressal mechanisms. Globally, jurisdictions such as the European Union have taken significant steps to regulate ADM through instruments like the General Data Protection Regulation (GDPR), which introduces safeguards such as the "right to explanation" and restrictions on solely automated decisions.⁶¹ These regulatory measures emphasize the importance of transparency, accountability, and fairness in protecting minority rights in an increasingly digital society.

V. OPPRESSION IN AUTOMATED VOTING

Automated voting systems based on smart contracts have emerged as a transformative approach to conducting elections in a secure, transparent, and efficient manner. By leveraging blockchain technology, these systems can automate vote collection, verification, and counting without the need for centralized intermediaries. Smart contracts execute predefined voting rules automatically, reducing the possibility of human error, manipulation, or electoral fraud. Furthermore, the immutable nature of blockchain records ensures that votes cannot be altered once they are cast, thereby enhancing trust in the electoral process.⁶² Transparency represents one of the most significant advantages of automated voting systems. Voting transactions can be

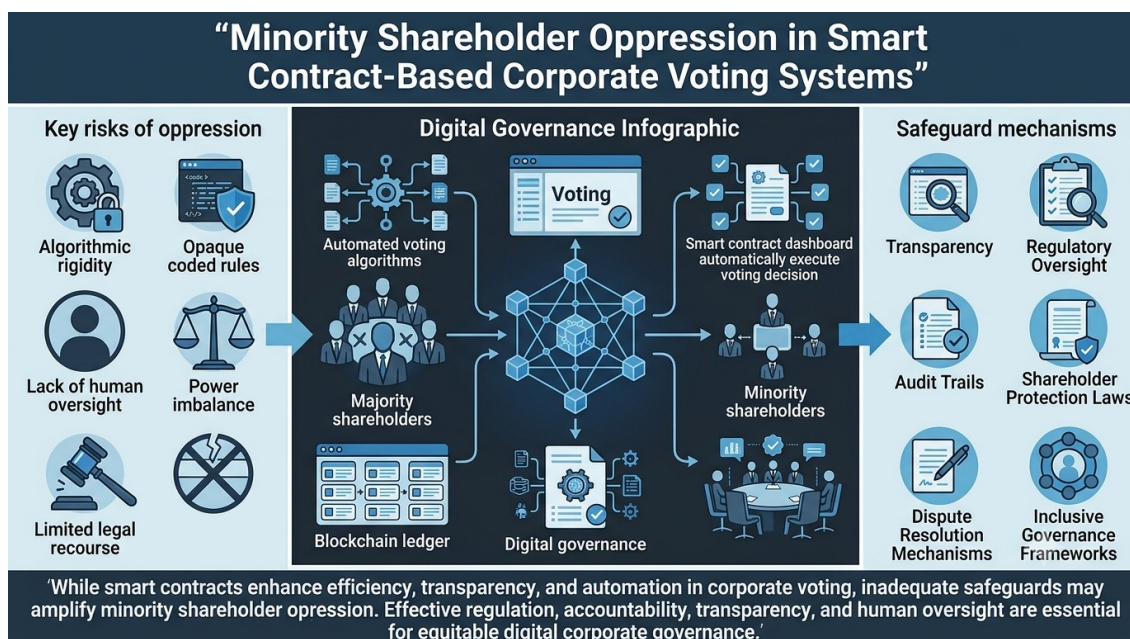
⁵⁹ Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/810 (Dec. 10, 1948); International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

⁶⁰ Will Kymlicka, *MULTICULTURAL CITIZENSHIP: A LIBERAL THEORY OF MINORITY RIGHTS* (1995).

⁶¹ Voigt & von dem Bussche, *supra* note 40.

⁶² Yaga et al., *supra* note 54.

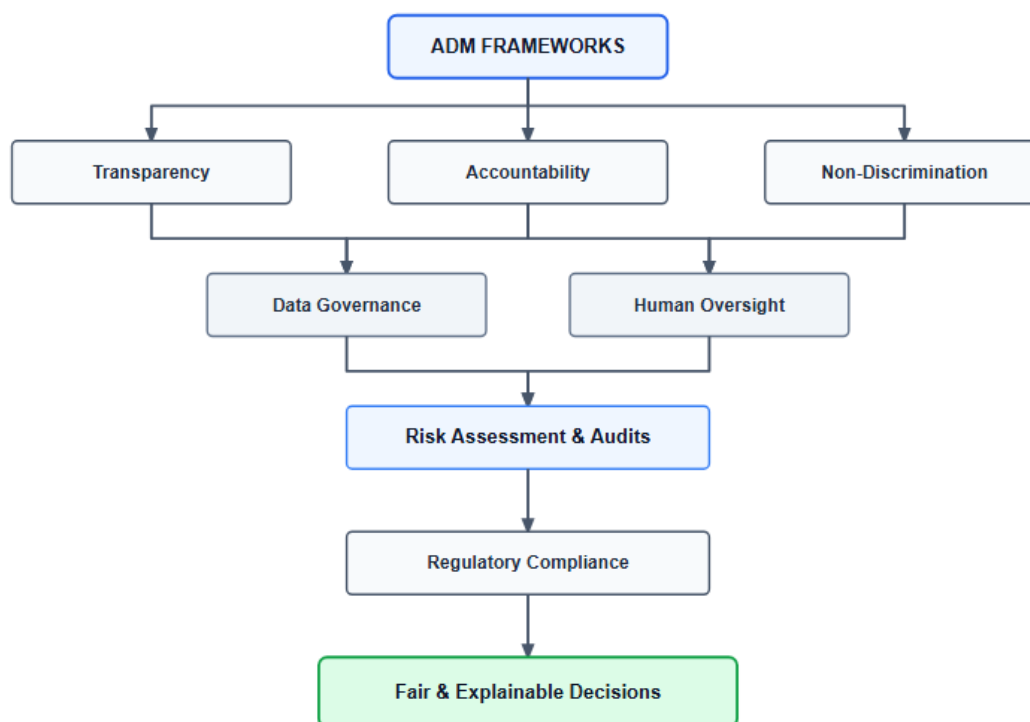
permanently recorded on a distributed ledger, enabling authorized participants to verify election outcomes and ensuring accountability throughout the process. At the same time, advanced cryptographic mechanisms can safeguard voter anonymity and confidentiality, maintaining a balance between transparency and privacy. These features make automated voting particularly suitable for applications such as corporate governance, shareholder voting, public elections, and decentralized autonomous organizations (DAOs).⁶³ However, the adoption of automated voting systems also presents several challenges. Vulnerabilities in smart contract programming may create opportunities for cyberattacks, software bugs, or unintended execution outcomes. Moreover, limited digital literacy, inadequate internet infrastructure, and scalability concerns may hinder broad implementation. Regulatory and legal uncertainties further complicate deployment, particularly regarding the legal validity of blockchain-based voting records and the determination of liability when technical failures occur. Addressing these challenges is essential to ensure that automated voting systems remain secure, inclusive, and reliable in future governance frameworks.⁶⁴



⁶³ Id.

⁶⁴ Atzori, *supra* note 55.

ADM FRAMEWORKS FOR ETHICAL GOVERNANCE



VI. ALGORITHMIC BIAS AND POWER

In today's digital society, algorithms play a significant role in shaping decisions related to employment, healthcare, education, banking, and social media. Although algorithms are often viewed as objective and efficient tools, they are created and trained using human-generated data. As a result, they may unintentionally reflect existing social inequalities and prejudices present in society.⁶⁵ Algorithmic bias refers to systematic and unfair outcomes that disadvantage certain individuals or groups. Such bias can emerge when historical datasets contain discriminatory patterns or when developers fail to consider diversity during system design. For example, recruitment algorithms trained on past hiring records may favour applicants who resemble previously selected candidates, thereby limiting opportunities for women or minority populations.⁶⁶

The issue of power is closely connected to algorithmic systems because organizations that develop and control these technologies possess considerable influence over social and economic opportunities. Large technology companies, governments, and institutions use algorithms to filter information, recommend content, assess creditworthiness, and support decision-making processes. Consequently, algorithms can shape not only individual experiences but also broader

⁶⁵ Safiya Umoja Noble, *ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM* (2018); O'Neil, *supra* note 47.

⁶⁶ O'Neil, *supra* note 47; UNESCO, *RECOMMENDATION ON THE ETHICS OF ARTIFICIAL INTELLIGENCE* (2021).

societal outcomes.⁶⁷ Furthermore, algorithmic power often operates in ways that are difficult for ordinary users to understand. Many systems function as "black boxes," where the criteria used to make decisions remain hidden from public scrutiny. This lack of transparency can reduce accountability and make it challenging for affected individuals to question or appeal algorithm-driven decisions.⁶⁸

Social media platforms provide a clear example of how algorithmic power influences public opinion. Recommendation systems prioritize content that generates engagement, which may unintentionally promote misinformation, reinforce existing beliefs, and create ideological echo chambers. As these platforms increasingly mediate access to information, algorithms have become powerful tools capable of shaping cultural and political discourse.⁶⁹ Addressing algorithmic bias requires a commitment to fairness, transparency, and accountability. Researchers, policymakers, and technology developers must work together to ensure that artificial intelligence systems are regularly audited, trained on diverse datasets, and designed to minimize discriminatory outcomes. Ethical governance of algorithms is essential to ensure that technological advancements benefit society equitably and do not reinforce existing forms of inequality.⁷⁰

VII. LEGAL CHALLENGES IN SMART CONTRACTS

Smart contracts are self-executing digital agreements stored on blockchain networks that automatically perform actions when predefined conditions are met. They have gained significant attention because they reduce the need for intermediaries, increase efficiency, and enhance transparency. However, despite these advantages, several legal challenges continue to limit their widespread adoption.⁷¹ One major challenge is the issue of legal enforceability. Traditional contracts are generally written in natural language and interpreted by courts, whereas smart contracts are coded in programming languages. If a coding error occurs or the programmed outcome does not reflect the parties' intentions, determining legal responsibility can become difficult.⁷² Furthermore, many legal systems have not yet established clear regulations regarding the legal status of smart contracts.

⁶⁷ Shoshana Zuboff, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* (2019); OECD, *OECD PRINCIPLES ON ARTIFICIAL INTELLIGENCE* (2019).

⁶⁸ UNESCO, *supra* note 66; Zuboff, *supra* note 67.

⁶⁹ Noble, *supra* note 66; OECD, *supra* note 67.

⁷⁰ UNESCO, *supra* note 66; O'Neil, *supra* note 47.

⁷¹ Werbach & Cornell, *supra* note 8.

⁷² Aleksei Savelyev, *Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMM. TECH. L. 116 (2017).

Another challenge involves jurisdiction and dispute resolution. Blockchain transactions often occur across national borders, making it difficult to determine which country's laws apply when conflicts arise. Since smart contracts execute automatically, reversing transactions or correcting mistakes may be complex and costly.⁷³ Privacy and data protection also present significant concerns. Blockchain records are generally immutable and transparent, which may conflict with data protection laws such as the European Union's General Data Protection Regulation (GDPR). Personal information stored on a blockchain may be difficult to modify or erase, raising questions about compliance with privacy regulations.⁷⁴ Additionally, smart contracts may contain vulnerabilities in their code. Security flaws can be exploited by hackers, resulting in financial losses. The well-known DAO incident demonstrated how coding weaknesses can lead to significant legal and economic consequences, highlighting the need for robust legal and technical safeguards.⁷⁵

VIII. GLOBAL PRACTICES AND COMPARISON

Countries around the world have adopted different approaches toward regulating and implementing smart contracts. Some nations actively support blockchain innovation, while others remain cautious due to legal and regulatory uncertainties. In the United States, several states, including Arizona and Tennessee, have enacted legislation recognizing the legal validity of blockchain records and smart contracts. These initiatives aim to encourage technological innovation while providing legal certainty for businesses.⁷⁶ The European Union focuses on balancing innovation with consumer protection and data privacy. Through various digital governance frameworks, the EU seeks to ensure that blockchain applications comply with existing legal standards, particularly regarding personal data protection and cybersecurity.⁷⁷

Countries such as Singapore and Switzerland have emerged as global leaders in blockchain regulation. Their governments have introduced clear legal frameworks that support blockchain-based businesses while maintaining regulatory oversight. These jurisdictions are often viewed as attractive destinations for blockchain startups and fintech companies.⁷⁸ In contrast, some developing countries are still in the early stages of establishing blockchain regulations.

⁷³ Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305 (2017).

⁷⁴ Michèle Finck, BLOCKCHAIN AND THE GENERAL DATA PROTECTION REGULATION: CAN DISTRIBUTED LEDGERS BE SQUARED WITH EUROPEAN DATA PROTECTION LAW? (Eur. Parliamentary Research Serv. 2019).

⁷⁵ De Filippi & Wright, *supra* note 5.

⁷⁶ Eliza Mik, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 11 LAW, INNOVATION & TECH. 269 (2019); see Ariz. Rev. Stat. § 44-7061 (2017); Act of Mar. 22, 2018, ch. 591, 2018 Tenn. Pub. Acts (codified at Tenn. Code Ann. § 47-10-201).

⁷⁷ Finck, *supra* note 74.

⁷⁸ De Filippi & Wright, *supra* note 5.

Regulatory uncertainty, limited technical expertise, and infrastructure challenges can slow the adoption of smart contract technologies. Nevertheless, many governments are exploring pilot projects in areas such as supply chain management, digital identity systems, and financial services.⁷⁹ Overall, global practices reveal that successful implementation of smart contracts depends on achieving a balance between technological innovation, legal certainty, consumer protection, and regulatory compliance. As blockchain technology continues to evolve, international cooperation and harmonized legal frameworks may help address existing challenges and promote broader adoption.

IX. ACCOUNTABILITY AND REMEDIES

Accountability is a fundamental principle of corporate governance that ensures companies, directors, and management are answerable for their decisions and actions. It promotes transparency, ethical conduct, and responsible decision-making, helping to protect the interests of shareholders and other stakeholders. When corporate leaders are held accountable, organizations are more likely to maintain trust, comply with legal requirements, and achieve sustainable growth.⁸⁰ In modern corporations, accountability is achieved through mechanisms such as independent boards of directors, financial reporting standards, audits, and regulatory oversight. These mechanisms allow shareholders to monitor management performance and reduce the risk of fraud, misconduct, or misuse of corporate resources. Effective accountability systems also encourage managers to act in the best interests of the company rather than pursuing personal gains.⁸¹

Remedies are legal and regulatory measures available when accountability fails. Shareholders may seek remedies through litigation, derivative actions, compensation claims, or regulatory complaints if directors breach their fiduciary duties. Regulatory authorities can impose penalties, fines, or other sanctions on organizations that violate corporate laws and governance standards. These remedies provide a means to correct wrongdoing and deter future misconduct.⁸² The increasing complexity of global business operations has highlighted the need for stronger accountability frameworks and effective remedies. As corporations expand their influence, stakeholders expect greater transparency and responsibility. Therefore, robust

⁷⁹ Werbach & Cornell, *supra* note 8.

⁸⁰ Bob Tricker, *CORPORATE GOVERNANCE: PRINCIPLES, POLICIES, AND PRACTICES* (4th ed. 2019); Robert A.G. Monks & Nell Minow, *CORPORATE GOVERNANCE* (5th ed. 2011).

⁸¹ Christine A. Mallin, *CORPORATE GOVERNANCE* (6th ed. 2019); OECD, *G20/OECD PRINCIPLES OF CORPORATE GOVERNANCE 2023* (2023).

⁸² Andrew Keay, *THE CORPORATE OBJECTIVE: CORPORATIONS, GLOBALISATION AND THE LAW* (2022); OECD, *supra* note 81.

accountability mechanisms and accessible remedies remain essential for maintaining investor confidence and ensuring long-term corporate sustainability.⁸³

X. FUTURE SHAREHOLDER PROTECTION

Future shareholder protection refers to the measures and strategies designed to safeguard the rights and interests of shareholders in an evolving business environment. As technology, globalization, and financial markets continue to develop, corporations face new governance challenges that require stronger protections for investors. Effective shareholder protection promotes confidence in capital markets and encourages long-term investment.⁸⁴ One of the most important aspects of future shareholder protection is enhanced transparency and disclosure. Companies are increasingly expected to provide accurate and timely information regarding financial performance, environmental practices, governance policies, and potential risks. Improved disclosure enables shareholders to make informed investment decisions and hold management accountable for corporate actions.⁸⁵

Technological advancements are also shaping future protections. Digital voting systems, blockchain-based record keeping, and real-time communication platforms can strengthen shareholder participation and reduce opportunities for manipulation. These innovations enhance corporate transparency while making governance processes more efficient and accessible to investors worldwide.⁸⁶ Furthermore, future shareholder protection will require stronger legal frameworks and regulatory oversight to address emerging risks such as cybersecurity threats, data privacy concerns, and the growing influence of artificial intelligence in corporate decision-making. Policymakers and regulators must continuously adapt governance regulations to ensure that shareholder rights remain protected in a rapidly changing corporate landscape. Strong investor protection mechanisms will remain essential for promoting fairness, trust, and sustainable economic growth.⁸⁷

XI. BIBLIOGRAPHY

1. Saleema Umoja Noble, *ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM* (2018).
2. Nicola Atzei, Massimo Bartoletti & Tiziana Cimoli, *A Survey of Attacks on Ethereum Smart Contracts*, in *PRINCIPLES OF SECURITY AND TRUST* 164 (2017).

⁸³ Tricker, *supra* note 80; Mallin, *supra* note 81.

⁸⁴ OECD, *supra* note 81; Monks & Minow, *supra* note 80.

⁸⁵ Mallin, *supra* note 81; OECD, *supra* note 81.

⁸⁶ Keay, *supra* note 82; Tricker, *supra* note 80.

⁸⁷ OECD, *supra* note 81; Keay, *supra* note 82.

3. Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 6(1) J. GOVERNANCE & REG. 45 (2017).
4. Vitalik Buterin, A NEXT-GENERATION SMART CONTRACT AND DECENTRALIZED APPLICATION PLATFORM (Ethereum White Paper, 2014).
5. Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018).
6. Frank H. Easterbrook & Daniel R. Fischel, THE ECONOMIC STRUCTURE OF CORPORATE LAW (1991).
7. Michèle Finck, BLOCKCHAIN AND THE GENERAL DATA PROTECTION REGULATION (Eur. Parliamentary Research Serv. 2019).
8. Samer Hassan & Primavera De Filippi, *Decentralized Autonomous Organization*, 10(2) INTERNET POL'Y REV. (2021).
9. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
10. Andrew Keay, THE CORPORATE OBJECTIVE: CORPORATIONS, GLOBALISATION AND THE LAW (2022).
11. David Kershaw, COMPANY LAW IN CONTEXT: TEXT AND MATERIALS (2d ed. 2012).
12. Will Kymlicka, MULTICULTURAL CITIZENSHIP: A LIBERAL THEORY OF MINORITY RIGHTS (1995).
13. Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE (1999).
14. Christine A. Mallin, CORPORATE GOVERNANCE (6th ed. 2019).
15. Eliza Mik, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, 11 LAW, INNOVATION & TECH. 269 (2019).
16. Robert A.G. Monks & Nell Minow, CORPORATE GOVERNANCE (5th ed. 2011).
17. Satoshi Nakamoto, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008).
18. Cathy O'Neil, WEAPONS OF MATH DESTRUCTION (2016).
19. Organisation for Economic Co-operation and Development, OECD PRINCIPLES ON ARTIFICIAL INTELLIGENCE (2019).
20. Organisation for Economic Co-operation and Development, G20/OECD PRINCIPLES OF CORPORATE GOVERNANCE 2023 (2023).
21. Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305 (2017).

22. Aleksei Savelyev, *Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMM. TECH. L. 116 (2017).
23. Nick Szabo, *The Idea of Smart Contracts* (1997).
24. Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2(9) First Monday (1997).
25. Don Tapscott & Alex Tapscott, *BLOCKCHAIN REVOLUTION* (2016).
26. Bob Tricker, *CORPORATE GOVERNANCE: PRINCIPLES, POLICIES, AND PRACTICES* (4th ed. 2019).
27. UNESCO, *RECOMMENDATION ON THE ETHICS OF ARTIFICIAL INTELLIGENCE* (2021).
28. Universal Declaration of Human Rights, G.A. Res. 217 A (III), U.N. Doc. A/810 (Dec. 10, 1948).
29. Paul Voigt & Axel von dem Bussche, *THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE* (2017).
30. Kevin Werbach, *THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST* (2018).
31. Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017).
32. Dylan Yaga et al., *BLOCKCHAIN TECHNOLOGY OVERVIEW* (NIST Internal Rep. 8202, 2019).
33. Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 REGUL. & GOVERNANCE 505 (2018).
34. Dirk A. Zetsche, Ross P. Buckley, Douglas W. Arner & Linus Föhr, *The Rise of Decentralized Autonomous Organizations*, 6 J. FIN. REG. 257 (2020).
35. Zibin Zheng et al., *Blockchain Challenges and Opportunities: A Survey*, 14 INT'L J. WEB & GRID SERVS. 352 (2018).
36. Shoshana Zuboff, *THE AGE OF SURVEILLANCE CAPITALISM* (2019).
