

Stanford – Vienna Transatlantic Technology Law Forum



A joint initiative of Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 113

A Comparative Analysis of Blockchain and Competition Law in the European Union and the United States: Decentralization, Data Accumulation, and Collusion

Charles Ho Wang Mak

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum http://ttlf.stanford.edu

Stanford Law School Crown Quadrangle 559 Nathan Abbott Way Stanford, CA 94305-8610 University of Vienna School of Law Department of Business Law Schottenbastei 10-16 1010 Vienna, Austria

About the Author

Charles Ho Wang Mak is a Lecturer in Law at Robert Gordon University, a PhD Candidate in law at the University of Glasgow, a Fellow of the Stanford-Vienna Transatlantic Technology Law Forum at Stanford Law School, a Fellow of the Centre for Chinese and Comparative Law at the City University of Hong Kong, an Honorary Fellow of the Asian Institute of International Financial Law at the University of Hong Kong, a Research Affiliate at SovereigNet at The Fletcher School, Tufts University, and a Research Associate at China, Law and Development Project at the University of Oxford. E-mail: charleshwmak@gmail.com.

General Note about the Content

This paper was presented at the Symposium 'Ensuring Digital Justice: Tackling Technology-Enhanced Economic Crime' at the University of Liverpool (United Kingdom).

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:

Charles Ho Wang Mak, A Comparative Analysis of Blockchain and Competition Law in the European Union and the United States: Decentralization, Data Accumulation, and Collusion, Stanford-Vienna TTLF Working Paper No. 113, http://ttlf.stanford.edu.

Copyright

© 2024 Charles Ho Wang Mak

Abstract

This paper scrutinizes blockchain and competition law in the European Union ('EU') and the United States ('US'), investigating the multi-jurisdictional challenges caused by this emerging technology. The paper argues that while blockchain technology can potentially increase competition in certain markets, it poses new antitrust concerns requiring careful consideration. The paper argues that while blockchain technology can potentially increase competition in certain markets, it poses new antitrust concerns requiring careful consideration.

This paper explores the potential for blockchain technology to enable collusion, cartel formation, and monopolization through data aggregation. Additionally, it delves into the difficulties of applying competition law in a decentralized setting where conventional methods might be inadequate. To address these problems, the paper puts forth several recommendations. First, it proposes fostering collaboration between blockchain developers and competition regulators to address antitrust concerns during the initial stages of blockchain projects. Second, it advises competition authorities to consider adopting blockchain technology for enforcement purposes, particularly in data gathering and analysis. Finally, the paper encourages competition authorities to collaborate and establish a common understanding of the opportunities and challenges posed by blockchain technology, through continuous dialogue and cooperation on a transatlantic scale.

In summary, this paper highlights the significance of a collaborative strategy in tackling blockchain-related challenges and competition law within an EU-US comparative framework. Offering practical guidance to policymakers and practitioners on managing competition law concerns arising from blockchain technology, this paper contributes to the ongoing international law dialogue. The expected outcome of this project is to equip policymakers and practitioners with pragmatic guidance to address competition law challenges associated with blockchain technology.

Table of Contents

1. Introduction	1
2. Blockchain Technology: Opportunities and Challenges	3
	7
	11
	14
6. Addressing the Challenges: Recommendations	16
7. Conclusion	19

1. Introduction

In the rapidly evolving digital economy, blockchain technology emerges as a beacon of innovation, offering unprecedented opportunities for efficiency, transparency, and security. Such a technology has become a transformative force in various sectors, promising data integrity, security. Its integration into various sectors presents a paradigm shift in how data is stored, transactions are executed, and value is transferred. However, the disruptive nature of blockchain technology also presents complex challenges for competition law frameworks worldwide. This paper explores the sophisticated landscape of blockchain within the field of

_

¹ For a more in-depth analysis of the socio-economic impact of blockchain technology, *see* Fred Steinmetz, Lennart Ante, and Ingo Fiedler, *Blockchain and the Digital Economy: The Socio-Economic Impact of Blockchain Technology* (Agenda Publishing 2020).

competition law across multiple jurisdictions, with a keen focus on the European Union ('EU') and the United States ('US').²

The objective of this paper is twofold. Firstly, it aims to dissect and compare the approaches taken by the EU and the US in integrating blockchain technology within their respective legal frameworks for competition law. The EU's proactive stance, characterized by its early regulatory interventions and legislative initiatives, contrasts sharply with the US's more reactive approach, grounded in the application of existing antitrust laws to new blockchain-related challenges. This comparative analysis seeks to uncover the strengths and potential pitfalls of each approach, providing insights into how different regulatory environments adapt to technological advancements. The importance of this paper extends beyond academic interest, touching upon the very core of global economic competition and the future of technological innovation. As blockchain technology continues to permeate various industries, understanding its implications for competition law becomes crucial. This paper sheds light on the delicate balance regulators must strike between fostering innovation and preventing anticompetitive practices that could hinder the growth and widespread adoption of blockchain technology.

_

² Choosing the EU and US as focal points for the comparative analysis is not arbitrary; rather, it is grounded in their roles as pioneers and leading regulators in the realm of competition law. The EU, with its proactive regulatory approach, offers a model of governance that anticipates and shapes the digital marketplace through comprehensive frameworks like the Treaty on the Functioning of the European Union (specifically, Articles 101 and 102), the Digital Markets Act and the General Data Protection Regulation. This contrasts with the US, where a more reactive application of antitrust laws, such as the Clayton Antitrust Act, seeks to address blockchain's challenges within the established paradigms of market competition and consumer protection. This comparative analysis is vital for several reasons. First, it highlights the diverse methodologies and regulatory philosophies adopted by two of the world's largest economies in response to the same technological innovation. Second, it provides valuable insights into the effectiveness of different regulatory approaches in fostering innovation while ensuring market fairness and consumer protection. Lastly, it underscores the global nature of blockchain technology and the need for a coherent, international regulatory framework to navigate the complex landscape of digital competition law effectively.

This paper begins with a contextual background that provides a brief introduction to blockchain technology, highlighting its significance in today's digital economy. The paper then turns into a detailed comparative analysis of the EU and US legal frameworks, examining how each region addresses the unique challenges posed by blockchain. The conclusion synthesizes the insights gained from this analysis, emphasizing the need for regulatory agility and international cooperation to ensure that blockchain technology can flourish within a legal framework that promotes competition and innovation.

2. Blockchain Technology: Opportunities and Challenges

Blockchain technology, in its essence, represents a paradigm shift in how information is recorded, stored, and shared across a digital landscape. Described as a 'structured collection of information', blockchain serves as a sophisticated, secure database or ledger technology that has captivated the interest of industries worldwide due to its promise of data integrity, identity authentication, and a significant reduction in the need for intermediary verification processes.³

At the core of blockchain technology lies the principle of decentralization.⁴ Unlike traditional databases that centralize data storage, blockchain distributes its data across a network, utilizing

³ Jean Bacon, Johan David Michels, Christopher Millard, and Jatinder Singh, 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' (2018) 25 (1) Richmond Journal of Law and Technology 1, 6; Pierluigi Cuccuru, 'Beyond Bitcoin: An Early Overview on Smart Contracts' (2017) 25 International Journal of Law and Information Technology 179; and Nathan Fulmer, 'Exploring the Legal Issues of Blockchain Applications' (2019) 52(1) Akron Law Review 161 at 164.

⁴ See Vitalik Buterin, 'On Public and Private Blockchains' Ethereum Foundation Blog (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed 22 August 2023) where

encryption and consensus protocols to ensure the immutability and transparency of records.⁵ This is achieved through cryptographic hashes, a unique digital fingerprint for each block, and public-key cryptography, which secures transactions and verifies the identity of participants. Blockchain networks can broadly be categorized into two types: centralized and decentralized (often referred to as distributed ledger technology).⁶ Centralized blockchains, typically managed by a single entity, offer efficiency and control, allowing for flexible rule changes and transaction reversals. These blockchains often find utility in institutional settings where privacy, control, and cost-effectiveness are prioritized. Conversely, decentralized blockchains distribute data storage across a peer-to-peer network, making unilateral alterations exceedingly difficult and enhancing security against data tampering. This form of blockchain, exemplified by Bitcoin and other cryptocurrencies, provides transparency and resilience against centralized points of failure but often at a higher operational cost due to the energy-intensive consensus mechanisms required.

The rise of blockchain technology signifies a new competitive era in numerous sectors such as finance, healthcare, and other fields that require efficient data management.⁷ Blockchain technology can help new players to enter markets, which were traditionally controlled by

_

the author, the founder of ETHEREUM, identifies three different types of blockchains namely: public, consortium and fully private blockchains.

⁵ Subhadeep Mandal, Arpan Kumar Kar, and Shivam Gupta, 'Blockchain-Based Application Security Versus Centralized and Distributed Data Management Systems – A Comparative Study' in SK Sharma, YK Dwivedi, B Metri, B Lal and A Elbanna (eds), *Transfer, Diffusion and Adoption of Next-Generation Digital Technologies* (IFIP Advances in Information and Communication Technology, vol 697, Springer, Cham 2024).

⁶ Jean Bacon, Johan David Michels, Christopher Millard, and Jatinder Singh, 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' (2018) 25 (1) Richmond Journal of Law and Technology 1.

⁷ For the implications of blockchain to financial sectors, *see* Petar Radanliev, 'The Rise and Fall of Cryptocurrencies: Defining the Economic and Social Values of Blockchain Technologies, Assessing the Opportunities, and Defining the Financial and Cybersecurity Risks of the Metaverse' (2024) 10 *Financial Innovation* 1.

entities that had substantial control over central databases or ledgers. In the finance sector, blockchain's impact is particularly profound. Traditionally, this industry has been under the purview of large banks and financial institutions, which act as intermediaries in transactions, thereby controlling access to financial services and information. However, blockchain introduces a decentralized ledger system, enabling peer-to-peer transactions without the need for such intermediaries. For example, cryptocurrencies like Bitcoin and Ethereum, built on blockchain technology, offer a new way of conducting transactions that are open, transparent, and accessible to anyone with internet access, challenging traditional banking's hegemony. The blockchain technology has brought about significant advancements that offer new opportunities for decentralisation, improved data analytics, and the integration of internet of things, leading to the emergence of Web 3.0.8 By embracing these technologies, as *Radanliev* pointed, the market can move towards a future where assets are used as services, supported by streamlined processes and trustworthy exchanges facilitated by the blockchain.9 Acknowledging the transformative role blockchain technology plays in finance, where it dismantles traditional barriers and fosters an inclusive transactional environment, blockchain has broader implications. This paradigm shift is not confined to financial transactions alone. In sectors such as supply chain management, blockchain allows real-time tracking of goods and automatic execution of contracts. 10 This helps streamline operations and reduces the reliance on intermediaries. This not only enhances efficiency but also opens up the market to smaller participants who can now compete on equal footing with established players. Furthermore, the immutable nature of blockchain records can revolutionize intellectual property rights management, providing artists and creators with a robust mechanism to assert ownership and

⁸ ibid, 14.

⁹ ibid.

¹⁰ See Muhammad Shujaat Mubarik and Muhammad Shahbaz (eds), Blockchain Driven Supply Chain Management: A Multi-dimensional Perspective (1st edn, Springer Singapore 2023).

receive fair compensation, thus fostering a more vibrant and diverse marketplace of ideas and products.¹¹

While blockchain technology offers promising avenues for enhancing market competition, it is not without its antitrust concerns. *Arcelus, Yenikomshian*, and *Nocera* highlight that, while blockchain platforms may offer efficiency gains through collaboration, they also raise concerns about anticompetitive outcomes due to their potential to facilitate collusion among firms, such as price-fixing and bid-rigging, by making sensitive data like price readily accessible to competitors. This accessibility could enable cartel members to monitor adherence to agreed-upon terms and tacitly cooperate in oligopolistic markets, thus posing significant risks of anticompetitive practices. Further, the decentralized nature of blockchain, particularly in public networks, could potentially lead to the emergence of new forms of cartels or coordinated market behaviors that are difficult to detect and regulate. Participants might collude, leveraging smart contracts to enforce agreements that could restrict competition or manipulate market conditions. Moreover, the concentration of mining power in a few entities, a phenomenon known as 'mining pools' in the cryptocurrency world, raises questions about market power and the potential for monopolistic control over the blockchain network. Such centralization of power contradicts the foundational ethos of blockchain as a decentralized and democratic

¹¹ See Atharv Chandratre and Abhinav Pathak, Blockchain Based Intellectual Property Management (10 December 2019) SSRN https://ssrn.com/abstract=3800734; Severin Bonnet and Frank Teuteberg, 'Impact of Blockchain and Distributed Ledger Technology for the Management, Protection, Enforcement and Monetization of Intellectual Property: A Systematic Literature Review' (2023) 21 Information Systems and e-Business Management 229; and Michèle Finck and Valentina Moscon, 'Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0' (2019) 50 IIC - International Review of Intellectual Property and Competition Law 77.

¹² Almudena Arcelus, Mihran Yenikomshian, and Noemi Nocera, 'Mitigating Antitrust Concerns When Competitors Share Data Using Blockchain Technology' (2021) 34 Harvard Journal of Law & Technology 1, 5; and Thibault Shrepel, 'Collusion by Blockchain and Smart Contracts', (2019) 33 Harvard Journal of Law & Technology 1.

¹³ ibid.

technology platform. For instance, the Blockchain Technology and Competition Policy - Issues paper by the *Organisation for Economic Co-operation and Development* suggests that in markets where a private, permissioned blockchain becomes essential for competition, there is a risk that control over network access could lead to exclusionary practices. ¹⁴ If dominant market players, who also administer the blockchain, possess the authority to grant access, they might be incentivized to block new entrants, effectively hindering their ability to compete without access to this crucial technology. ¹⁵

Additionally, the integration of blockchain technology in critical infrastructure sectors could lead to interoperability issues, where dominant players might enforce standards that sideline competitors, creating barriers to entry and stifling innovation. The role of governance in decentralized networks also poses antitrust challenges, as decision-making power concerning protocol changes or dispute resolutions could become concentrated among a select few, undermining the equitable and open nature of the network.

3. Competition Law in the European Union

The EU boasts a sophisticated and inclusive framework for competition law, meticulously crafted to maintain fair competition within its internal market.¹⁶ This legal structure not only fosters a level playing field for businesses but also aims to protect consumers by promoting

¹⁴ Organisation for Economic Co-operation and Development, *Blockchain Technology and Competition Policy, Issues Paper by the Secretariat* (2018) https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf, 7.

¹⁶ See Konstantinos Stylianou and Marios Iacovides, 'The Goals of EU Competition Law: A Comprehensive Empirical Investigation' (2022) 42(4) Legal Studies 620.

innovation, enhancing efficiency, and ensuring lower prices.¹⁷ The relevance of the EU's competition law extends across various sectors, notably embracing the challenges and possibilities presented by emergent technologies such as blockchain.¹⁸ This expansive approach underscores the EU's commitment to adapting its regulatory environment to the evolving dynamics of the global market.

Central to the EU's competition law are Articles 101 and 102 of the Treaty on the Functioning of the EU ('TFEU'), which together lay the foundation for most competition policies within the bloc. 19 Article 101 of the TFEU is designed to safeguard the internal market against any agreements or practices between companies that might impede competition. This provision targets practices such as cartels, price fixing, production limitations, and the partitioning of markets or customers. 20 At first glance, blockchain technology could seem to provide a conducive environment for collusion. However, for the application of Article 101(1) of the TFEU to be considered, specific criteria must be fulfilled. 21 These include the demonstration of an agreement between undertakings, a decision by an association of undertakings, or a concerted practice that, whether by intent or effect, restricts competition within the common market. On the other hand, Article 102 of the TFEU distinctly addresses the conduct of entities occupying a dominant stance within the marketplace. 22 It is specifically designed to prevent the exploitation of such a position in manners detrimental to the competitive environment.

¹⁷ Rex Ahdar, 'Consumers, redistribution of income and the purpose of competition law' (2002) 23 European Competition Law Review 341, 349–351.

¹⁸ For detail analysis of the complicative of blockchain and the EU competition law, *see* Marixenia Davilla, 'Unravelling the Complexity of Blockchain and EU Competition Law' (2022) 13 (6) Journal of European Competition Law & Practice 387.

¹⁹ Consolidated version of the Treaty on the Functioning of the European Union ('TFEU') [2012] OJ C 326/1.

²⁰ ibid.

²¹ ibid.

²² ibid.

Examples of such exploitative practices include predatory pricing, exclusive agreements, or product tying, all of which could undermine market competition. Furthermore, in the realm of emerging technologies like blockchain, there arises a potential for dominance abuse. This can manifest through actions that either directly impair the functionality and competitive edge of the blockchain technology itself or limit the access of competitors to crucial blockchain networks. Notably, established operators in sectors such as banking, transportation, and insurance might resort to strategies aimed at obstructing blockchain integration. These strategies could involve lobbying for regulatory hindrances, artificially escalating costs for competitors, obstructing cryptocurrency transactions, or initiating baseless legal challenges. Should these entities be adjudged as holding a dominant market position, such conduct may be interpreted as an infringement of Article 102 of the TFEU, signaling a breach of EU competition regulations.²³ This regulatory perspective underscores the necessity for vigilant oversight to safeguard against abuses of market dominance, thereby ensuring a balanced and competitive economic ecosystem.

The European Commission, serving as the executive arm of the EU, is vested with the authority to review and assess mergers, with the power to either approve, impose conditions upon, or block mergers that pose a threat to competitive markets. The enforcement of these laws is a concerted effort involving both the European Commission and national competition authorities within EU member states. The Commission plays a leading role, equipped with the power to conduct investigations, impose fines, and mandate companies to alter or cease practices deemed anti-competitive. National authorities complement this framework by applying EU

9

²³ ibid.

competition law at the national level, ensuring a comprehensive enforcement landscape throughout the EU.²⁴

The intersection of EU competition law and blockchain technology introduces a complex array of challenges and opportunities. Blockchain's intrinsic characteristics—such as decentralization, transparency, and immutability—present novel scenarios for the application of competition law. For instance, the decentralized nature of blockchain can disrupt traditional market structures, potentially altering the dynamics of market power and competition. A critical concern arises when a small number of participants gain significant control over a blockchain network's computational resources. Such concentration can lead to the risk of these entities manipulating the network to their advantage, thereby stifling competition. In this context, Article 102 of the TFEU may be invoked to address instances where such dominance is abused.²⁵

Furthermore, the transparent nature of blockchain transactions might inadvertently facilitate anti-competitive collusion. Participants within a blockchain network could theoretically leverage the visibility of transaction data to coordinate strategies that restrict competition, such as price-fixing or market sharing. Here, Article 101 of the TFEU becomes relevant, providing a legal basis to tackle such collusive behaviors. The European Commission has acknowledged these challenges, indicating a willingness to adapt its competition policy framework to address the nuances of blockchain technology.²⁶ This includes exploring how decentralization affects market dynamics and assessing the competitive implications of the technology's transparency.

²⁴ For detail analysis of the EU competition law enforcement, *see* Jurgita Malinauskaite, *Harmonisation of EU Competition Law Enforcement* (1st edn, Springer Cham 2020).

²⁵ Consolidated version of the Treaty on the Functioning of the European Union ('TFEU') [2012] OJ C 326/1.

²⁶ ibid.

Moreover, the Commission's interest in promoting innovation and supporting the digital economy suggests a balanced approach to regulation—one that prevents anti-competitive practices without stifling the growth and development of blockchain technology.

To effectively navigate these challenges, the Commission, along with national authorities, must foster a deep understanding of blockchain technology and its implications for competition. This might involve engaging with stakeholders from various sectors, conducting market studies, and developing guidelines that clarify how competition law applies to blockchain-based activities. There have been several instances where the EU's competition law has been applied to digital markets, providing valuable lessons for its application to blockchain. For example, the European Commission's investigations into tech giants like Google and Facebook have highlighted the challenges of applying competition law to digital platforms. In the context of blockchain, one hypothetical scenario could involve a consortium of companies that establish a private blockchain network for supply chain management. If the consortium were to use its control over the network to exclude competitors or coordinate prices, this could potentially constitute an anti-competitive agreement under Article 101 of the TFEU.²⁷

4. Competition Law in the United States

The US has developed a comprehensive legal framework to govern competition, known as antitrust law.²⁸ This framework aims to ensure fair competition and to prevent anti-competitive behavior across all sectors of the economy, including innovative and rapidly evolving areas

²⁷ ibid.

²⁸ See Einer Elhauge, United States Antitrust Law and Economics (4th edn, Foundation Press 2021).

such as blockchain technology. At the core of US antitrust law are three important statutes: The Sherman Antitrust Act of 1890, the Clayton Antitrust Act of 1914, and the Federal Trade Commission ('FTC') Act of 1914.²⁹ Together, these acts prohibit a range of anti-competitive activities, including monopolistic practices, unfair mergers, and other behaviors that harm competition and consumers.³⁰

The Sherman Antitrust Act of 1890 stands as the foundational pillar of US antitrust law, delineating two principal categories of anti-competitive behavior: trade-restraining agreements among competitors, as outlined in Section 1, and monopolistic or monopolization attempts by single entities, covered under Section 2. Characterized by its expansive and adaptable language, the Act has proven itself remarkably resilient, capable of addressing the intricacies and challenges posed by evolving market landscapes. This adaptability is particularly pertinent in the context of digital and decentralized technologies, including blockchain. In the blockchain sphere, as mentioned above, antitrust concerns might emerge through collusive arrangements among participants in a blockchain network, potentially restricting entry or setting standards that unfairly disadvantage competitors. Similarly, a dominant entity's use of blockchain technology could raise issues under Section 2, especially if it employs the technology in a manner that excludes competitors or controls a critical blockchain infrastructure, thereby attempting to monopolize the market. The Act's flexibility allows it to be applied to these modern contexts, ensuring that its enduring principles can be interpreted to prevent anticompetitive practices even in sectors as innovative and dynamic as blockchain. This ensures that the Sherman Antitrust Act of 1890 remains a vital tool in safeguarding market

²⁹ William H. Rooney and Timothy G. Fleming, 'Time For A New Sherman Act? The Debate On Antitrust Reform In Historical Perspective' (2022) Columbia Business Law Review 1, 2.

³⁰ ibid.

competitiveness and consumer welfare in the face of new technological advances, by addressing both overt and nuanced forms of antitrust behavior within these cutting-edge domains.

Enacted in 1914, the Clayton Antitrust Act of 1914 supplements the Sherman Antitrust Act of 1890 by addressing specific practices that could lead to anti-competitive effects. Notably, it focuses on mergers and acquisitions that significantly lessen competition, as well as certain behaviors that could lead to monopolies. The Act also prohibits the practice of interlocking directorates, where the same individuals serve as directors of competing companies, potentially leading to anti-competitive collusion.

The FTC Act of 1914, established the FTC and broadened the scope of US antitrust law to include unfair methods of competition, as well as unfair or deceptive acts or practices affecting commerce. This Act allows the FTC to act against a wide array of practices that harm competition or consumers, even if they do not fit neatly into the categories prohibited by the Sherman Antitrust Act of 1890 or Clayton Antitrust Act of 1914. The enforcement of US antitrust laws is primarily the responsibility of two federal agencies: the FTC and the Department of Justice ('DOJ'). While both agencies have the authority to enforce antitrust laws, they have different focuses. The FTC primarily oversees civil enforcement, especially concerning practices that harm the competitive process or consumers. The DOJ, on the other hand, handles both civil and criminal enforcement, focusing on agreements and conduct that restrict competition, such as cartels and monopolistic practices.

The application of antitrust laws to digital markets offers valuable insights for addressing blockchain technology. Investigations into companies like Google and Apple by the DOJ have

underscored the complexities of applying antitrust principles in digital contexts, where market power can be subtle and competition dynamics are different from traditional markets. Considering hypothetical scenarios, such as a consortium of companies using a private blockchain to manage supply chains, can illustrate potential antitrust issues. If such a consortium were to exclude competitors or coordinate prices through its control of the blockchain, it could face scrutiny under the Sherman Antitrust Act of 1890 for anti-competitive agreements.

5. Comparative Analysis: European Union vs United States

The EU and the US represent two of the most significant and sophisticated legal jurisdictions in the sphere of competition law. Their respective legal frameworks, although converging towards the common goal of maintaining fair competition and fostering innovation, manifest distinct characteristics, reflective of diverse legal traditions and policy priorities. This comparative analysis illuminates the similarities and differences between EU and US approaches to competition law, examining the implications for blockchain innovation and the broader legal and economic landscapes. At their core, both the EU and US regimes share a foundational principle: the prohibition of anti-competitive practices to protect consumer welfare and promote efficient markets. The EU's TFEU (Articles 101 and 102) and the US's Sherman Antitrust Act of 1890 (Sections 1 and 2) are testament to this shared value. Both jurisdictions recognise the need to curb agreements that restrict competition, whether these are cartels in the EU or collusive restraints in the US, and both target abuse of dominant market positions. The enforcement structures in both jurisdictions are also similar, with centralised authorities — the European Commission in the EU and the FTC and DOJ in the US — equipped

with investigative and punitive powers. Mergers and acquisitions undergo rigorous scrutiny in both territories to forestall market concentration that could hamper competition.

While the underlying objectives are aligned, the EU and US diverge in their approach and focus. The EU framework, particularly under Article 101 of the TFEU, tends to be more formalistic, with certain types of agreements being almost automatically considered restrictive of competition. The US approach under the Sherman Antitrust Act of 1890 is more pragmatic, employing a rule of reason analysis that considers the overall impact of an agreement on competition. Furthermore, the EU's approach is often influenced by broader policy objectives, such as market integration and social welfare, while US antitrust law prioritises economic efficiency and consumer welfare, typically interpreted through price effects. The EU is also more predisposed towards regulatory interventions, while the US often favours market-based solutions unless there is clear and substantial harm to competition. The concept of market dominance is treated differently as well. In the EU, possessing a dominant market position is closely monitored and regulated, whereas, in the US, it is the abuse of such dominance, rather than its mere existence, that attracts legal sanction. This distinction reveals a variance in tolerance for market concentration provided that consumer benefits can be demonstrated.

Blockchain technology, by virtue of its decentralised and transparent nature, tests the boundaries of existing competition law. Both the EU and US recognise the transformative potential of blockchain but approach it differently. The EU's precautionary principle could lead to a more stringent application of competition rules to blockchain networks, especially where dominant positions or anti-competitive agreements are suspected. In contrast, the US may allow greater leeway for blockchain evolution under its more permissive attitude towards market dominance and innovation incentives, intervening when clear anti-competitive

behaviour emerges. Both jurisdictions must grapple with the reality that blockchain's transparency could inadvertently enable collusion, yet also appreciate that the decentralisation aspect may inherently resist monopolistic structures. Therefore, while the EU might focus on how blockchain consortia could facilitate anti-competitive agreements, the US might scrutinise such consortia for exclusionary practices that amount to an abuse of market power. The differences in competition law between the EU and US have substantial legal and economic implications. The EU's more regulatory approach may result in higher compliance costs for blockchain enterprises operating within its borders, possibly slowing innovation. Conversely, the US's focus on economic efficiency might promote a more rapid integration of blockchain technologies but could risk insufficient oversight of anti-competitive practices.

Economically, the EU's stance might preserve traditional market structures longer, potentially allowing for a more gradual adaptation to blockchain innovations. The US's approach may facilitate a swifter economic transformation, but with the risk of market distortions if blockchain networks become concentrated or abused. The choice of legal regime under which a blockchain initiative is developed could shape its architecture and governance. Developers may prefer the US's more liberal regime for innovative freedom, but they might value the EU's approach for greater legal certainty, particularly in cross-border blockchain applications.

6. Addressing the Challenges: Recommendations

As the advent of blockchain technology reshapes economic landscapes and presents novel challenges to established legal frameworks, regulatory authorities in both the EU and the US are tasked with safeguarding competitive markets without stifling innovation. Proactive

strategies and international cooperation will be instrumental in achieving these ends.³¹ Regulatory bodies should seek a balance between oversight and fostering innovation, engaging with blockchain developers from the nascent stages of technological development. A multistakeholder approach, involving regulators, developers, and industry experts, is imperative to create an environment where potential competition issues can be identified early and addressed efficiently. This could take the form of regulatory sandboxes, where developers can test new blockchain applications in a controlled environment under the watchful eye of competition authorities. Such initiatives would enable regulators to assess the implications of blockchain in real-time, granting them a nuanced understanding without prematurely imposing restrictive regulations.

Avenues for continuous education and dialogue between developers and regulators must be established. Workshops, symposia, and collaborative working groups can serve as platforms for knowledge exchange, ensuring that regulators remain well-informed about technological advancements and developers gain insight into competition law requirements. This bilateral exchange is essential; regulators will understand the technical possibilities and constraints of blockchain, while developers will be cognisant of the legal and competitive contexts within which they operate. Guidance and regulatory clarity are also vital. Authorities should strive to provide clear guidelines that articulate how competition law applies to blockchain activities. This includes defining what constitutes anti-competitive behaviour in the blockchain space and setting out the parameters for lawful collaboration between competing entities within a blockchain network.

³¹ For other sorts of recommendations, see Almudena Arcelus, Mihran Yenikomshian, and Noemi Nocera, 'Mitigating Antitrust Concerns When Competitors Share Data Using Blockchain Technology' (2021) 34 Harvard Journal of Law & Technology 1, 6-7.

Competition authorities can harness blockchain technology to enhance their enforcement capabilities. Blockchain's attributes of immutability and transparency could prove invaluable in monitoring and recording market activities, thereby aiding in the detection and investigation of anti-competitive practices. For instance, a blockchain-based registry for company mergers and acquisitions could provide a transparent and tamper-proof record of corporate transactions, simplifying the review process for potential competition concerns. Smart contracts — self-executing contracts with the terms of the agreement directly written into code — could also be utilised by competition authorities. These could be programmed to report and act upon anti-competitive behaviours, such as price-fixing, in real-time. Moreover, competition authorities could leverage blockchain to create a secure, decentralised database of decisions and precedents, improving consistency in enforcement and accessibility for stakeholders.

Given the global nature of blockchain technology and the significant influence of EU and US markets, transatlantic cooperation is indispensable. Joint initiatives could include the formation of a transatlantic working group dedicated to blockchain and competition law. This group would be tasked with harmonising regulatory approaches to ensure a consistent application of competition law to blockchain initiatives that span both jurisdictions. Regular dialogue between the European Commission and US competition authorities, such as the FTC and the DOJ, would facilitate the sharing of best practices and insights. Cooperation on investigations involving multinational blockchain consortia or networks could prevent jurisdictional conflicts and ensure a coordinated approach to enforcement. The EU and US could also benefit from aligning their technological standards and interoperability requirements for blockchain. This alignment could help in the creation of a seamless environment for blockchain applications, which, in turn, would support a more integrated and competitive market. Training programs,

exchange schemes for regulatory staff, and joint research initiatives could further bolster this transatlantic partnership. Furthermore, the EU and US could jointly develop frameworks to address new forms of anti-competitive behaviour that blockchain may enable, such as algorithmic collusion. By collaborating on policy development and enforcement strategies, both entities can ensure that their respective markets remain competitive and fair, while also setting a global standard for other jurisdictions to follow.

7. Conclusion

In conclusion, the analysis of competition law in the EU and US revealed divergent regulatory philosophies and enforcement strategies. The EU's proactive regulatory stance is characterized by a comprehensive legal framework that anticipates digital market challenges. Conversely, the US adopts a more reactive approach, relying on existing antitrust laws to address emerging challenges posed by blockchain technologies. This comparative lens highlighted the strengths and weaknesses of each approach, shedding light on the necessity for regulatory agility and international cooperation in the face of rapid technological advancements.

There are numerous practical recommendations for policymakers and regulators tasked with overseeing blockchain technology within competitive markets. Firstly, there is a pressing need for a balanced regulatory approach that encourages innovation while safeguarding against anti-competitive practices. Regulatory sandboxes and multi-stakeholder dialogue can provide valuable insights into the practical applications of blockchain, enabling regulators to formulate nuanced policies that reflect the technology's complexities. Moreover, competition authorities should leverage blockchain technology to enhance their enforcement capabilities, utilizing its

transparency and immutability features to detect and investigate anti-competitive behaviors. This includes the development of blockchain-based registries for corporate transactions and smart contracts to monitor compliance with competition law. Transatlantic cooperation between the EU and US is paramount in harmonizing regulatory approaches and ensuring a consistent application of competition law to blockchain initiatives. Joint working groups and regular dialogue can facilitate the sharing of best practices and foster a coordinated approach to investigating multinational blockchain consortia or networks.

The dynamic interplay between blockchain technology and competition law opens up several avenues for further research and investigation. Future studies could explore the impact of blockchain on specific industries, examining how decentralized ledger technology reshapes market structures and competitive dynamics in sectors such as finance, supply chain management, and intellectual property rights. Additionally, research into the legal and economic implications of different blockchain architectures (for example, public versus private blockchains) could provide deeper insights into their potential antitrust concerns. Another promising area of research involves the examination of informal regulatory mechanisms and their effectiveness in governing blockchain networks. This includes the role of consensus protocols, smart contracts, and decentralized autonomous organizations in facilitating self-regulation and compliance with competition law.