EUI ROBERT SCHUMAN CENTRE

RSC 2025/10
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

WORKING PAPER

BLOCKCHAIN INTEROPERABILITY: IMPLICATIONS FOR EU COMPETITION LAW AND DATA PROTECTION LAW

Klaudia Majcher, Marco Botta

European University Institute
Robert Schuman Centre for Advanced Studies
Centre for a Digital Society

BLOCKCHAIN INTEROPERABILITY: IMPLICATIONS FOR EU COMPETITION LAW AND DATA PROTECTION LAW

Klaudia Majcher, Marco Botta

RSC Working Paper 2025/10

ISSN 1028-3625

Published in March 2025 by the European University Institute.
Badia Fiesolana, via dei Roccettini 9
I – 50014 San Domenico di Fiesole (FI)

Italy

Views expressed in this publication reflect the opinion of individual author(s) and not those of the European University Institute.

With the support of the
Erasmus+ Programme
of the European Union

The European Commission supports the EUI through the European Union budget. This publication reflects the views only of the author(s), and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Robert Schumann Centre for Advanced Studies

Robert Schuman Centre for Advanced Studies The Robert Schuman Centre for Advanced Studies, created in 1992 and currently directed by Professor Erik Jones, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe’s place in 21st century global politics. The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe’s neighbourhood and the wider world.

For more information: http://eui.eu/rscas

The EUI and the RSC are not responsible for the opinion expressed by the author(s).

Centre for a Digital Society

The Centre for a Digital Society (CDS), created in 2022 and directed by Prof. Pier Luigi Parcu, analyses the challenges of digital transformation and its impact on markets and democracy. Within the EUI, the CDS is part of the Robert Schuman Centre for Advanced Studies. With its research, policy debates and executive training programmes, the CDS aims at advising policy makers on how to cope with the challenges generated by the digitalisation process. To do so, it adopts an inter-disciplinary approach relying on in-house expertise in law, economics and political sciences, and by actively cooperating with computer scientists and engineers from partner institutions.

For further information: https://digitalsociety.eui.eu/.

Abstract

Since the launch of Bitcoin in 2009, blockchain technology has undergone significant development and demonstrated its potential to revolutionize several industries. Distributed Ledger Technologies (DLTs) enable the transparent recording and secure sharing of data across a network of participants in a decentralized manner. However, the adoption of DLTs has been hindered by the existence of numerous protocols and diverging standards, leading to the creation of isolated 'walled gardens' where each blockchain operates independently. Achieving interoperability between different blockchains is thus essential for the broader application of the blockchain technology beyond cryptocurrencies.

So far, blockchain interoperability has been analysed primarily from a technical perspective, with a noticeable gap in scholarly contributions addressing its legal implications. This article is the first attempt to examine how EU competition law and data protection law will be affected by, and can support, the evolution towards interoperable blockchains. To this objective, it first provides the background by briefly explaining blockchain interoperability and its underlying mechanisms, as well as demonstrates the benefits of fostered interoperability and the challenges preventing it from fully materializing. As regards a competition law assessment, our analysis identified three potential areas that might be affected by blockchain interoperability: collusion and information exchanges, anti-competitive foreclosure, and standardization. A data protection analysis focuses on evaluating the potential impacts of blockchain interoperability on the principles of accountability, data minimization, and purpose limitation, as well as on the rights of individuals, particularly the 'right to be forgotten'.

The article concludes that blockchain interoperability does not introduce entirely new legal challenges beyond those already identified in the existing literature on blockchain's compatibility with competition law and data protection law. However, it has the potential to exacerbate these challenges. By enhancing the degree of data sharing among different parties, blockchain interoperability may foster collusion and complicate compliance with the GDPR. At the same time, blockchain interoperability could lower market entry barriers and reduce market concentration, thereby decreasing the risk of foreclosure practices. Our analysis also revealed that, in the near future, particular attention should be paid to the standardization efforts surrounding blockchain interoperability, which are likely to become a crucial nexus between blockchain technology and competition law.

Keywords

Distributed Ledger Technology; blockchain interoperability; data sharing; EU competition law; EU data protection law; EU General Data Protection Regulation

JEL classification

K21, K38, L40, O30

Acknowledgments

The authors would like to thank Viktoria Robertson, Niccolò Galli, and Natalia Menéndez González for their helpful feedback and discussion. All errors remain our own.

1. Introduction

Blockchain technology, which is defined as ‘a tamper-proof, shared digital ledger that records transactions in a decentralized peer-to-peer network’,[1] holds a promise to fundamentally transform a range of industries and sectors. During the past years, blockchain applications have spread beyond the area of cryptocurrencies, where this technology was initially conceived. Blockchain is nowadays utilized across various sectors and areas that require a transparent and safe recording of data, such as Intellectual Property (IP) rights, Non-Fungible Tokens (NFTs), as well as land registries and voting results.[2] The technology is also increasingly relied upon in the logistics sector to trace the origin, production, and movement of goods across the supply chain, while smart contracts powered by blockchain applications facilitate the exchange of goods and services between various actors.[3] In addition, blockchain applications are increasingly widespread in industries that require a trusted system of data sharing. In the healthcare sector, for instance, blockchain-based technologies are used to improve the security of patients’ data and digital records, and to enhance the transparency, traceability, and security of pharmaceutical supply chains, among other.[4]

Blockchain also interacts with and improves the functioning of other technologies: its integration with the Internet of Things (IoT), for example, and leveraging blockchain in contexts such as smart homes, allows the IoT to operate more safely and overcome challenges related primarily to the lack of trust.[5] At the moment, blockchain is also gaining a new momentum as a technology with the ability to help create a more equitable future of Artificial Intelligence (AI) and prevent the monopolization of the AI market by big tech companies. The movement towards decentralized AI, which places AI at the intersection with Web 3.0, involves a reliance on distributed ledger technologies to decentralize, enhance transparency, and democratize AI resources such as data, models, and computing power.[6]

While blockchain has potential applications across various industries, its use cases remain limited beyond cryptocurrencies and the fintech sector. This is largely due to technical limitations, such as low scalability, performance issues, and high costs, which hinder the widespread adoption of this technology.[7] As noted by Finck, ‘blockchains are inefficient by design’, since blockchain node must process every transaction and maintain a copy of the entire dataset.[8] Duplicating datasets across nodes enhances data integrity and reduces the risk of data loss from cyberattacks. However, as blockchain networks grow, their decentralized nature increases the complexity of block validation, resulting in lower scalability, reduced performance, and higher costs as compared to centralised databases.

[1] EU Blockchain Observatory and Forum, ‘Blockchain for beginners – basic guiding principles’ (2024), 7.

[2] ibid 16.

[3] ibid 17-18.

[4] Turing, ‘Blockchain for Healthcare: Benefits, Use Cases & Real-World Examples’ (15 September 2023) https://www.turing.com/resources/blockchain-for-healthcare#top-ten-real-world-examples-of-blockchain-in-healthcare last accessed 22 November 2024. For a more comprehensive discussion on blockchain’s use in the healthcare sector, see e.g., EU Blockchain Observatory and Forum, ‘Blockchain Applications in the Healthcare Sector’ (2022).

[5] See e.g., Sonia Kotel et al., ‘A Blockchain-based approach for secure IoT’ (2023) 225 Procedia Computer Science 3876. https://doi.org/10.1016/j.procs.2023.10.383.

[6] Victoria Chynoweth, ‘Web3 Meets AI: Blockchain Technology Revolutionizes The AI Landscape’ (*Forbes,* 8 May 2024) https://www.forbes.com/sites/digital-assets/2024/05/08/web3-meets-ai-blockchain-technology-revolutionizes-the-ai-landscape/ last accessed 22 November 2024.

[7] For a critical view of blockchain technology, see e.g., David Gerard, *Attack of the 50 Foot Blockchain: Bitcoing, Blockchain, Ethereum & Smart Contracts* (2017).

[8] Michèle Finck, *Blockchain Regulation and Governance in* Europe (Cambridge University Press 2018), 31.

Besides these technical limitations, the diffusion of blockchain technology is also hindered by the limited interaction between different blockchains. At present, coordination between blockchains is challenging, as systems diverge in relation to their models of governance, consensus mechanisms and robustness, permissibility levels, as well as the anonymity and security of their nodes.[9] The existence of numerous protocols and architectures for blockchain – hence no common blockchain architecture standards – results in blockchains being isolated in 'walled gardens'.[10] The EU Blockchain Observatory and Forum noted recently that enhancing interoperability constitutes a 'key challenge' that is pivotal to address for a blockchain-empowered future to realize.[11] Importantly, interoperability is considered 'essential in maintaining the core ethos of decentralization', as without it, 'we may inadvertently end up with new form of centralization, where certain blockchain ecosystems dominate at the expense of others'.[12] Achieving interoperability between different blockchains is thus considered essential to solve the technical limits that have so far characterized the deployment of this technology, thereby fostering its mainstream adoption across a larger number of industries and use cases.

So far, blockchain interoperability has been analysed primarily from a technical perspective, with a noticeable gap in scholarly contributions addressing its legal implications. The legal literature has focused on whether and to what extent blockchain might be considered 'alegal' (i.e. not subject to State regulations due to its distinctive characteristics).[13] In Europe, legal scholars have explored potential conflicts between the fundamental features of blockchain technology and competition[14] and data protection laws.[15]

This article is the first attempt to examine how EU competition law and data protection law will be affected by, and can support, the evolution towards interoperable blockchains. It examines both the challenges and opportunities that blockchain presents for these two areas of EU law. While blockchain interoperability may have implications for a number of other EU regulatory and legal instruments, including the recently adopted EU Data Act[16] and the Regulation on Markets in Crypto-Assets (MiCA)[17], these remain outside the scope of this article.

Blockchain interoperability can be categorised into three types: interoperability between blockchains, interoperability among decentralized applications ('dApps') on the same blockchain, and interoperability between blockchains and other technologies.[18] Given that these various forms of interoperability may present distinct legal challenges, this article will concentrate exclusively on interoperability between different blockchains – i.e. cross-chain.

[9] EU Blockchain Observatory and Forum (n 1) 26.

[10] Seth Djanie Kotey et al., 'Blockchain interoperability: the stage of heterogenous blockchain-to-blockchain communication' (2023) 17 IET Communications 891, 892.

[11] EU Blockchain Observatory and Forum, 'The current state of interoperability between blockchain networks' (2023) 5.

[12] ibid 6.

[13] In relation to this debate, see e.g., Esen Esener, 'Adaptive Governance for Blockchain Networks' (2024) Stanford Journal of Blockchain Law and Policy https://stanford-jblp.pubpub.org/pub/adaptive-governance-blockchain-networks/release/1 last accessed 22 November 2024; Primavera De Filippi, Morshed Mannan and Wessel Reijers, 'The Alegality of Blockhain Technology' (2022) 41 Policy and *Society* 358; Mimi Zou 'Code, and Other Laws of Blockchain' (2020) 40 Oxford Journal of Legal Studies 645.

[14] See, in particular, Thibault Schrepel, *Blockchain + Antitrust: The Decentralization Formula* (Edward Elgar Publishing 2021).

[15] Finck (n 8).

[16] Regulation (EU) of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L, 2023/2854.

[17] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, OJ L150/40.

[18] Léo Besançon, Catarina Ferreira da Silva and Parisa Ghodous, 'Towards Blockchain Interoperability: Improving Video Games Data Exchange' (2019) IEEE International Conference on Blockchain and Cryptocurrency, 81-85. 1https://doi.org/10.1109/BLOC.2019.8751347.

The article is structured as follows. Following the introductory remarks in Section 1, Section 2 provides the background by briefly introducing blockchain technology as well as explaining blockchain interoperability and its underlying mechanisms. It also shows the value of fostered interoperability – its benefits and concrete applications, – and demonstrates the challenges that prevent blockchain interoperability from materializing. Section 3 moves to a legal perspective and discusses whether and to what extent blockchain interoperability can be either limited or facilitated by legal mechanisms contained in EU law, especially in the field of competition law and data protection law. Concluding remarks are provided in Section 4.

The legal analysis carried out in the present paper is clearly future-oriented. To date, no National Competition Authority (NCA) or Data Protection Authority (DPA) has issued specific decisions or guidelines addressing the issue of blockchain interoperability. Additionally, as discussed in this article, while methods to achieve blockchain interoperability exist, technical obstacles still prevent widespread interoperability from being realized. At the same time, there is a broad agreement that blockchain interoperability is a crucial step towards the wider adoption of the blockchain technology, hence its potential legal implications merit a thorough analysis. The present article is therefore a crucial 'forward-looking' exercise; the key research question discussed in this paper is how can the law shape blockchain interoperability and, once blockchain interoperability becomes a reality, what will be its repercussions for EU competition law and data protection law.

2. Understanding blockchain interoperability

2.1. A brief introduction to blockchain technology

Introduced in 2009 as the technology behind Bitcoin, blockchain has since evolved into a disruptive innovation with applications extending beyond cryptocurrency.[19] Blockchain is a form of a distributed ledger technology employing a chain of blocks that store information and are connected to one another. The information that can be stored on blockchains varies and may include data as different as money, contracts, medical records, administrative certificates, or data related to the sale and purchase of goods or services.[20] Cryptography solutions ensure that the data is safely stored in the blocks. Blockchain relies on an append-only structure, meaning data can only be added to the database and cannot be altered or deleted once recorded.[21] A distinguishing feature of blockchain is its decentralized structure, eliminating the need for a centralized intermediary managing the blockchain. It thus overcomes the problem of limited trust in a third party by offering an architecture for secure and transparent peer-to-peer interactions, and enabling 'trustless' transactions.[22]

Comprehensively defined, blockchain is a decentralized computing system consisting of five components: (1) decentralized networking, (2) mathematical cryptography, (3) transaction ledger, (4) distributed consensus, and (5) smart contracts.[23] The first feature – decentralized networking – entails the operation of a blockchain through an interconnected network of independent computers, known as 'nods', which function autonomously and communicate directly with one another.[24] Mathematical cryptography means that a cryptographic hash is relied upon to create linkages between data blocks in the chain, guaranteeing the security of transactions by disabling post-recording alterations.[25] As a transaction ledger, blockchain has the capability to store transactions sequentially in blocks. The

[19] The foundation for blockchain technology was established already in the early 1990s, when researchers introduced a prototype for securely stamping digital documents: EU Blockchain Observatory and Forum (n 1) 7-8.

[20] Marixenia Davilla, 'Unravelling the Complexity of Blockchain and EU Competition Law' (2022) 13 Journal of European Competition Law & Practice 387, 387. https://doi.org/10.1093/jeclap/lpab078.

[21] Shaan Ray, 'The Difference Between Blockchains & Distributed Ledger Technology' (*Medium,* 20 February 2018) https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92 last accessed 22 November 2024.

[22] EU Blockchain Observatory and Forum (n 1) 7.

[23] Duc A. Tran and Bhaskar Krishnamachari, 'Blockchain in a Nutshell' in Duc A. Tran, My T. Thai and Bhaskar Krishnamachari (eds.) *Handbook on Blockchain* (Springer 2022) 6.

[24] ibid.

[25] ibid.

mechanism of distributed consensus enables blockchain decentralization by requiring consensus among the participants to take a decision.

Consensus protocols vary, and selecting the right one is a crucial decision when designing a blockchain. The original mechanism, 'Proof-of-Work', grants decision-making power to the nodes with greater computing power. Proof-of-Work was the first consensus protocol used in blockchain, initially introduced with Bitcoin.[26] Miners solve complex mathematical puzzles to validate transactions and create new blocks, and they are awarded tokens for their efforts. The Proof-of-Work protocol is a fully decentralized system of validation. However, as the blockchain expands, the mathematical puzzles have become increasingly complex, requiring miners to use higher computing power and, consequently, more energy to validate new blocks.[27] Due to Proof-of-Work's environmental impact and limited efficiency, new consensus protocols have been introduced in recent years. Notable examples are 'Proof-of-Stake', 'Proof-of-Authority', and 'Byzantine-Fault-Tolerance', which select validators based on predefined criteria.[28] While these protocols are considered more efficient, they tend to offer a lower degree of decentralization compared to Bitcoin's original vision of an open peer-to-peer network.

As regards the blockchain's governance and access structure, blockchains can be divided into two broad categories: permissioned and permissionless. Permissioned blockchains are characterized by restricted access to participate in the network, with network administrators controlling membership and transaction capabilities. Permissionless blockchains, in contrast, are entirely decentralized platforms allowing everyone to participate in the consensus mechanism and make changes.[29] Another categorization of blockchains divides them into private (usually corresponding to permissioned blockchains), public (often corresponding to permissionless blockchains), hybrid, and consortium blockchains. Hybrid blockchains combine the characteristics of public and private blockchains: they can be utilized if controlled data access is required (i.e. making some information publicly available and some restricted).[30] Consortium blockchains usually fall under the category of permissionless blockchains. The governance of the network is entrusted to a group of organisations, with each consortium participant holding equal decision-making authority over the network.[31]

Smart contracts represent a significant advancement in blockchain technology, enabling its application beyond cryptocurrencies and into a variety of new use cases. Smart contracts are self-executing agreements that activate when specific conditions are met – e.g. payment for products is automatically carried out by a computer, without any human intervention, once proof of delivery is received.[32] While smart contracts were first theorized by Nick Szabo in 1994, blockchain technology has provided the infrastructure needed to deploy them in practice. Today, smart contracts running on blockchain networks are considered 'a fundamental building block for the Web3 industry'.[33] Building on smart contracts, Decentralized Applications (DApps) represent a further evolution. Unlike traditional applications hosted on centralized servers, DApps are open-source software operating on blockchain network of computers and relying on smart contracts to perform certain functions.[34] In recent years, DApps have been developed for various purposes, including digital wallets, exchanges, gaming, personal finance, and social media.[35]

[26] Ahmed Banafa, *Blockchain Technology and Applications* (River Publishers Series in Security and Digital Forensics 2020), Chapter 2.1.

[27] ibid.

[28] ibid.

[29] Blockchain Council, 'Permissioned and Permissionless Blockchains: A Comprehensive Guide' (2024) https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/ last accessed 22 November 2024.

[30] Paxos, 'Understanding the Different Blockchain Types' (22 May 2024) https://paxos.com/2024/05/22/understanding-the-different-block-chain-types/#:~:text=Four%20common%20types%20of%20blockchain,it%20comes%20to%20categorizing%20blockchains last accessed 22 November 2024.

[31] ibid.

[32] Banafa (n 26), Chapter 4.5.

[33] Chainlink, 'What Are Smart Contracts and How Do They Work?' (2023) https://chain.link/education/smart-contracts last accessed 22 November 2024.

[34] Banafa (n 26), Chapter 5.

[35] Investopedia, 'Decentralized Applications (dApps): Definition, Uses, Pros and Cons (updated 28 June 2024) https://www.investopedia.

2.2. An overview of blockchain interoperability

Blockchain interoperability refers to the ability of multiple blockchains to connect in order to 'access information and to act on the information'.[36] In practice, this means enabling blockchain networks to communicate by seamlessly transferring assets, such as cryptocurrency or data, between one another, and allowing users to view and interact with information available on one blockchain while operating on another.[37] Framed differently, 'blockchain interoperability technology is a communication protocol that enables one chain to interact with another and allows for the control of the flow and sharing of data in a uniform and reliable manner'.[38]

While blockchain interoperability has gained considerable attention in recent years, the discussion can be traced back to 2014, when the absence of built-in communication capabilities of blockchains was referred to as 'the oracle problem'.[39] The oracle problem has been explained as follows:

'The blockchain oracle problem refers to the inability of blockchains to access external data, making them isolated networks, akin to a computer with no Internet connection. Bridging the connection between the blockchain (onchain) and the outside world (offchain) requires an additional piece of infrastructure – an oracle'.[40]

The connection that the oracle is supposed to enable is one between the blockchain on the one hand, and off-chain systems that include APIs, data providers, cloud providers, IoT devices, payment systems, and other blockchains, on the other one.[41] The oracle problem extends thus beyond blockchain interoperability, with cross-chain communication being just one challenge.

As regards blockchain interoperability specifically, there continues to be a significant fragmentation of the industry, with a large number of networks operating as 'walled gardens' disconnected from other blockchains. This fragmentation arises partially because blockchains are developed to meet specific industry and application needs, necessitating the optimization of their systems and protocols.[42] This has resulted in the development of several blockchains with different structures, consensus mechanisms, or privacy and security functionalities, among others.[43]

As it is becoming clear that the technology's full potential cannot be realized as long as blockchains operate in siloes without the ability to communicate with one another, there is a rising demand for interoperable blockchain solutions. Both academia and industry are thus dedicating significant efforts to the question of how to develop a blockchain interoperability system that is highly efficient, secure, universal, and guarantees a high degree of privacy protection.[44]

com/terms/d/decentralized-applications-dapps.asp last accessed 5 August 2024.

[36] Kotey et al. (n 10) 892.

[37] ibid; Chainlink, 'What Is Blockchain Interoperability?' (2023) https://chain.link/education-hub/blockchain-interoperability last accessed 22 November 2024. Blockchain interoperability is defined as 'the ability of blockchain networks to communicate with each other, sending and receiving messages, data, and tokens'.

[38] Ruoyu Yin et al., 'A survey on privacy preservation techniques for blockchain interoperability' (2023) 140 Journal of System Architecture 102892, 2. https://doi.org/10.1016/j.sysarc.2023.102892.

[39] EU Blockchain Observatory and Forum (n 11) 4.

[40] Chainlink, 'The Blockchain Oracle Problem' (29 November 2023) https://chain.link/education-hub/oracle-problem#:~:text=The%20oracle%20problem%20revolves%20around,computer%20with%20no%20Internet%20connection last accessed 22 November 2024.

[41] ibid.

[42] See e.g. Haonan Yuan, Shufan Fei and Zheng Yan, 'Technologies of blockchain interoperability: a survey' (2023) Digital Communications and Networks, 1. https://doi.org/10.1016/j.dcan.2023.07.008.

[43] ibid.; see also Chainlink (n 37).

[44] Yin et al. (n 38) 1.

From a technical point of view, there can be different classifications of blockchain interoperability based on how it can be achieved. Blockchain interoperability schemes fall commonly under the following four categories: (1) notary schemes, (2) Hash-Locking, (3) side chains, and (4) relay chains.[45] From a technological point of view, notary schemes are the most straightforward method for achieving blockchain interoperability. This approach relies on a trusted intermediary, known as the 'notary', who is tasked with managing multiple blockchains, overseeing and verifying transactions between them, and ensuring the integrity and accuracy of the data transferred across blockchains.[46] In practice, a notary is relied upon 'to claim to chain X that a given event on chain Y took place, or that a particular claim about chain Y is true'[47] – a process known as 'notarization'.[48] For this to occur, a notary needs to have accounts on both blockchains X and Y: if a user 1 on blockchain X wants to transfer the asset to a user 2 on blockchain Y, user 1 needs to transfer this asset to the notary account on Blockchain X, who then locks it, confirms it, and transfers it from their account on Blockchain Y to user 2.[49] Whereas the notary scheme mechanism is flexible and easily implementable since it does not require technological changes to the blockchain, avoiding centralization is a challenge.[50] Additionally, the scheme's success relies entirely on the trustworthiness of the notary, which can carry some risks related to 'a single point of failure'.[51] To overcome the issue of centralization and dependence, the solution can be to rely on a 'multi-signature notary' mechanism instead of a 'single-signature notary'. A multi-signature notary mechanism requires the approval of the transaction from multiple trusted parties, ensuring decentralization and reducing reliance on a single entity.[52] As further discussed in Section 2, however, this carries the risk of collusion between notary nods.[53]

Another method of realizing interoperability, which removes the need for having a trusted notary, is hash-locking or hashed time-lock contracts (HTLCs). It is a way 'of exchanging value across blockchains by locking cryptocurrency assets on a blockchain X and releasing the asset after the recipient on blockchain Y confirms readiness to receive the asset'.[54] The technique to perform such a transaction – called 'a cross-chain atomic swap' – occurs with the aid of an advanced form of smart contract called HTLC. This mechanism requires the recipient of the transaction to confirm the transaction by providing cryptographic proof within a short timeframe.[55] Put differently, a transaction is conditional on the revelation of a pre-agreed secret – a 'hash' – by the recipient, and assets are transferred only when the correct hash value is provided. Even though hash-locking is currently one of the most common methods of asset exchange, it suffers from inefficiency as it can be performed only between two parties: if more parties want to exchange assets, separate contracts need to be initiated for each couple of members.[56] As further discussed in Section 2, this also raises important privacy challenges.

[45] See e.g., Kotey et al. (n 10); Vitalik Buterin, 'Chain Interoperability' (2016) R3 Research Paper 9 https://allquantor.at/blockchainbib/pdf/vitalik2016chain.pdf last accessed 21 February 2025. Whereas Kotey et al. and Buterin discuss the categories 1, 2 and 4, the third category – sidechains – has been listed as relevant by others: see e.g., Yuan, Fei and Yan (n 42).

[46] EU Blockchain Observatory and Forum (n 11) 11.

[47] Buterin (n 45) 4.

[48] Kotey (n 10) 896.

[49] Techstill Brew, 'Blockchain interoperability and how does it work? (Part 75)' (*Medium,* 8 November 2022) https://medium.com/techs-kill-brew/blockchain-interoperability-and-how-does-it-work-part-75-f5d0a70d12b0#:~:text=Hash%2Dlocking%20or%20hash%2D-time,is%20also%20called%20atomic%20swaps last accessed 22 November 2024.

[50] Kotey (n 10) 896; EU Blockchain Observatory and Forum (n 11) 11.

[51] EU Blockchain Observatory and Forum (n 11) 11.

[52] Techstill Brew (n 49).

[53] Shuhi Zhang et al., 'Cross-Chain Asset Transaction Method Based on Ring Signature for Identity Privacy Protection' (2023) 12 Electronics 5010, 2. https://doi.org/10.3390/electronics12245010.

[54] Kotey (n 10) 898.

[55] EU Blockchain Observatory and Forum (n 11) 12.

[56] Fadi Barbàra and Claudio Schifanella, 'MP-HTLC: Enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract' (2023) 35 Concurrency and Computation: Practice and Experience, 2. https://doi.org/10.1002/cpe.7656.

Sidechains fall under the third category of schemes enabling cross-blockchain transactions. A sidechain is an auxiliary blockchain connected to a primary blockchain (i.e. the mainchain). While a sidechain operates independently, the link to the mainchain allows a secure transfer of assets between them.[57] The transfer process involves locking the asset on the mainchain and creating an equivalent representation on the sidechain. Once the asset has been utilized on the sidechain, it is returned to and unlocked again on the mainchain.[58] While sidechains are easily applicable and enhance the scalability of the mainchain, they also introduce additional network complexity and increase vulnerability to attacks.[59]

The final category, known as 'relays', offers a direct method for achieving interoperability without relying on a trusted middleman. Instead, a blockchain can communicate its own data directly to another blockchain. The transmitting blockchain first shares a 'block header' – a compact piece of information which represent all the transactions included in the blockchain.[60] The receiving blockchain then verifies the block header as a first step in establishing a connection between the two blockchains. Essentially, a relay is thus a type of a bridge that reads data from one blockchain and relays/transmits it to another.

2.3. Benefits of fostered blockchain interoperability and current challenges

Interoperability has the potential to solve some of the technical challenges that have constrained the broader adoption of blockchain technology. It could enhance blockchain scalability and solve the 'walled garden' issues that have so far restricted its use beyond cryptocurrencies.

The technical literature has thoroughly examined the advantages and disadvantages of the four interoperability solutions discussed above. A trade-off appears to exist between a higher degree of centralization and efficiency:[61] the notary scheme seems more efficient (i.e., has lower latency response), but is a rather centralized solution, which clashes with the decentralized ethos of blockchain technology. In contrast, sidechains and relay chains are complex technical solutions that reduce the efficiency of cross-chain data transfers but do not require the involvement of a trusted middleman. There is no consensus in the literature on the optimal approach for ensuring blockchain interoperability: the best solution may vary depending on the specific needs of different industries and use case. A single technical solution for blockchain interoperability seems unlikely in the near future.[62]

It is also important to note that blockchain interoperability has largely focused on the transfer of tokens and digital assets between different chains. The technical literature on interoperability has primarily debated how different cryptocurrencies may be converted and exchanged. However, as noted by Khan et al., future technical research on blockchain interoperability will need to address the enforcement of smart contracts and decentralized applications ('DApps'), which will involve the exchange of data across different blockchains.[63] Others observed that facilitating data exchange between blockchains will require new forms of interoperability – i.e., 'semantic' and 'syntactic' interoperability will be essential for successful cross-chain transactions.[64] This means that not only will data need to be transferred from one blockchain to another, but the blockchains will also need to 'speak' a common language to become truly interoperable.

[57] EU Blockchain Observatory and Forum (n 11) 11.

[58] Nervos Network, 'Sidechains: Unlocking the Potential of Blockchain Scalability and Interoperability' (14 June 2023) https://www.nervos.org/knowledge-base/sidechains_unlocking_the_potential last accessed 22 November 2024.

[59] EU Blockchain Observatory and Forum (11) 11.

[60] Kotey et al. (n 10) 900-901.

[61] Yuan et al. (n 42).

[62] ibid.

[63] Sajjad Khan et al., 'Towards Interoperable Blockchains: a Survey on the Role of Smart Contracts in Blockchain Interoperability (2021) Institute of Electrical and Electronics Engineers (IEEE) https://ieeexplore.ieee.org/document/9519640 last accessed 5 August 2024.

[64] Tommy Koens and Erik Poll, 'Assessing Interoperability Solutions for Distributed Ledgers' (2019) 59 Pervasive and Mobile Computing 1574. https://doi.org/10.1016/j.pmcj.2019.101079.

Another notable challenge accompanying the development of interoperable blockchains relates to privacy. Despite the ongoing efforts towards blockchain interoperability, the critical issue of privacy – stemming from the inherent transparency and openness of blockchain and the lack of trust among parties, among others, – remains insufficiently addressed.[65] Transparency, in fact, is at the core of this technology: every user has access to the data recorded on the blockchain. Cross-chain interoperability thus increases the number of users who can access to the same pool of data. A number of technical solutions, such as 'digital signatures' and 'homomorphic encryption' that apply asymmetric cryptography techniques, 'zero-knowledge proofs' that limit the disclosure of data for interoperability verification purposes, and 'trusted execution environment', are potential privacy-preserving solutions in the context of blockchain interoperability.[66] While these solutions enhance the privacy of blockchain users by making data fully or partially anonymous through encryption, they do not necessarily improve users' control over their personal data and thus may not be fully compatible with the GDPR requirements.

In the next section, the technical perspective presented above will be complemented by an analysis of EU law as a source of opportunities and limitations for blockchain evolution towards interoperability.

3. A legal perspective on blockchain interoperability

3.1. Blockchain and EU law: from 'alegelity' to MiCA

In recent years, a combination of distinctive features of blockchains – their decentralization, transnationality, tamper-resistance, pseudonymity, absence of coercion, trustlessness and operational autonomy – have triggered a reflection on how this technology challenges traditional legal boundaries.[67] The imposition of sovereign regulatory powers is complicated by the inability to see, understand, and describe operations on blockchain networks, among other factors.[68] Some went further, suggesting not that blockchain technology might be complicated to regulate, but rather that it can entirely circumvent legal norms and the rule of law.[69] Already a decade ago, Wood coined the concept of 'alegality' to describe the phenomenon of blockchain's ability to exist outside the realm of law.[70] Alegality implies the 'capacity to be neither legal or illegal, the ability to exist and act in the interstices, or perhaps beyond or outside, the dominant modes […] of legal production'.[71] The regulatory reality unfolding as a result might be one that features *lex cryptographica*, which De Filippi and Wright describe as 'new self-contained and autonomous systems of rules that create order without law and implement what can be thought as private regulatory frameworks'.[72]

[65] Yin et al. (n 38) 1.

[66] ibid 5-6.

[67] Primavera De Filippi, Morshed Mannan and Wesel Reijers, 'The alegality of blockchain technology' (2022) 41 Policy and Society 358, 359. https://doi.org/10.1093/polsoc/puac006. For a comprehensive analysis of blockchain and law, see Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2019).

[68] De Filippi, Mannan and Reijers (n 67) 11.

[69] Richard Miller, 'Continuing challenges to international law and order from evolving technologies such as blockchain' (2019) 9 Hirao School of Management Review 41, 41-52.

[70] Gavin Wood, 'Alegality: Systems that can't care' (2014) https://www.youtube.com/watch?v=Zh9BxYTSrGU last accessed 22 November 2024.

[71] Vanja Hamzić, 'Alegality: Outside and beyond the legal logic of late capitalism' in Honor Brabazon (ed.) *Neoliberal legality: Understanding the role of law in the neoliberal project* (Routledge 2017) 191; quoted in De Filippi, Mannan and Reijers (n 67) 3.

[72] Primavera De Filippi and Aaron Wright, 'The Rule of Code vs. The Rule of Law' (*Harvard University Press Blog,* 10 April 2018) https://harvardpress.typepad.com/hup_publicity/2018/04/blockchain-and-the-law.html last accessed 22 November 2024.

An alternative reality, one that sees legal reforms aimed at incorporating new blockchain-related practices and market constructs into the realm of the law, however, has emerged in the past years.[73] Scholars have suggested that the legal ambiguity surrounding blockchain can be resolved by either expanding current legal provisions to include new activities or by narrowing these provisions to exclude them, thereby allowing these new activities to occur without the typical legal constraints.[74]

The EU Regulation on the Markets in Crypto-Assets (MiCA) represents the first attempt in the world to introduce specific financial market rules for crypto-assets (e.g., cryptocurrencies and blockchain tokens). Applicable in its entirety as of December 2024, MiCA aims to promote innovation by harmonizing the rules on crypto-assets, crypto-assets issuers, and crypto-asset service providers.[75] For crypto-assets that are financial instruments, the EU introduced in 2022 a Regulation on a pilot-regime for market infrastructures based on Distributed Ledger Technologies (DLT).[76] This six-year DLT pilot regime was established to enable certain DLT market infrastructures to receive exemptions form the applicable financial regulations that might otherwise impede their development.

Even though crypto-assets is the only area where regulatory actions have been taken, the European Commission has emphasized the 'importance of legal certainty and a clear regulatory regime in areas pertaining to blockchain-based application', indicating that it 'strongly supports a EU-wide rules for blockchain to avoid legal and regulatory fragmentation'.[77] As blockchain technology evolves and its use cases have a strong potential to proliferate further, future regulatory actions in the EU cannot by excluded.

As regards other policy initiatives, in February 2023, the European Commission launched the European Regulatory Sandbox for Blockchain, offering a pan-European framework for companies to test their blockchain-related innovations in a controlled and confidential environment, and in cooperation with the relevant regulator.[78] The initiative is supposed to support approximately 20 projects of public and private sector use cases of blockchain technology in the period between 2023-2026. This framework is expected to support a number of blockchain's use cases, including 'data portability, business-to-business data spaces, smart contracts, and digital identity'.[79] Even if not mentioned explicitly, blockchain interoperability solutions could also be tested in the sandbox environment. The idea of alternative policy interventions such as sandboxes was also advocated by De Filippi et al., for example. As noted by these authors, this approach has the advantage of delegating the task of proposing and designing innovative regulatory solutions to actors with a more profound understanding of the technology than regulators and policymakers.[80]

To sum up, the legal debate in this field has evolved since the Bitcoin release in 2009: from a *laissez-faire* approach, where blockchain was considered 'alegal', this technology is subject nowadays to an increased regulatory scrutiny. This is especially the case for cryptocurrencies and digital assets, which represent the most important use cases of blockchain.

[73] De Filippi, Mannan and Reijers (n 67) 6.

[74] De Filippi, Mannan and Reijers (n 67) 9-10.

[75] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (EU) No 1093/2010 [2023] OJ L 150.

[76] Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU [2022] OJ L 151.

[77] European Commission, 'Legal and regulatory framework for blockchain' https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain last accessed 22 November 2024.

[78] European Commission, 'Launch of the European Blockchain Regulatory Sandbox' (14 February 2023) https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox last accessed 22 November 2024. A designated website for the initiative: https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project last accessed 22 November 2024.

[79] European Commission, 'Pan-European blockchain regulatory sandbox' https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain last accessed 22 November 2024.

[80] De Filippi, Mannan and Reijers (n 67) 12.

The next sub-Sections turn to blockchain interoperability specifically, and how EU law – in particular competition law and data protection law – can create opportunities or hinderances for blockchain interoperability solutions.

3.2. Competition law

Competition law is a powerful tool in the hands of public authorities to discipline markets and protect the process of competition to the benefit of consumers. The core provisions of competition law, Article 101 and 102 TFEU, set out the rules for addressing anti-competitive agreements and abuse of a dominant position, respectively. The EU Merger Regulation[81] contains the rules for the assessment of concentrations that have a Union dimension: concentrations can be prohibited if they would significantly impede effective competition in the common market or in a substantial part of it.

While blockchain technology has not yet been the subject of significant competition law enforcement action, either in the EU or in other jurisdictions, theoretical discussions point to several potential antitrust challenges and opportunities.[82] Challenges include in particular the risk of collusion, for example if firms that compete on the same market use a single blockchain to exchange competitively strategic information. There are also potential issues related to abuse of a dominant position: for instance, a blockchain consortium can refuse access to a permissioned blockchain. Risks to competition might also arise in relation to standard-setting, for example when the process results in the restriction of price competition or innovation. At the same time, blockchain technology also presents competition-related opportunities, for example in the context of designing remedies, monitoring commitments, as well as enabling efficiency gains, innovation, and market entry for new undertakings.

The next sub-Sections discuss blockchain interoperability through the lens of three scenarios under EU competition law: (1) collusion and information exchange, (2) anti-competitive foreclosure, and (3) standardization.

3.2.1. Collusion and information exchange

A. Competition law assessment

In a competitive market, undertakings independently determine their strategies regarding pricing, quantity of production, as well as investments in innovation, production facilities, and marketing. However, in more concentrated or oligopolistic markets, competing undertakings often ‘look at each other’ – e.g. smaller firms may follow the retail price set by a market leader. Following the market behaviour of the leader does not violate competition law, provided there is no systematic coordination, meaning collusion, between firms.[83] Collusion encompasses a broad range of practices from cartels (i.e. where undertakings explicitly agree on implementing a specific conduct in the future, such as setting prices for an upcoming period) to concerted practices (i.e., regular exchange of sensitive information). This exchange can be carried out directly by the parties, through intermediaries like industry associations (i.e. the ‘hub and spoke’ scenario), as well as via common platforms (e.g. blockchain) or algorithms that monitor competitors’ prices and automatically adjust a firm’s market

[81] Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation) [2004] OJ L 24.

[82] See e.g. Davilla (n 20); Schrepel (n 14); Maria Teresa Maggiolino and Laura Zoboli, ‘Blockchain and antitrust law: A roadmap’ in Oreste Pollicino and Giovanni De Gregorio, *Blockchain and Public Law: Global Challenges in the Era of Decentralisation* (Edward Elgar 2021); OECD, ‘Blockchain Technology and Competition Policy’ (2018) Issues paper by the Secretariat, DAF/COMP/WD(2018)47; Ioannis Lianos, ‘Blockchain Competition: Gaining Competitive Advantage in the Digital Economy – Competition Law Implications’ in Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos and Stefan Eich (eds.) *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019); Michael Ristaniemi and Klaudia Majcher, ‘Blockchains in competition law – friend or foe?’ (*Kluwer Competition Law Blog,* 21 July 2018) available at https://competitionlawblog.kluwercompetitionlaw.com/2018/07/21/blockchains-competition-law-friend-foe/ last accessed 22 November 2024.

[83] Case C-74/14 *Eturas and Others* ECLI:EU:C:2015:493, para 27; Case C-8/08 *T-Mobile Netherlands and Others* ECLI:EU:C:2009:343, paras 32-33.

behaviour. The 2023 EU Commission Guidelines on Horizontal Agreements provide a broad definition of 'information', covering both 'physical information sharing and digital data sharing between actual or potential competitors.'[84] The term 'digital data' includes both 'raw, unorganized digital content' as well as 'pre-processed' and 'manipulated data'.[85]

While a cartel is considered an 'object restriction' under Art. 101(1) TFEU – meaning it is *per se* prohibited –, the exchange of information among competitors can be classified as either a restriction 'by object' or 'by effect'. In the latter case, the EU Commission would assess the actual or potential effect of the information exchange on market dynamics by comparing the effects of data sharing to a counterfactual scenario in which no exchange takes place. This assessment considers also the type of information exchanged and at the market characteristics - i.e. exchange of information in a oligopolistic market is more likely to hamper competition.[86] An exchange of information deemed to restrict competition by effect could be justified if it fulfils the four cumulative conditions set out in Art. 101(3) TFEU: (1) the information exchange generates efficiency gains (e.g. it resolves information asymmetries that facilitate the introduction of a new product), (2) these benefits are passed on to consumers, (3) the exchange is indispensable for achieving the efficiency gains, (4) and the conduct does not fully eliminate competition in the market (i.e. independent undertakings not involved in the information exchange remain active in the market).[87]

Several factors must be considered when determining whether an information exchange system qualifies as a restriction by object or effect under Art. 101(1) TFEU. The first factor is the type of information exchanged: if competitors exchange commercially sensitive information, such as pricing details or planned future market strategies, this is more likely to be considered a restriction by object. Conversely, the exchange of non-sensitive information, for example publicly available data like public health and safety standards, is more likely to fall under the category of restriction by effect.[88]

The 'granularity' of the exchanged data is another important factor to consider. Exchanging highly specific, individualized information is more likely to facilitate collusion between undertakings, whereas sharing aggregated data poses less risk.[89] For example, exchanging information about future prices is generally considered a restriction by object. In contrast, the exchange of aggregated statistics on prices applied in the previous quarter of the year by the firm is less problematic, and thus more likely to fall under the category of restriction by effect.

What should also be taken into account is the age of the information. Exchanging information about future market conduct is more likely to be considered a restriction by object, while the exchange of historical data is less problematic.[90] The relevant age of the information varies by industry. In fast-moving markets where prices change very frequently, past pricing data quickly becomes historical and loses its commercial sensitivity. In contrast, in markets where prices are stable over the time, information about prices can remain commercially sensitive for a longer period.

Whether the conduct is classified as by object of by effect also depends on the frequency of information exchange: a frequent exchange may facilitate collusion.[91] Like the age of the information, the frequency of exchange is influenced by the degree of market stability. In markets characterized by long-term contracts, periodic exchanges may be sufficient to encourage collusion.

[84] European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements [2023] C 259, para 367.

[85] ibid para 367.

[86] ibid paras 420-422.

[87] ibid paras 425-428.

[88] Case C-286/13 P *Dole Food and Dole Fresh Fruit Europe v Commission* ECLI:EU:C:2015:184, para 121; Case C-883/19 P *HSBC Holdings and Others v Commission* ECLI:EU:C:2023:11, para 115.

[89] EU Commission Guidelines on Horizontal Agreements (n 85) paras. 390-391.

[90] ibid paras 393-394.

[91] ibid paras 393-394.

The case law of the CJEU has introduced a rebuttable presumption that a firm receiving commercially sensitive information is presumed to engage in collusion if it does not openly distance itself from the collusive practice.[92] For instance, a firm would be presumed to breach Art. 101 TFEU if one of its representatives attends a meeting where commercially sensitive information is exchanged, unless the representative leaves the meeting and openly declares they will not participate in similar meetings in the future. Similarly, in *Eturas*, the CJEU clarified that a firm passively receiving commercially sensitive information through an industry platform can be held liable for a competition law infringement, unless it demonstrates it had no access to the contested information.[93] The burden of proof is thus reversed, requiring any firm involved in the exchange to demonstrate active distancing from the practice before detection by competition authorities to avoid liability.

The 2023 EU Commission Guidelines acknowledge the importance of data sharing in the digital economy, including the creation of data pools, where the holders of data group together in order to share data. They recognize that information exchange is becoming a common feature of many markets,[94] aligning with the EU Data Sharing Strategy.[95] Information exchange can help address information asymmetries among market players, foster innovation, and facilitate the introduction of new products.[96] According to the Guidelines, a data sharing arrangement such as a data pool 'in which (partly) commercially sensitive data is exchanged which address information asymmetry in a non-concentrated market and that will result in benefits for consumers' is not likely to be classified as a restriction by object under Art. 101(1) TFEU 'if the participants ensure that any commercially sensitive data that they exchange through the pool is necessary and proportionate to achieve the pro-competitive aim'.[97]

The inclusion of this paragraph in the 2023 Horizontal Guidelines is a sign of the EU Commission's more favourable approach vis-à-vis B2B data sharing and data pools. The Guidelines do not clarify the meaning of 'partly' commercially sensitive data; instead, this should be evaluated on a case-by-case basis, taking into account the type of data exchanged, its degree of aggregation, information age, and frequency of the exchange.

B. Application to blockchain interoperability

The 2023 Horizontal Cooperation Guidelines do not explicitly mention blockchain technology. However, since the Guidelines cover all types of digital and non-digital information exchanges between competitors, blockchain could be used as a technology for data sharing in data pools, offering an alternative to centralized platforms. At the same time, blockchain technology might facilitate collusion among competitors due to its unique technical features.[98] DLTs, such as blockchain, enable secure and confidential exchanges of different categories of data among the members of the same blockchain. Since each member has access to the entire dataset stored on the blockchain and given that data is encrypted, it could be challenging for external parties, like competition authorities, to detect a collusive data exchange. The risk of collusion is particularly high with private or permissioned blockchains, where access is restricted to only a limited number of participants, compared to public or permissionless blockchains that operate on a fully decentralized model.

[92] Case C-373/14 P *Toshiba Corporation v Commission* ECLI:EU:C:2016:26, paras 62-63; Case C-199/92 P *Hüls* v *Commission* ECLI:EU-:C:1999:358, para. 162; Case C-49/92 P *Commission v Anic Partecipazioni* ECLI:EU:C:1999:356, para 121.

[93] *Eturas and Others* (n 83) para 48.

[94] Guidelines on Horizontal Agreements (n 84) para 373.

[95] 'Data sharing and competition law' https://data.europa.eu/en/publications/datastories/data-sharing-and-competition-law last accessed 8 August 2024.

[96] Guidelines on Horizontal Agreements (n 84) para 373.

[97] ibid para 418.

[98] Davila (n 20).

Under EU competition law, the legality of information exchanges is assessed on a case-by-case basis. The same approach would apply to exchanges between undertakings that rely on a blockchain to share data, including to cases of blockchain interoperability. Blockchain interoperability could lead to more firms having access to a larger dataset. This would increase the risk of competing firms obtaining commercially sensitive information, thereby increasing the potential of collusion. Additionally, interoperability might result in higher market concentration, since a single interoperable blockchain could replace previously competing DLTs. On the other hand, the increased degree of data sharing enabled by blockchain interoperability could help resolve certain information asymmetries that individual DLTs cannot address, opening up opportunities for developing innovative products.

Specific measures would need be implemented to limit the risk of sharing commercially sensitive information via blockchain interoperability. Firstly, sensitive data such as future pricing should not be shared via a DLT. Secondly, only historical and aggregated data should be shared, avoiding disclosure of individual firm's future market strategies. Finally, technical solutions could be developed to limit the potential collusive impact of data sharing via interoperable blockchains: for instance, commercially sensitive data could be stored on a 'sidechain' that is accessible only to non-competing firms.

As a practical example, consider three distinct DLTs developed by a group of banks, a group of insurance companies, and a few boutique firms operating in the private banking sector. Each DLT is designed to enable its members to share customer data in order to facilitate the development of targeted financial and insurance products. If interoperability among the three blockchains was achieved from a technical point of view, these separate DLTs could be replaced by a single interoperable chain. This would grant a larger number of participants access to a more comprehensive dataset. The higher degree of market concentration and the increased data access could raise the risk collusion, however, especially in markets where the activities of these three groups overlaps. On the positive side, as mentioned earlier, the interoperable blockchain could address information asymmetries: by having access to a larger pool of customer data, blockchain participants could develop more personalized and innovative financial and insurance services for their clients. To mitigate the risk of sharing commercially sensitive information, blockchain participants could avoid exchanging such data and instead store it on sidechains.

Competition law is technology-neutral: the specific technical approach to blockchain interoperability is therefore irrelevant. Whether interoperability is achieved through notary schemes, Hash-Locking, side chains or relay chains, all can potentially generate the same collusive risks discussed above. Any blockchain interoperability solution would thus require a case-by-case analysis under Art. 101 TFEU, its collusive potential depending on the type and modality of data exchanged.

A further point of discussion concerns the reversed burden of proof in cases of concerted practices involving systemic exchange of information, as established by the CJEU. Considering the *Eturas* case law,[99] it would be highly difficult – if not impossible – for a firm to claim it did not have access to the sensitive information exchanged via a blockchain. Given that every blockchain user typically has access to the entire dataset, they would be presumed liable for a breach of Art. 101 TFEU if sensitive business information is systematically exchanged among competitors. This presumption applies not only to individual blockchain but also to multiple interoperable blockchains.

[99] *Eturas and Others* (n 83).

A final issue to consider is the competitive relationship between the different members of a blockchain. Firms relying on the same DLT are not necessarily competitors. A blockchain may include firms operating in different markets or at various levels of the supply chain, all using a common DLT to pull together their data or carry out specific transactions. As demonstrated in the judgement of the US District Court of Southern Florida in *United Am. Corp. v. Bitmain Inc.,*[100] if the firms involved in the same blockchain are not direct competitors, it would be quite hard for the plaintiff to prove that the defendants engaged in a joint collusive strategy. In the case, United American Corp. alleged that a group of firms involved in Bitcoin mining conspired during a major software upgrade (i.e. the 'hard fork') that took place on 15th November 2018. The plaintiffs claimed that the defendants coordinated their voting rights during the software upgrade to maintain the existing Bitcoin architecture, thus violating Section 1 Sherman Act. However, the Court dismissed the claim, partly because the defendants included non-competing firms. The group included firms engaged in Bitcoin mining, as well as in the manufacturing of chips used by mining computers and by firms engaged in cryptocurrencies exchange, making collusion unlikely. Although this case was decided under U.S. Section 1 of the Sherman Act, its reasoning could be applied, *mutatis mutandis,* to similar cases under Art. 101 TFEU.

3.2.2. Anti-competitive foreclosure

A. Competition law assessment

Broadly speaking, foreclosure refers to a situation where a company restricts the access of its competitors to the market. This can occur in two main ways:[101] (1) upstream/input foreclosure whereby a company is denied access to an essential supplier or an essential input for production; and (2) downstream/customer foreclosure whereby a firm is denied access to important buyers. These practices can harm competition by limiting rivals' ability to compete effectively, potentially leading to higher prices, reduced quality, and stifled innovation. EU competition law addresses both upstream and downstream market foreclosure using a variety of tools.

Art. 101 TFEU prohibits collusive practices among competitors that aim at boycotting a third party, which is typically considered a restriction by object and thus *per se* prohibited under competition law.[102] Upstream and downstream foreclosure is also addressed under Art. 101 in the context of vertical agreements, meaning agreements between undertakings that operate at different levels of supply chain and therefore do not compete within the same relevant market (e.g. manufacturer-wholesaler; wholesaler-retailer).[103] Additionally, upstream foreclosure can be sanctioned under Art. 102 TFEU. A dominant firm that controls an essential facility (e.g. IP rights, infrastructure in a network industry) may abuse its position by refusing access to the facility to a competitor.[104] Alternatively, it could grant competitors access to the facility but under less favourable or discriminatory terms compared to its own subsidiaries.[105] Refusal to deal is an example of upstream foreclosure, which is deemed abusive conduct under Art. 102 TFEU. Potential foreclosure can also be scrutinized by competition authorities during merger review. When firms notify a concentration that substantially increases market concentration, the competition authority assesses whether the merging parties

[100] US District Court of Southern Florida, *United Am. Corp v. Bitmain Inc.* Decided on 31st March 2021. 530 F. Supp. 3rd 1241.

[101] European Commission, Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertaking [2008] OJ C 265/6, para 30.

[102] Guidelines on Horizontal Agreements (n 84) para 284.

[103] According to the Vertical Block Exemption Regulation, if the parties engaged in a vertical agreement each have a market share below 30% of their relevant market, they are presumed not to have a sufficient degree of market power that could lead to the foreclosure of competing firms both in the upstream and downstream market: Commission Regulation (EU) 2022/720 of 10 May 2022 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices [2022] OJ L 134/4, Art. 3.

[104] Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs*, ECLI:EU:C:1998:569.

[105] See Case C-42/21 P *Lietuvos geležinkeliai AB v. European Commission* ECLI:EU:C:2023:12; Case C-165/19 P *Slovak Telekom a.s. v. Commission* ECLI:EU:C:2021:239.

could, in the future, have the incentive and ability to foreclose competitors from the market.[106] To sum up, foreclosure is a common theory of harm in EU competition law, and could also be relevant in investigations involving undertakings operating a DLT.

With the exception of boycotting, which is considered *per se* prohibited under Art. 101 TFEU, foreclosure requires defining the 'relevant market'[107] and assessing 'market power' under Art. 102 TFEU. A firm gains market power by holding a substantial share of a relevant market, typically characterized by high and stable entry barriers (e.g. regulatory permission to operate, economies of scale). Additionally, firms with market power often control key assets, such as IP rights, network infrastructure, or state concessions. To have the ability to foreclose a competitor from the relevant market, a firm must possess substantial and stable market power, amounting to dominance under Art. 102 TFEU.

B. Application to blockchain interoperability

The European Commission examined a potential input foreclosure in the context of blockchain in the *Archipels* case.[108] In 2019, French public financial institution Caisse des Dépôts et Consignation, energy providers EDF and Engie, and postal operator La Poste concluded a joint venture agreement aimed at establishing a private DLT system to share customer data. Archipels, a private permissioned blockchain, was supposed to verify the authenticity of the documents collected by its members from individuals; this would make Archipels the first provider of blockchain-based certification service in France. The joint venture was notified to the Commission under the EU Merger Control Regulation. In the substantive assessment, the Commission investigated whether EDF and Engie would have the ability and incentive to foreclose access to their data by giving an exclusive access to Archipels.[109] Interestingly, the Commission did not analyse in its decision whether and to what extent Archipels members would rely on the blockchain to exchange sensitive information.[110] Firstly, Archipels members were not direct competitors. Secondly, Archipels did not intend to share confidential information among its members, but simply verify the validity of the documents stored on the blockchain and add a digital verification stamp.[111]

The Commission's decision focused on the vertical relationship between EDF and Engie (i.e., the main energy providers in France) and Archipels. As EDF and Engie had access to a large customers dataset, the Commission analysed whether and to what extent EDF and Engie could grant exclusive data access to Archipels, potentially generating a downstream foreclosure for other energy companies in France.[112] The Commission concluded that EDF and Engie lacked both the ability and the incentive to foreclose other energy operators: those operators could access customer data through third parties, such as water and telecom providers. Moreover, internal documents revealed that it would be more profitable for EDF and Engie to sell their data to third parties than to maintain exclusive control.[113] Based on these considerations, the Commission approved the transaction, authorizing the establishment of Archipels.

[106] Guidelines on non-horizontal mergers (n 101) paras 93-110; European Commission, Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings [2004] OJ C 31/5, para 61.

[107] Products and geographic area considered interchangeable by customers: Communication from the Commission, Commission Notice on the definition of the relevant market for the purposes of Union competition law [2024] OJ C/2024/1645.

[108] European Commission, Case M.11008 - *CDC GROUP / EDF / ENGIE / IN GROUPE / ARCHIPELS,* Art. 6(1)(b), Non-Opposition Decision, adopted on 17th April 2023.

[109] Antoine Babinet and David Dubois, 'Archipels Case: EU's First Merger Control Analysis of a Private Blockchain Consortium' (2021) 12 Journal of European Competition Law and Practice 630, 630.

[110] ibid.

[111] ibid.

[112] ibid.

[113] ibid.

Archipels is the only case where the Commission has had the opportunity to analyse the foreclosure effect in the context of a private blockchain consortium. This case represents well the limitations of applying the foreclosure theory of harm to blockchain technology. Data is an essential input that can be stored, verified, and shared via DLTs. At the same time, data is usually a non-rivalrous resource, meaning the user can provide their data to different operators (a concept known as 'multi-homing'); only in rare cases can a firm collect and process data exclusively. In view these peculiarities of data, it is unlikely that a group of firms could use a DLT to foreclose competitors by denying access to data stored on a blockchain. This scenario becomes even less plausible if the blockchain is permissionless or public, of if there is blockchain interoperability. Interoperability between different DLTs would increase the degree of data sharing across various blockchains, making it harder for blockchain operators to block third parties from accessing the data.

To sum up, while the theory of anti-competitive foreclosure is well-established in EU competition law, it appears to have limited relevance in the context of blockchain technology. The *Archipels* case demonstrates that DLT users generally lack both the ability (i.e. in terms of market power) and the incentive to foreclose data access for competing firms. This is particularly true for permissionless or public blockchains, as well as in cases where blockchain interoperability exists.

3.2.3. Standardization

A. Competition law assessment

From a legal perspective, blockchain interoperability standards are likely to become one of the key touchpoints between blockchain technology, competition law, as well as intellectual property law. According to the 2023 Commission's Guidelines on Horizontal Agreements, standardization aims to define 'the technical or quality requirements with which current or future products, production processes, … services or methods may comply.'[114] The development of common industry standards through Standard Development Organizations (SDOs) is crucial for ensuring interoperability between products from different manufacturers, which is particularly important in the ICT sector.

Due to its benefits, standardization is generally considered pro-competitive. However, SDOs can also be misused by industry players to coordinate prices or their future market behaviour, or to limit technical development and innovation.[115] In addition, the standardization process could exclude certain competitors. For example, standards mandating the exclusive use of a specific technology can have a foreclosing effect in relation to competing technologies developed by other market players.[116] Finally, once the standard is established, holders of patents deemed 'essential' for the standard implementation (i.e. Standard Essential Patents, SEPs) may exploit their market power by imposing excessive and discriminatory patent licensing conditions on companies seeking to implement the standard in their products. Holders of standard essential patents may also threaten patent implementers with a court injunction for a patent violation if these companies do not accept the proposed licensing conditions, a tactic known as a hold-up strategy.[117]

[114] Guidelines on Horizontal Agreements (n 84) para 436.

[115] ibid paras 441-442.

[116] ibid para 443.

[117] ibid para 443.

While collusive practices among SDO members are considered *per se* prohibited under Art. 101 TFEU, foreclosure strategies may be assessed as 'effect' cases and could be justified under Art. 101(3). An effect-based analysis of a standardization agreement under Art. 101 TFEU would consider several factors. These include whether industry players have the ability to introduce 'alternative standards' alongside those defined by the SDO,[118] and whether the technical specifications of the standard are freely accessible.[119] It is also crucial to assess whether participation in the SDO is open to any industry player willing to contribute to the standardization process.[120] Additionally, the market share of goods and services implementing the agreed standard should be examined.[121] Finally, it is important to ensure that any patents relevant to the standard are disclosed before the standard's adoption by the SDO.[122]

Hold up strategies by the holders of SEPs can be assessed as an abuse of dominance case under Art. 102 TFEU. To limit the risk of a hold up strategy, SEP holders are typically required by SDOs to commit to licensing their patents to any willing licensee on fair, reasonable, and non-discriminatory (FRAND) terms.[123] In addition, in the *Huawei* ruling,[124] the CJEU established a negotiation framework that both the SEP holder and the potential licensee should follow: the SEP holder may only seek a court injunction if the implementer fails to engage in negotiations. If the SEP holder seeks a court injunction for patent infringement without adhering to this negotiation framework*,* it would breach Art. 102 TFEU. In *Huawei*, however, the CJEU did not discuss the meaning of FRAND, and the EU Commission has yet to sanction excessive licensing rates (i.e. non-FRAND terms) as an exploitative abuse of dominance under Art. 102(a) TFEU. This possibility has primarily been discussed in the literature.[125]

B. Application to blockchain interoperability

As already evident from the ongoing activities related to blockchain standardization, interoperability standards are expected to play a critical role in blockchain evolution and uptake. The International Standards Organisation (ISO) established a Technical Committee (ISO/TC 307) dedicated to blockchain and distributed ledger technologies.[126] The Committee includes one group on interoperability (SG 7) and indicates 'interoperability between different ledger technologies and between ledger technologies and other system components' as an expected benefit.[127] One document currently under review by the Committee is 'Interoperability Framework' for blockchain and DLT.[128] At the same time, the Institute of Electrical and Electronics Engineers (IEEE) has published an IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol and an Approved Draft Standard for Blockchain Interoperability Naming Protocol.[129] A Standard for Blockchain Interoperability – Cross Chain Transaction Consistency Protocol – is currently under review by the IEEE. Other organizations involved in the standardization of blockchain interoperability include the European

[118] ibid para 464.

[119] ibid para 465.

[120] ibid para 467.

[121] ibid para 472.

[122] ibid para 473.

[123] ibid para 451.

[124] Case C-170/13 *Huawei Technologies Co. Ltd v. ZTE* ECLI:EU:C:2015:477.

[125] See e.g., Niccolò Galli and Marco Botta, 'It's Unfair! Non-price Exploitation in ICT Patents Licenses' (2023) 54 International Review of Intellectual Property and Competition Law 200; Marco Botta, 'The challenge of sanctioning unfair royalty rate by the SEP holder: "when", "how" and "what"' (2021) 44 World Competition 3 https://doi.org/10.54648/woco2021002; Marco Botta, 'Non-Discrimination in Standard Essential Patents; ND Prong v. Art. 102(C) TFEU' (2021) 17 Journal of Competition Law and Economics 947 https://doi.org/10.1093/joclec/nhab011.

[126] See https://www.iso.org/committee/6266604.html last accessed 26 July 2024. For more on the Committee, see e.g., 'Blockchain Standardization: Decoding ISO/TS 307 for Global Impact' (*Future Citizen News,* 26 August 2023) https://www.futurecitizen.news/article/iso-tc-307-the-comprehensive-guide-to-global-blockchain-dlt-standardization last accessed 26 July 2024.

[127] ISO/TC 307 Strategic Business Plan.

[128] As noted on the ISO webpage, the document under review 'specifies a framework, recommendations and requirements for interoperability between DLT systems, between DLT and entities outside the DLT system, the relationship and interactions between these and cross-cutting aspects': https://www.iso.org/standard/82098.html last accessed 22 November 2024.

[129] See https://blockchain.ieee.org/standards last accessed 24 November 2024.

Telecommunications Standard Institute (ETSI)[130] and the Joint Technical Committee 19 (JTC19) set up by the European Committee for Standardisation and the European Committee for Electrotechnical Standardization (CENELEC).[131] All in all, interoperability is considered the critical area in blockchain technology that stands to benefit most from cohesive and collaborative standardization, followed by issues of identity, smart contracts, governance, and security.[132]

Establishing common technical standards is crucial to fostering interoperability among different blockchains. To be compatible with Arts. 101 and 102 TFEU, the standardization process must comply with the requirements mentioned above. In particular, standardisation should be open to all players in the blockchain industry, and the technical specifications of the standard should be freely accessible. In case the agreed standard involves specific patents considered essential for its implementation, the SEP holder must disclose the patent(s) before the standard is adopted within the SDO and commit to licensing it on FRAND terms. Overall, blockchain interoperability is unlikely to present new legal challenges in comparison to those previously encountered in mobile technology standardization. The likelihood of legal disputes in this area will depend on the number and significance of SEPs involved in blockchain interoperability standards.

3.3. Data protection law

Even though blockchain interoperability is still far from being fully realized, advancements in this area bring to light emerging concerns that require attention. While existing research reveals that blockchain interoperability can amplify in particular security vulnerabilities, privacy and data protection emerge as other critical areas that must be closely monitored.[133]

In the EU, data protection is a fundamental human right enshrined in Art. 8 of the Charter of Fundamental Rights of the European Union[134] and in Art. 16 TFEU. The General Data Protection Regulation (GDPR)[135] provides a primary legislative framework that harmonizes personal data protection across the EU. It pursues two main objectives: safeguarding fundamental rights and freedoms, in particular the right to data protection, and ensuring the unrestricted movement of personal data.[136] The GDPR is applicable to all organizations that process personal data of individuals based in the EU.

[130] See in particular the activities on Permissioned Distributed Ledgers (PDL): https://www.etsi.org/technologies/permissioned-distributed-ledgers accessed 22 November 2024.

[131] See CEN-CENELEC, ‘Digital in Standards: Supporting the Digital Transition Through Standardization’ (2021). For a more complete overview of organizations involved in blockchain standardisation, see e.g., European Commission, ‘Blockchain standards’ https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards last accessed 22 November 2024.

[132] European Commission, Rolling Plan for ICT Standardization, Blockchain and Distributed Digital Ledger Technologies (RP2024) https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/blockchain-and-distributed-digital-ledger-technologies-rp2024 last accessed 28 November 2024.

[133] E.g., André Augusto et al., ‘SoK: Security and Privacy of Blockchain Interoperability’ (2024) 2024 IEEE Sumposium on Security and Privacy (SP).

[134] Charter of Fundamental Rights of the European Union, 2000/C 364/01.

[135] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119.

[136] Art. 1 GDPR.

Data processed and stored on blockchains can clearly include personal data, rendering the GDPR applicable to data processing operations on blockchain.[137] Logically, blockchain interoperability solutions underpinned by the very idea of data exchanges must also ensure compliance with the GDPR whenever personal data processing is involved. The aim of this section is to provide an overview of selected potential data protection challenges posed by blockchain interoperability. While the focus in this section is on three issues, namely accountability and controllership, data minimization and purpose limitation, and the right to be forgotten, it should be underscored that blockchain interoperability may also trigger other data protection issues.

3.3.1. Accountability and controllership

Accountability is one of the main principles of the GDPR ensuring that the controller is responsible for and able to demonstrate its compliance with the data protection provisions.[138] In relation to blockchains and blockchain interoperability, accountability presents some crucial challenges.

One of such challenges relates to the identification of a 'data controller' or 'joint controllers'. Art. 4(7) GDPR defines the controller as 'the natural or legal person, public authority, agency or other body with, alone or jointly, determines the purposes and means of the processing of personal data'. The GDPR also envisages in Art. 26 the existence of joint controllers, who 'jointly determine the purposes and means of processing'. In relation to blockchain-based data processing operations, it might be unclear who determines the purposes and means of data processing. In decentralized blockchain networks, there are numerous participants involved in a series of transactions. In relation to public blockchains, this implies that no actor can influence the determination of the purposes and means of data processing.[139] A range of actors may thus qualify as controllers: for example, software developers, miners, nodes, or users.[140] Identifying a controller or joint controllers might be easier in the context of private blockchains, as in such cases there is commonly a legal entity – a company or a consortium – determining the means and purposes of data processing, hence qualifying as a data controller.[141] It has also been argued that individual companies joining the consortium can be qualified as joint controllers for the purpose of the GDPR.[142]

When considering interoperable blockchain, where multiple networks interact with each other, the challenge of identifying controllers becomes even more pronounced. Unlike single-blockchain ecosystems, interoperable blockchains may involve many networks and a diverse array of participants across these networks, each of whom may have different roles, responsibilities, and degrees of influence over data processing activities.

Problems with assigning controllership raise serious issues for GDPR compliance. For example, controllers must comply with all the principles listed in Art. 5 GDPR. These include the principles of lawfulness, fairness and transparency, purpose limitation (discussed in more detail in the following section), data minimization, accuracy, storage limitation, as well as data integrity and confidentiality. The ambiguity regarding controllership has also repercussions for the rights of data subjects: who is ultimately liable, and to whom should data subjects turn to enforce their rights, such as the right to access or the right to object? This is an unresolved issue in the context of blockchains and can further complicate compliance if blockchains become interoperable.

[137] Under the GDPR, the term 'personal data' is interpreted broadly: it is 'any information relating to an identified or identifiable natural person' (Art. 4(1)). This extensive interpretation was confirmed by the CJUE: see, e.g., Case C-604/22 *IAB* Europe ECLI:EU:C:2024:214, paras 35-41. Similarly, 'data processing' is understood broadly, as 'any operation or set of operations which is performed on personal data or on sets of personal data' (Art. 4(2)). Even though there is a 'household exemption' envisaged in Art. 2(2)(c), Fink noted that it is unlikely that this exemption can apply to data processing through blockchains: Michèle Fink, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?' (2019) EPRS Study, Panel for the Future of Science and Technology, 13.

[138] Article 5(2) GDPR. See also Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (13 July 2010).

[139] Fink (n 137) 42-44.

[140] ibid 45-48.

[141] ibid 44-45.

[142] ibid 45.

3.3.2. Data minimization and purpose limitation

Data minimisation and purpose limitation are among the main principles in data protection law. Art. 5(1)(b) GDPR stipulates that data shall be 'collected for specified, explicit and legitimate purposes' (purpose specification requirement) and that it shall not be 'further processed in a manner that is incompatible with those purposes' (compatible use requirement). It also envisages exceptions that include further processing for the public interest, research, and statistical purposes.

Considering that interoperability solutions – be it in the context of blockchain or elsewhere – aim at removing technical obstacles to exchanging data, their underpinning rationale is to increase data sharing across networks. The risk to the principle of purpose of limitation is thus one of the most evident challenges arising in relation to cross-chain interoperability that must be thoroughly considered, along with potential measures to mitigate the envisaged risks. In relation to interoperability and data protection law, the European Data Protection Supervisor (EDPS) noted the following:

'[t]he EDPS recalls that a technological environment with information systems that are not inter-operable with each other has provided a very strong safeguard against the violation of the fundamental data protection principle of purpose limitation. […] Technical non-feasibility has made it harder to use large amounts of data for purposes for which they were not collected. Removing that technical barrier requires consciousness for the legal limitations and might also warrant new safeguards to ensure lawfulness of the processing and accountability'.[143]

Even though this statement has been expressed in a context unrelated to blockchain interoperability, the insights expressed by the EDPS are equally applicable to the ongoing cross-chain interoperability efforts. This is not to say, however, that interoperability and data protection cannot co-exist, or that interoperability is not an objective worth pursing – to the opposite. Many exchanges facilitated through interoperable blockchains might not involve personal data in the first place. It can also well be that further data processing facilitated by interoperability is compatible with the purpose for which the data was initially collected; in such case the requirement of compatible use is fulfilled.

In case potential incompatibility issues arise, however, to address the tension with the GDPR's requirement of compatible use, users of blockchain platforms that embark on interoperability must introduce the necessary measures and safeguards. Importantly, it should be noted that the fact that further processing serves a different purpose than the original one does not automatically render it incompatible with data protection law; this has to be established on a case-to-case basis.[144] Factors that are considered in conducting this assessment include the relationship between the initial and new purposes, the context of data collection and data subjects' reasonable expectations related to further processing, data's nature and the impact of further processing on data subjects, and the safeguards implemented by the controller.[145] Such safeguards range from increased transparency vis-à-vis data subjects as well as the introduction of technical or organisational measures such as anonymization or pseudonymization.[146]

[143] European Data Protection Supervisor, 'Opinion 1/2023 on the Proposal for an Interoperable Europe Act' (2023) para 7.

[144] Article 19 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation' (2013) 21.

[145] ibid 23-26.

[146] ibid 26.

If the purpose(s) for which personal data is further processed in the context of interoperability exchanges is incompatible with the initial purpose(s), a new legal basis for data processing might also be established, alongside with the provision of information about the purposes of further processing. Even though user consent might be the most relevant legal basis in this context,[147] whether and how a data subject can provide a free, specific, informed and unambiguous consent[148] for data processing in a blockchain environment remains an unresolved issue.[149] Furthermore, for consent to be freely given, the data subject must be able to withdraw it at any time without detriment. Withdrawal implies that processing operations must cease, and personal data must be erased. However, as the next section explains, achieving data erasure on a blockchain is challenging due to its 'immutability': once the chain that store the data is created, it is difficult to modify it.[150] Blockchain interoperability thus further exacerbates the challenges related to the application of the basic provisions of the GDPR in the blockchain environment.

3.3.3. The 'right to be forgotten'

The 'right to be forgotten' was first established by the CJEU in *Google Spain*[151] and later codified in Art. 17 GDPR. This right allows data subject to request a controller to erase/delete his/her personal data. However, the right to be forgotten is not absolute. First, the data subject can only exercise this right in specific situations listed in Art. 17(1).[152] For example, the data subject may request data erasure if he/she have withdrawn his/her consent to data processing. However, the request cannot be fulfilled if the controller processes the data to comply with a legal obligation. Second, Art. 17(2) GDPR imposes additional limitations when the data has been made 'public' by the controller. In such cases, the controller must take 'reasonable steps', including implementing technical measures, to comply with the request for erasure, considering the available technology and the costs of implementation – i.e. a proportionality test to assess the practical feasibility of erasing data. The controller should also inform other controllers processing the data that has become public of the data subject's request to erase their data. However, Art. 17(2) GDPR does not clarify whether the original controller is liable in case the additional controllers do not comply with the data subject's request. Lastly, Art. 17(3) GDPR provides a list of exceptions where the right to be forgotten does not apply. In particular, the right to erasure should be balanced against other fundamental rights, such as freedom of expression and information. In *TU v. Google*,[153] the CJEU emphasised that this balance must be assessed on a case-by-case basis. In particular, if the data subject is a public figure with a 'degree of notoriety', it may be more difficult for them to enforce their right to be forgotten.[154]

[147] Article 6 GDPR envisages six different legal bases: consent, contract, compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in a public interest, and legitimate interest.

[148] Article 4(11) GDPR.

[149] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2018) 1 European Data Protection Law 17*,* 28. https://doi.org/10.21552/edpl/2018/1/6.

[150] Steve Wright and Ezgi Pilavci, 'Personal Data Protection in Blockchain' (2019) 3 Journal of Data Protection and Privacy 43, 44. https://doi.org/10.69554/ASWW3312.

[151] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ECLI:EU:C:2014:317.

[152] The following grounds are mentioned in Art. 17(1) GDPR: the personal data are 'no longer necessary'; the data subject 'withdraw consent' to the data processing and 'there is no longer legal ground for the processing'; the data subject 'object' to the data processing and there are no 'overiding legitimate grounds for the processing'; the personal data has been 'unlawfully processed'; personal data have to be erased in accordance with a legal obligation; personal data has been unlawfully collected to offer a digital service to a child.

[153] Case C-460/20 *TU, RE v. Google* ECLI:EU:C:2022:962.

[154] ibid para 60.

Art. 17 GDPR does not provide specific examples for its practical application. The provision uses the terms 'forget' and 'erase' interchangeably, without clarifying how a data controller could comply with the data subject's request. The CJEU's jurisprudence is similarly ambiguous. In *Google Spain*,[155] the CJEU recognised the 'de-referencing' of the individual's name from a search engine as an example of exercising the right to be forgotten. De-referencing does not require the search engine to delete the data entirely; instead, it mandates that the search engine no longer display certain personal data in search results. Conversely, in *Nowak,*[156] the CJEU appeared to suggest that controllers may need to 'destruct' personal data following a request by the data subject under Art. 17 GDPR. This illustrates the differing interpretations of what 'erasure' entails in practice.

The precise meaning of the term 'erase' is an important unresolved issue in the context of applying the right to be forgotten to blockchain technology. The essence of the right forgotten appears to be fundamentally at odds with a central feature of blockchain technology - i.e. its capacity to record transactions permanently, unalterably, and indelibly. Achieving blockchain interoperability would further complicate compliance with Art. 17 GDPR. Interoperability between blockchains means that the number of controllers responsible for enforcing a data erasure request would increase. Additionally, interoperability implies that personal data would be stored permanently on multiple chains, further complicating the process of erasing data.

A few authors have argued in favour of a flexible interpretation of Art. 17 GDPR, suggesting that blockchain technical solutions could facilitate the implementation of the right to be forgotten.[157] Ibáñez et al., for instance, propose a 'hashing-out' technical solution, where personal data intended for erasure would be stored in a separate 'hash' outside of the shared blockchain.[158] Alternatively, the authors argue in favour encryption methods that would 'hide' the personal data to be erased, rather than 'delete' it. These technical approaches could also be relevant in the context of blockchain interoperability.

Another unresolved issue in Art. 17 GDPR is the geographic scope of the right to be forgotten. Although the GDPR has an extra-territorial scope of application, in *Google v. CNIL*[159] the CJEU seemed to suggest that the enforcement of this right should not extend beyond the EU. In the judgement, the Court ruled that Google was only required to de-reference the name of one EU citizen in relation to search engines domains based in the EU Member States.[160] Google was not required under Art. 17 GDPR to comply with an erasure request for its search engines domains outside the EU. The Court clarified that the right to de-referencing (i.e. the right to be forgotten) does not exist outside of the EU,[161] and the GDPR currently lacks mechanisms for cooperating with authorities in third countries to enforce de-referencing requests.[162]

Most DLTs function as global chains that extend well beyond the EU, and interoperability could extend the 'length' of individual blockchains, further complicating the enforcement of Art. 17 GDPR. Nevertheless, the restrictive approach to the extra-territorial enforcement of the right to forgotten taken by the CJEU in *Google v. CNIL* marks an important development in this area. In the context of blockchain technology, this ruling could confine the enforcement of the right to be forgotten to nodes located within the EU territory, allowing for personal data to be 'hidden' through methods such as hashing or encryption.

[155] *Google Spain* (n 151).

[156] Case C-434/16 *Peter Nowak v. Data Protection Commissioner* ECLI:EU:C:2017:582.

[157] See in particular Finck (n 149) 17-35.

[158] Luis-Daniel Ibáñez, Kieron O'Hara and Elena Simperl, *On Blockchains and the General Data Protection Regulation* (2016) https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf last accessed 12 August 2024.

[159] Case C-507/17 *Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:772.

[160] ibid para 62.

[161] ibid para 61.

[162] ibid para 63.

In summary, reconciling the 'right to be forgotten' (i.e. right to erasure) enshrined in Art. 17 GDPR with the immutability of blockchains remains a largely unresolved challenge,. Blockchain interoperability may exacerbate this tension. Art. 17 GDPR can be reconciled with the peculiarities of blockchain technology only if a pragmatic interpretation of this provision is adopted, viewing the right to be forgotten as the right to 'hide' personal data rather than to permanently 'delete' it. By restricting the extra-territorial application of the right to be forgotten, the CJEU's ruling in *Google v. CNIL* embraces this pragmatic approach and opens the possibility for finding a suitable solution in the future.

4. Conclusions

Blockchain interoperability holds significant promise for unlocking the full potential of blockchain technology and broadening its application. In this article, which is the first to explore blockchain interoperability from a legal perspective, we explored how this emerging technology might impact EU competition law and data protection law.

Our analysis of competition law identified three potential areas that might be affected by blockchain interoperability: (1) collusion and information exchanges, (2) anti-competitive foreclosure, and (3) standardization. As regards the first area, blockchain interoperability can facilitate data exchanges, creating benefits such as reducing information asymmetries between blockchain market participants, fostering innovation, and enabling the creation of new products. However, such data exchanges may also increase the risk of collusion, triggering concerns under Art. 101(1) TFEU. The increased access to large datasets through interoperability mechanisms, no matter whether these are notary schemes, Hash-Locking, side chains or relay chains, could heighten concerns about competitors gaining access to commercially sensitive information. Addressing these risks requires a case-by-case analysis of the collusive potential of the data exchanges and the modalities employed.

In the context of anti-competitive foreclosure, we examined the potential of individual blockchains to embark on exclusionary data strategies - i.e. foreclosing access to data stored on a blockchain. We concluded that this scenario is unlikely to materialize in the context of blockchain interoperability, which increases the degree of data sharing across various blockchains, making it more difficult for blockchain operators to prevent third parties from accessing the data.

Blockchain interoperability standards will likely be a crucial nexus between blockchain technology and competition law. The importance of blockchain interoperability standards is evident from the activities of various standardisation bodies, including the ISO and IEEE. While establishing common standards is key to fostering blockchain interoperability, the standardisation process needs to comply with Arts. 101 and 102 TFEU. Among other requirements, standardisation must be open to all blockchain stakeholders, and the technical specifications of the standard should be freely accessible.

In addition to its impacts on competition law, blockchain interoperability can have also significant implications for EU data protection law, given that the data shared through interoperability solutions is likely to include personal data. This article examined three compliance challenges posed by blockchain interoperability: (1) accountability and controllership, (2) data minimization and purpose limitation, and (3) the right to be forgotten.

As one of the main principles of data protection law, accountability requires data controllers to be responsible for and demonstrate compliance with the GDPR. However, blockchain technology – and especially interoperable blockchains – makes it challenging to determine who qualifies as the controller responsible for determining the purposes and means of data processing. When considering interoperable blockchain, where multiple networks interact with each other, the challenge of identifying controllers becomes even more acute.

Blockchain interoperability might also impact data protection principles of data minimization and purpose limitation. By design, interoperability solutions aim to remove barriers to data exchanges, inherently increasing data sharing across networks rather than minimizing it. While not all blockchain interoperability solutions are necessarily expected to be incompatible with the GDPR, it is crucial to ensure that the purpose for which data is exchanges aligns with the original purpose, or that a new legal basis is established for such exchange. Additionally, relevant safeguards such as transparency vis-à-vis data subjects and implementing robust technical and organisational measures will be essential to ensure compliance with GDPR principles in this context.

Blockchain interoperability can also present challenges for the exercise of data subjects' rights, in particular the right to be forgotten. The immutability characteristics of blockchains is inherently at odds with the right to be forgotten, and interoperability may exacerbate this tension. A pragmatic interpretation of the right to be forgotten – such as interpreting it as a right to 'hide' personal data (via encryption methods) rather than permanently delete it – could help address this conflict.

Overall, the analysis presented in this article indicates that blockchain interoperability does not introduce entirely new legal issues compared to those already identified in the existing literature on the compatibility of blockchain technology with competition law and data protection law. By enhancing the degree of data sharing among different parties, blockchain interoperability may foster collusion and complicate compliance with the GDPR, especially in terms of accountability, data minimization, and purpose limitation. At the same time, blockchain interoperability could lower entry barriers in the market and reduce market concentration, thereby decreasing the risk of foreclosure practices.

In view of these considerations, the compatibility of blockchain technology with competition and data protection law should be assessed on a case-by-case basis. Both legal fields are technology-neutral. As a consequence, whether interoperability is achieved via notary schemes, Hash-Locking, sidechain, or relay solutions is irrelevant for assessing their compliance with competition and data protection law. In other words, regulators will not be asked to evaluate the lawfulness of these technical solutions, but rather the compatibility with the relevant rules of the manner in which these technologies are used by market participants.

Such self-compliance would be facilitated if regulators and courts clarified how the relevant legal framework applies in the context of blockchain interoperability. For example, market participants would benefit from a clarification of the exact scope of the right to be forgotten enshrined in Art. 17 GDPR. Similarly, the European Commission could adopt specific guidelines to explain to the potential compliance risks under Arts. 101 and 102 TFEU related to the use of blockchain technology, and specifically blockchain interoperability.

Besides clarifying the existing legal framework and providing guidance to the market participants, both competition and data protection authorities will need to face a 'detection problem': as with all new technologies, it will take time for regulators to understand how this technology functions and to assess claims put forward by third parties regarding alleged breaches of the existing legal framework.

To conclude, blockchain interoperability promises to expand the use cases of this technology beyond the world of cryptocurrencies. It has the potential to increase the degree of data sharing between different market players, generating both benefits and potential compliance challenges with existing competition and data protection rules in Europe. To ensure compliance with the EU legal framework, a vigilant and proactive approach by regulators will be necessary. The expected blockchain use cases brought by enhanced blockchain interoperability will certainly increase the degree of regulatory scrutiny. In the near future, competition authorities might need to pay particular attention to the ongoing standardisation efforts in the area of blockchain interoperability, as standardisation may become a crucial intersection between blockchain technologies and competition law.

Authors

Klaudia Majcher

Global Governance Program

European University Institute

klaudia.majcher@eui.eu

Marco Botta

Centre for a Digital Society

European University Institute

marco.botta@eui.eu