# THE IMPACT OF EMERGING TECHNOLOGIES ON BUSINESS LAW CHALLENGES AND OPPORTUNITIES

Smiriti Michel Lakra, B.B.A. LL.B. (Hons), Bharath Institute of Law


## ABSTRACT

New technologies have transformed the world of work the way in which organizations operate develop and change and leadership management and professional. They have become an integral element of business, industry and common worldwide, driving the growth of the two most powerful forces in the global economy cyberspace and computer power. However, while they have brought with them foreknowable challenges for all organization, they are only the most being forerunners of yet more powerful and more radical technologies.

The potential impact of which few business leaders or academies really understand. This article examines these considers the immediate effects of emergent technologies on organization, notes the impact of these on traditional leadership management and business practices in the near future and suggests ways in which business leaders may look ahead to the effect of these new technologies on their organization and leadership and management practices in the future.

In the speculates about the likely impact of new technologies on humanity in the 21st Century with a warning about the possible dangers which these may bring. It also explores impact of emergent technologies on business law with emphasis on area like antitrust enforcement, data privacy, platform economies, ESG compliance and cross boarder M&A. It also pays close attention to issues of e-commerce regulations, blockchain in debt restructuring, digital asset insolvency green tech IP Defi, and algorithmic trading. Through the lens of the intersection of law and innovation.

Consider the future of work in an increasing automated world. These concerns linger despite the fact that the period before 2018 was characterized by exploring and implementing these options it is impossible not to be optimistic, while they were already in the past thanks to this development digitization continues to develop.


**Keywords:** Emerging technologies, artificial intelligence, cyberspace, computer power, technologies and challenges, digital revolution, traditional impact.

## INTRODUCTION

New technologies like artificial intelligence (AI), blockchain, big data and internet of thing (IOT) are revolutionizing the way businesses are radically altering how business operate. Although AI improves efficiency but possess legal concerns with the liability, bias and regulations. Blockchain technology with its decentralized and secure transactions complicates enforceability as well as fraud prevention, particularly related to smart contracts and digital assets.[1] Similarly, IOT devices that network ordinary things generate massive volumes of data that requires more enhanced features and laws that can address liability concerns resulting from misuse of data or malfunctioning devices.[2]

AI is stepping into the game for businesses by simplifying operations through automation, predicting trends with analytics, and helping with smarter decision making. But it also raises some tricky legal questions around accountability, algorithm bias, and how we manage oversight. For instance, when an AI makes a mistake or causes harm, who takes the blame? Is it the developer, the user, or the AI itself? This is still a hot topic for debate. Plus, many AI algorithms are pretty opaque, making it hard to figure out if they're fair and transparent.[3] On another hand, blockchain technology is shaking things up with its decentralized, secure way of keeping transaction records. It's changing finance, supply chains, and contracts through things like smart contracts and digital assets. But the same features that make blockchain so appealing also make legal agreements complex. There are a lot of questions about jurisdiction, whether contracts hold up, how to prevent fraud, and how to regulate digital currencies and tokens.[4]

Then there's big data analytics, which helps companies really understand what consumers want and keep up with market trends. This can lead to better decision-making that's more targeted and efficient. However, the way we gather, store, and use all that data brings up serious concerns about privacy and security. Businesses have to deal with tricky global regulations, like Europe's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), which set strict rules about how data can be used and how user consent is handled.

The Internet of Things (IoT) connects everyday devices to the internet, creating a wealth of real-time data. While this brings great innovation and convenience, it also opens the door to

[1] Kuner, *Transborder Data Flows* (2017).
[2] COM (2020) 825 final.
[3] UNCITRAL, U.N. Doc. A/CN.9/1043 (2021).
[4] OECD, *Gig Economy Report* (2021).

legal issues about data misuse, surveillance, and device failures. If something malfunctions or gets hacked, it could lead to serious problems like physical injuries or data breaches, complicating liability matters.

To wrap things up, these technologies are driving major changes in business, but they also come with a set of legal challenges that are constantly changing. It's critical that our regulatory frameworks keep pace with these advancements to ensure we have clear laws, protect consumers, and use technology ethically.

## ANTITRUST CHALLENGES AND GOVERNMENT INTERVENTION IN REGULATING BIG TECH'S MARKET DOMINANCE

With tech giants' behemoths holding unmatched clout the worlds regulators around the world are paying closer attention to anti-competitive behavior. The companies use their enormous market clout to stifle acts of self-preferencing favoring their own or allied services at the expense of others and predatory pricing suppressing competitors.[5] Dominance over vital digital infrastructure such as computer platforms and app stores, it also raises questions about fair competition and market access. Governments are also implementing new antitrust measures more frequently. These including stricter merger control requirements, regulatory investigations, even structural unbundling to contains this risk.[6]

To provide a level playing field in the digital economy, policymaker must strike a balance between enforcing competition and innovation, not stifling technological advancements while still ensuring fair level playing field in the digital economy. As tech giants gain more and more power in the digital economy, regulators around the world are stepping up their efforts to keep a closer eye on their possibly unfair practices. These companies often use their strong market positions to engage in tactics like **self-preferencing,**[7] which means they promote their own products over those from other companies, and **predatory pricing**, which involves pricing things so low that it pushes competitors out and makes it tough for new businesses to enter the market. Their grip on essential digital tools like app stores, cloud services, search engines, and advertising platforms raises big questions about **fair access to the market, barriers for new**

[5] Compl., *U.S. v. Google*, No. 1:20-cv-03010 (D.D.C. 2020).
[6] Finck, 4 *Eur. Data Prot. L. Rev.* 112 (2018).
[7] WEF, *Blockchain Regs Report* (2022).

**entrants,** and **options for consumers.**

## DATA PRIVACY, CYBERSECURITY AND LEGAL LIABILITIES IN A CROSS BORDER DIGITAL ECONOMY

As a Big data and AI analytics are used increasing difficulties companies are going to face in terms maintaining data privacy and cybersecurity as more big data and AI are being utilized. Data breaches, unauthorized usage and misuse of business data are being gathered, there is an increased threat of data breaches, unauthorized use misue of sensitive data.[8]

Regulations such as the General Data Protection Regulations (GDPR) in the European Union and California Consumer Privacy Act (CCPA) in the United States impose tight requirements for protecting data. Yet companies with operations spanning various jurisdictions experience challenges in having their data treatment practices conform to varying regulatory land space.

In additional as technology develop conventional legal system struggle to keep up with emerging threats and innovations and therefore require responsive and adoptive legal approaches to protect consumer rights and corporate interest.[9]

## REGULATORY AND LABOUR LAW CHALLENGES IN THE PLATFORM ECONOMY GIG WORKER CLASSIFICATION AND INTERMEDIARY LIABILITY

The rise of platform-based gig economies exemplified by companies such as Uber and Door Dash have precipitated major legal controversies regarding work classification and Labour rights. Conventional employment model categorizes workers and their employee are entitled to benefits and labor protections or independent contract who generally are not entitled. However, gig worker often falls into a legal gray area as they sell services through online platform but do not always neatly fit within traditional labor law categories.[10] This ambiguity has prompted may lawsuits and legislatives attempt to reclassify employment categories courts and policymaker have to weigh the adaptability that gig worker provide companies and workers against the necessity for equitable wages, benefits and job security.

[8] SEC Press Release (Feb. 2023).
[9] Law Comm'n, *Smart Contracts Advice* (2022).
[10] PwC, *ESG & Tech Risk* (2021).

Additionally intermediary liability regimes are changing in order to outline disputes in employment, safety directive it necessary that the regulatory platform follow these work paradigm changes with regulation.

## CORPORATE RESPONSIBILITY IN SUSTAINABLE BUSINESS PRACTICES ESG COMPLIANCE, GREENWASHING RISKS AND LEGAL MANDATES

Companies are being subjected to growing pressure regarding environmental, social and Governance (ESG) compliance from stakeholders demanding more corporate responsibility. Emerging technologies like AI and backchain are taking center stage in monitoring and authenticating ESG metrics,[11] allow Companies to enhance transparency in sustainability initiative. Misuse of these technologies however puts companies at huge legal risk.

To address these issues in ESG compliance is greenwashing where business overstate or make false claims about their environmental activities to lure investors and customers, not only does this mislead stakeholders, but it also welcomes regulatory intervention and reputational risk. To solve these problems, legal systems need to change to implement tighter accountability measure ensuring that business follow true and verifiable sustainability practices while avoiding manipulation of EGS information using new technologies.[12]

## CROSS BORDER MERGER AND ACQUISITION IN DIGITAL WORLD TAX IMPLICATION, FOREIGN INVESTMENT LAWS, REGULATORY APPROVALS

Meger and acquisition (M&A) in the digital space bring with legal complexities beyond traditional business traditional transactions. The growing importance of intellectual property (IP) in such transactions necessitates that firm undertake rigorous evaluations of digital assets such as proprietary algorithms, software enormous customer datastores. Sine the value of these intangible assets frequently paramount as their value often dictates the strategic feasibility of the deal. Cybersecurity threats also have a central place in digital M&A. purchasing a business with poor cybersecurity infrastructure can put the acquiring company risk of data breaches

[11] EDPB Guidelines 05/2020.
[12] EU AI Act Proposal, COM (2021) 206 final.

regulatory fines and reputational damage.[13] Hence, Cybersecurity due diligence is crucial to detect vulnerabilities and reduce possible liabilities prior to closing a deal.[14]

Regulatory scrutiny further complicates digital M&A competition Regulatory scrutiny further complicates digital M&A competition regulators across the globe are increasingly concerned with preventing monopolized practices and undue data concentration.[15] Firm have to navigate intricate antitrust rules, making sure that merger do not suppress competition or infringe on consumer protection regulations. Compliance with data protection, including the GDPR and CCPA is also important when acquiring firms that process personal data. Failure to comply can result in significant fines and legal battle.

Detary controls also come into play as digital M&A in sensitive area is affected as government make it difficult by placing national security review on foreign investments that seek to undermine major digital infrastructure.[16]

As opposed to conventional M&A where physical property plays a central role the intangible character assets require specialized legal knowledge. The procedure of due diligence needs to adopt to involve sophisticated valuation methods, strong contractual safeguard and compliance tactics adopted to digital market. Legal professionals need to foresee regulation development, evaluate risk associated with emerging technologies and design deals to survive increased scrutiny.

## THE CHANGING REGULATORY FRAMEWORK OF E-COMMERCE CONSUMER PROTECTION, FAIR TRADE PRACTICES AND DIGITAL TAXATION.

The swift growth of online commerce has prompted governments across the globe to introduce fresh regulations for consumer rights, product liability and fair-trade practices with online transactions increasingly dominating retail markets, organization need to maneuver intricate legal structures to meet changing legislation. Consumer protection laws now require transparency in pricing, refunds and data managements, pushing online market places to strengthen their compliance processes.

[13] EDPB Guidelines 05/2020.
[14] CJEU, *Schrems II*, Case C-311/18 (2020).
[15] UK Gov't, *AI Regulation White Paper* (2023).
[16] FTC, *AI and Algorithmic Fairness* (2021).

One of the most urgent issues in the online market is taxation, cross border e-commerce has generated in consistencies in tax regimes placing compliance pressures on businesses operating across several jurisdictions.[17]

Digital services taxes (DSTS) rules and changing OECD recommendation on global taxation oblige business to reconfigure their financial models to clear of legal exposure and penalties. The expansion of online market places and direct to consumer (DTC) business model make regulatory compliance even more challenging.[18] Market place has to ensure that third party vendors comply with fair trade law, product safety regulation and data privacy data.

Liability for counterfeit products and fraudulent transactions has emerged as a major concern leading to increased enforcement measure against platforms that are not able to regulate their vendors properly.

Furthermore, competition law is adopting to avert market dominance by giant e-commerce companies regulatory are also more critically examining anti- competitive behavior, including preferential treatment of in-house products and algorithmic price manipulation. Companies need to craft their operational strategies with compliance in mind to stay char of legal battle and regulatory penalties.

In this rapidly changing environment legal flexibility is essential. Business needs to have strong compliance system track legislative updates and exercise proactive risk management.

## BLOCKCHAIN IN DEBT RESTRUCTURING: THE USE OF SMART CONTRACTS FOR AUTOMATING DEBT REPAYMENT AND INSOLVENCY RESOLUTIONS.

Financial transaction and undergoing a significant transformation due to advent of blockchain technology which make them more automated transparent and efficient. The two most innovation use of the technology include debt restructuring and contract execution. In debt restructuring the primary use of blockchain can enhance repayment schedules, monitor compliance in real time and eliminate overhead.[19]

Smart contract has great potential. They are however held back legally in a bug way

[17] IMF, *Crypto Regulation* (2023).
[18] FATF, *Virtual Assets Guidance* (2021).
[19] ESMA, *DeFi Risk Statement* (2022).

enforceability is the major problem different legal jurisdiction does not accept them as legally binding agreements.[20] Additionally, these smart contracts are not clearly defined is most legal system. Thus, the parties that depends on their outcomes are at risk.

Another issue that arises is the question of jurisdiction because of their nature blockchain transactions are decentralized and they don't have a border. This make it difficult to identify the laws that need to be enforced.

Also, substantial risk involves fraud and coding error. Smart contract performs exactly as coded which contracts the traditional contracts in a flaw or malicious backchain were to be present in the software this could result in serious financial or legal consequence.[21] This is with very few avenues of redress under existing laws.

Taking into consideration the benefits of blockchain protection of legal integrity requires a shift in regulatory and legal system to evolve this would involve setting standards for the legality of smart contracts, creating efficient mechanisms for resolving disputes and updating insolvency and financial regulations to take into accounts block-based transaction.[22] By reinforcing these issues, the legal framework will adopt in financial markets, thus providing both innovation and protection.

The parties that depend on their outcomes are at risk. This is with very few avenues of redress under existing laws. By reinforcing these issues, the legal framework will adopt in financial markets, thus providing both innovation and protection. Additionally, these smart contracts are not clearly defined is most legal system. Thus, the parties that depends on their outcomes are at risk.

## DIGITAL ASSETS INSOLVENCY PROCEEDINGS: LEGAL CHALLENGES IN VALUING AND DISTRIBUTING CRYPTOCURRENCIES AND NFTS DURING BANKRUPTCY

The growing adoption of cryptocurrencies and non-fungible tokens (NFTs) has introduced complex challenges for insolvency law. As debtors increasingly hold digital assets, courts are faced with determining how these assets should be classified, valued, and distributed during

[20] BIS, *CBDC Legal Frameworks* (2023).
[21] IOSCO, *AI in Securities Regulation* (2021).
[22] UNCTAD, *Digital Economy Report* (2022).

bankruptcy proceedings. Unlike traditional financial instruments, digital assets are characterized by decentralization, high volatility, and legal ambiguity.[23] This paper explores the specific legal challenges associated with valuing and distributing cryptocurrencies and NFTs during insolvency proceedings.

## II. Valuation Challenges

### A. Volatility and Timing

One of the primary hurdles in valuing cryptocurrencies is their extreme price volatility. The value of assets such as Bitcoin or Ethereum can fluctuate dramatically within short timeframes. In bankruptcy, valuation often hinges on a specific point in time—commonly the petition date or the distribution date.[24] This creates potential inequities, as the value of the estate could drastically change during proceedings.

For example, in *In re Celsius Network LLC*, the court faced significant debate on whether to fix the value of crypto assets as of the petition date, when prices were lower, or closer to the distribution date, when markets had partially recovered. This decision affects the pro-rata share creditors ultimately receive. Courts lack clear statutory guidance, often relying on traditional equitable principles to navigate this digital frontier.[25]

### B. Lack of Centralized Pricing Standards

Unlike publicly traded stocks with transparent market values, cryptocurrencies often trade across numerous decentralized exchanges, each with different prices and liquidity. Courts and trustees must decide which market or method to use for valuation—spot price, volume-weighted average, oracles, or expert analysis. Each method has its limitations, and no uniform standard exists under bankruptcy law.

### C. Valuing NFTs

NFTs pose a unique valuation challenge because of their non-fungible nature. Their worth is highly subjective, often driven by artistic value, brand reputation, or market hype. NFTs may

[23] ABI, *Crypto and Bankruptcy Law Survey* (2023).
[24] Harvard Blockchain & Fin. Law, *NFT Valuation and IP Issues in Insolvency* (2023)
[25] IMF, *Crypto Assets and Financial Stability* (2023).

also include future royalty streams or licensing rights that are hard to quantify.[26] Additionally, the liquidity of NFTs is limited, and in the absence of a robust secondary market, determining "fair market value" can be speculative at best.

## III. Distribution Challenges

### A. Asset Classification and Ownership

Determining whether digital assets are part of the bankruptcy estate under 11 U.S.C. § 541 depends on asset control and contractual arrangements. In *Voyager Digital Holdings, Inc.*, the court distinguished between custodial and proprietary crypto holdings. When crypto is held in a custodial structure, it may be considered customer property, not estate property, which affects creditor hierarchy.

Ownership of NFTs is even murkier. While a buyer may own the token, the actual rights such as IP licenses are often governed by off-chain terms.[27] In bankruptcy, it's unclear whether such off-chain rights are enforceable or transferable, complicating asset distribution.

### B. Smart Contracts and Auto-Royalties

Many NFTs are governed by smart contracts that enforce royalties upon resale. In bankruptcy, such obligations could conflict with court-approved distribution plans. The legal status of smart contracts and whether courts can override them remains a gray area, raising questions about enforceability and creditor priorities.

### C. Tracing and Asset Recovery

Blockchain's transparent ledger allows asset tracing, but practical recovery is not always simple. Issues arise when assets are stored in anonymous wallets, mixed through privacy protocols, or moved to decentralized platforms. Trustees may need to engage forensic blockchain analysts, increasing administrative costs and delaying distributions.

### Jurisdictional and Regulatory Gaps

Cryptocurrencies and NFTs often transcend jurisdictions. Insolvency cases involving debtors

[26] Norton Rose Fulbright, *Crypto Claims in Bankruptcy* (2023).
[27] Stanford J. Blockchain L. & Pol'y, *Valuation of Digital Assets in Liquidation* (2022).

with digital assets on global exchanges raise issues of asset situs and conflict of laws. For example, whether a wallet on a non-U.S. exchange falls under U.S. jurisdiction is still debated. Moreover, inconsistent treatment of digital assets by agencies—classified as property (IRS), securities (SEC), or commodities (CFTC)—adds complexity.

## Conclusion

The rise of cryptocurrencies and NFTs has forced bankruptcy courts to confront uncharted legal territory. From valuation volatility to ownership ambiguity, digital assets do not fit neatly within existing insolvency frameworks. Addressing these legal challenges requires both doctrinal clarity and practical reform. As digital assets continue to permeate financial systems, the development of consistent legal standards for their treatment in bankruptcy is not only necessary but urgent.