Part 2: Impacts on the Wider Landscape

Section 13

Competition

SECTION 13: COMPETITION

Brendan McGurk and Will Perry (Monckton Chambers)

Introduction

The principal purposes of competition law include enhancing consumer welfare (including through promoting innovation and price competition) and maximising productive and allocative efficiency by ensuring that competition takes place 'on the merits', requiring suppliers of goods and services to compete against each other on a level playing field and subject to rules and principles protecting the process of competition.[338]

Blockchain not only enables those seeking to transact business to do so without the traditional constraints of space (where one might need to transact in person) or time (where trading might be confined to office hours); it offers a way of transacting business digitally that is distinct from existing forms of online trading. The characteristics of a blockchain database offer many advantages over existing forms of digital trading: it provides a permanent, accurate record of transactions, that does not require the involvement of a 'middle-man' which, in the age of big tech often means two-sided platforms. Blockchain enables digital platforms to be run not centrally (as they are by the biggest tech companies like Amazon, Google and Facebook) but on a completely decentralised basis by all of those who participate in the particular chain. However, as discussed below, the technology is equally capable of facilitating concentrations of power and being used in a highly centralised fashion.

The potential competitive benefits that adoption of blockchain may bring are therefore apparent: if platforms can be operated by their participants on a decentralised basis, it is conceivable that users of those platforms may retain greater control of the content they produce on those platforms and thus the value of that content which might otherwise have been acquired by a powerful gatekeeper. One can see this, for example, in relation to blockchain's use for content distribution: the traditional model of content distribution tends to favour distributors over creators; blockchain technology may, by disrupting centralised platforms, eventually level the playing field.

As an example, YouTube provides a centralised platform enabling users to upload their content to the platform, albeit that YouTube will, as consideration for providing those hosting services, profit from that content. While many YouTubers make a healthy return, a very substantial proportion of revenues generated from their content ends up in YouTube's pockets. Blockchain offers an alternative to this model. For example, Flixxo, a decentralized content distribution platform, allows creators to offer their content to very specialized audiences, who pay cryptocurrency tokens to fund and enjoy their projects. To earn Flixxo tokens, participants in Flixxo simply make the videos on their computer available to the network on a peer-to-peer basis. Users in this decentralised model bear more of the running costs of the platform, but in turn retain more of the profits of the content they produce, not least since viewers will forego paying subscriptions to centralised platforms and can instead pay content providers directly.

Blockchain also gives online users more control over their data in relation to advertisers who would otherwise target them based on their knowledge of those users' browsing habits and preferences. Blockchain enables users to operate anonymously (or at least, pseudonymously), making it harder for those users to be identified and targeted by advertisers. New companies like Papyrus operate platforms that enable users to know exactly who is paying to advertise to them, and the source of the data about them on which those advertisers rely. Individuals can expressly identify their data-sharing preferences so that advertisers will know

[338] Of course some competition theorists, such as Robert Bork and the Chicago School, would contend that "antitrust laws, as they now stand, have only one legitimate goal, and that goal can be derived as rigorously as any theorem in economics … [- namely,] the maximisation of consumer welfare." The Antitrust Paradox (The Free Press, 1978 reprinted 1993), pp.50-51.

with certainty what type of adverts they wish to receive rather than seeking to profile individual users by parsing web-browsing and other online data which may be less accurate. These users can also decide not to share any of their browsing habits or other usage data, though in those circumstances, advertisers can offer to pay users directly for that data.

Blockchain is therefore capable of aggregating and distributing all of the online data that users create across the entire network, making it accessible to all potential advertisers on a level playing field for the acquisition of that data, thus enabling users to retain more of the value of the data trail they create, and promoting greater competition amongst those advertisers. This is in contrast to the situation were data acquired (through user agreement to company terms and conditions) is kept on secure company servers and put up for sale to bidders who wish to target those users, and where the revenues for that data is retained by selling companies, rather than users whose data is being sold. This promotes consumer welfare in giving users greater control over their data and privacy, ensuring that adverts are more accurately targeted and allowing users to monetise the value of that data, rather than advertisers paying Google or Facebook for the same. As Fred Ehrsam puts it:

> *"While some blockchain-based data will be encrypted and private, much of it will also be open out of necessity…this open data has the potential to commoditize the data silos most tech companies like Google, Facebook, Uber, LinkedIn and Amazon are built on and extract rent from. This is great for society: it incentivises the creation of a more open and connected world. And it creates an open data layer for AIs to train on."* [339]

Blockchain coupled with the use of smart contracts[340] will also promote competition in the context of property transactions, where blockchain platforms now allow real estate to be tokenized and traded like cryptocurrencies. Traditionally, properties for sale or lease have been listed through estate agents – again operating as a centralised platform on the supply side. As Deloitte have pointed out, new decentralised platforms may eventually assume the listing, payment and legal functions traditionally provided by intermediaries, thereby removing the middle-man, cutting transaction costs and increasing the speed at which such transactions might take place.[341] Tokenising assets like a house will facilitate joint ownership and will enable greater fluidity in buying and selling shares in individual properties. All of this will promote consumer welfare.

Competition law concerns

The distinction between permissioned and permissionless blockchains

Blockchains can be public/permissionless or private/permissioned. The distinction between these two general types has consequences for an analysis of how blockchains are capable of being instrumentalised to harm competition. Anybody can use public/permissionless blockchains, and users are anonymous. Private/permissioned blockchains, in contrast, are operated by a single entity or group of entities who control all aspects of the operation of the chain, and have developed protocols to govern their actions. Those features have the corollary that *"[p]rivate blockchains have the potential to lead to entrenchment of power within a blockchain system, as a select group of people can effectively act as gatekeepers because of the restricted access to digital keys"*. [342]In this section, we therefore focus principally on uses of private/permissioned blockchains. [343]

[339] Fred Ehrsam, Blockchains are a data buffet for Ais, Medium (6 March, 2017)

[340] A smart contract is a piece of computer code capable of verifying, executing and enforcing a set of instructions constituting an agreement between two parties. Smart contracts operate under a set of pre-conditions which, when satisfied, lead to the discharge of the obligations in the contract that were contingent on the satisfaction of those conditions. In the property context, a landlord might agree to give the tenant the door code to the rental property as soon as the tenant pays the security deposit. Both the tenant and the landlord would send their respective portions of the deal to the smart contract, which would hold onto and automatically exchange the door code for the security deposit on the date the lease begins.

[341] https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html

[342] Alex Latham, 'Blockchain and Competition Law' (2020) 41 E.C.L.R, p. 602, available here: https://www.bristows.com/app/uploads/2021/01/2020.12-ECLR-Blockchain-and-competition-law.pdf

[343] For a more complete taxonomy of blockchains see (which considers public/permissioned and private/permissionless types), see EY's "Discussion Paper on Blockchain Technology and Competition" of April 2021, p. 11, available here: https://www.cci.gov.in/sites/default/files/whats_newdocument/Blockchain.pdf. For a discussion of the potential interaction

All that follows should be read subject to the fact that there is nothing inherently anticompetitive about the uses of blockchain. However, for all the potential benefits to consumers, there are also a large number of competition law concerns. We have addressed those concerns as follows. First, we address potential harms to competition falling within the scope of Article 101 TFEU / the Chapter I Prohibition under the Competition Act 1998. Second, we consider potential harms falling under Article 102 TFEU / the Chapter II Prohibition under the Competition Act. Third and finally, we reflect on potential enforcement problems.

The three overarching conclusions that emerge from this analysis are:

— Competition concerns arising out of uses of blockchain can be effectively analysed under the existing analytical framework for competition harms. As is apparent below, possible anti-competitive conduct falls into existing categories of infringements. In this regard, we agree with Thibault Schrepel, the leading commentator on the competition law implications of blockchain, that the applicable theories of harm *"are entirely standard concerns that competition agencies already investigate in all manner of different market settings involving other types of technology"*. [344]

— The types of competition law harms that will arise in this context are likely to depend on two main factors: (a) the extent of transparency / data sharing within the blockchain and (b) the extent to which power is concentrated in the hands of the blockchain owner(s). Although the underlying technology may be the same, there is no one-size-fits all approach to evaluating anticompetitive conduct involving blockchain.

— Perhaps the greatest challenge blockchains present for competition lawyers and regulators is enforcement. As with the likely competition law harms, enforcement challenges will depend on the blockchain's degree of transparency and concentration of power.

1. Potential competition harms within the scope of Article 101 TFEU / Chapter I Prohibition

Article 101 TFEU and the Chapter I Prohibition in UK competition law (s.2 of the Competition Act 1998) prohibit *"agreements between undertakings, decisions by associations of undertakings or concerted practices"* which *"have as their object or effect the prevention, restriction or distortion of competition"* within the internal market (Article 101) or which may affect trade within the United Kingdom (the Chapter I Prohibition).

Consortia and access

Permissioned blockchains are often consortium platforms. By way of indication as to the prevalence of blockchain consortia, in August 2017 more than 40 had been set up globally, including, for example, PTDL (Post-Trade Distributed Ledger Group), B3i (Blockchain Insurance Industry Initiative) and the R3 Consortium, which developed the Corda distributed ledger platform to facilitate synchronised peer-to-peer contract execution.[345]

Access to private/permissioned blockchains or consortia depends on the authorisation granted by the owner or owners of the chain. Potential competition law infringements arising from refusal to grant access are also considered in our discussion of potential Article 102/Chapter II Prohibition infringements below. From the perspective of Article 101/the Chapter I Prohibition, if competitors within a

between collusive agreements and public blockchains, see Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", Harvard Journal of Law and Technology (2019), pp. 128-133, available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315182.

[344] https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf

[345] For more detail see Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", King's College London Dickson Poon School of Law Legal Studies Research Paper Series (2019-2020), p. 2-3, available here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256728.

market use a single blockchain, then there are inherent features of that chain that may cause concern. Those features are, in the broadest terms: (i) data transparency between competitors; (ii) co-operation between competitors; and (iii) the presence of mechanisms that can control transactions/competitor behaviour (in particular, smart contracts). Those three features and combinations thereof are discussed in the following paragraphs in the course of the discussion as to how blockchain has the potential to cause Article 101/Chapter I Prohibition harms.

Information exchange: horizontal and vertical

If competitors are able, through their membership of a consortium, to access information about the price at which they are entering into transactions and/or the level of rebates or discounts they are offering customers, that will reduce price competition and constitute a form of information sharing that violates competition law. If pricing of products begins to coalesce as a result of such information sharing, that would be clear evidence of coordination or collusion in breach of, in particular, the Chapter I prohibition. Similar risks arise if competitors each have access to each other's customer lists, costs, volumes of sales, etc, as this would also likely constitute unlawful information exchange. As ever, the exchange of information that relates to competitors planned future conduct on the market in question carries the greatest risk of violating competition law. Participants in a chain on which competitors operate will therefore have to consider the governance rules and software protocol, and the extent to which they permit rivals to obtain access to that very type of information. It may be sufficient, at least in some cases, to encrypt such information.

It is crucial also to consider that where vertically-related parties are members of the same blockchain, data transparency (and/or use of smart contracts) may facilitate anti-competitive regulation by upstream entities of their downstream buyers through, for example, resale price maintenance (i.e. preventing distributors from discounting their price, which eliminates intra-brand competition) and selective distribution agreements (i.e. which stipulate that sales may be made only through certain channels).

To date there have been only a few competition cases on internet selling, but when presented with the opportunity the CJEU and the UK Court of Appeal have not held back from analysing online sales and distribution agreements through the lens of Article 101 TFEU. In Ping Europe Ltd v CMA [2020] 4 CMLR 13, the Court of Appeal noted[346] that EU law considers website sales to be a form of "passive selling" (i.e. sales in response to unsolicited orders), and classifies agreed restrictions on such selling (e.g. through selective distribution) as "hardcore" restrictions on sales to end purchasers, which in turn are considered to be equivalently anti-competitive to "object" restrictions on competition under Article 101 TFEU/the Chapter I Prohibition. In Case C-230/16 Coty Germany GmbH v Parfümerie Akzente GmbH [2018] 4 CMLR 9, the CJEU held that there was no object restriction where a distribution agreement for luxury cosmetics confined online sales to websites which highlighted the luxury character of the brand, and prohibited sales via third-party sites, but only on the basis that this restriction of competition could be justified as proportionate to preserve the luxury image of the goods.[347]

As for the concern that arises from vertical information sharing on blockchains specifically, the solution may lie in the formal demarcation of sub-groups of users of the blockchain (e.g. as buyers and sellers) and separation of their activities, to restrict the sharing of sensitive activity information that could otherwise give rise to competition concerns.[348]

[346] See: Ping Europe Ltd v CMA [2020] EWCA Civ 13; [2020] 4 CMLR 13, ¶¶26-29, 39.

[347] See: Case C-230/16 Coty Germany GmbH v Parfümerie Akzente GmbH [2018] 4 CMLR 9, ¶36.

[348] Alex Latham, 'Blockchain and Competition Law', p. 606.

Research and development, and standardisation agreements

Many if not most existing blockchain consortia exist to facilitate R&D agreements (to develop new technologies or improve existing ones) and/or standardisation agreements (agreements on common technical standards to ensure interoperability).[349]

Many R&D agreements do not restrict competition at all. EU law recognises that such agreements can be problematic from a competition law perspective only if the combined market shares of the parties exceeds 25% on any relevant product and/or technology market (below that threshold, R&D agreements fall under the R&D Block Exemption Regulation, provided that other conditions for the application of that Regulation are fulfilled).[350] Where that threshold is exceeded, competition concerns can arise where the parties have market power on the relevant markets and/or where competition with respect to innovation is appreciably reduced.[351] If the parties to the agreement could independently have developed competing technologies that could be used for a particular purpose then the R&D agreement may restrict competition. When considering the competition implications of blockchain R&D, however, as Renato Nazzini has observed, there is a need to move beyond a classic structuralist assessment based on market share to consider competition between different blockchain applications and technologies, disruptive innovation, and the role of network effects in delivering efficiencies.[352]

Although the existence of common standards, facilitated by standardisation agreements, will generally be pro-competitive because they facilitate the compatibility of products and services, competition law recognises that Standardisation Agreements can restrict competition if: (i) standardisation between competitors has the corollary of eliminating price competition; (ii) the adoption of a single standard limits innovation and/or erects barriers to entry to the market for competitors; and/or (iii) the agreement prevents certain players from gaining access to the results of the standard-setting process. The respective solutions to those concerns in respect of blockchains are: (i) as indicated above in relation to horizontal information exchange more broadly, the adoption of strict protocols to ensure that no sensitive pricing information, or other sensitive commercial information relating to the intended use of the relevant application/technology; (ii) permitting parties to use alternative, competing technologies and/or ensuring interoperability; and (iii) providing access on FRAND (fair, reasonable and non-discriminatory) terms.[353]

Blockchain consortia are themselves a form of standardisation agreement (blockchains, as shared ledgers, could not operate without common technical standards and protocols as between their users)[354] and it will also be important to consider the basis on which participants are involved in setting or amending governance rules. If only some participants have access, some competing parties may have access while others do not, with the risk that governance standards are set in a way that favours those who benefit from such access over those who do not. The procedure for setting the consortium's governance rules and any applicable standards by which its blockchain operates will have to be transparent and based on FRAND terms.

Collusion through or by the blockchain, and the use of smart contracts

Since co-operation and transparency/data visibility are inherent characteristics of blockchains, there are multiple forms of anti-competitive co-ordination and collusion between competitors that may be made easier by blockchain technology, some of which have already been considered. Other obvious examples of collusion that

[349] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 3.
[350] Commission Regulation (EU) No 1217/2010 (14 December 2010), Article 4(2).
[351] Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements (2011/C 11/10), para 133.
[352] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 4.
[353] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 5.
[354] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 5.

may be facilitated by blockchains are: (i) the setting up of a cartel; (ii) the more effective monitoring of deviation from a cartel agreement (price fixing, customer or market allocation, or bid rigging), due to the real-time recording of transactions; and (iii) collusion by the entity or consortium operating the blockchain in the division of markets or price fixing.

The use of new technology to automate the monitoring and enforcement of a cartel is far from unprecedented: in its decision in Online sales of posters and frames, the CMA found that Trod Limited and GB eye Limited, both online suppliers of posters, had agreed that they would not undercut one another's prices for posters and frames sold via Amazon's UK website. The cartel was implemented through price-monitoring software (algorithms), which the parties configured to give effect to it.[355]

Smart contracts are programmable codes which facilitate, verify, and self-enforce the performance of agreements, through an "if X then Y" logic. They can be used in a way that is analogous to the way in which the colluders in Online sales of posters and frames used algorithms.[356] Schrepel has analysed the ways in which smart contracts may be used to create and maintain discipline and stability within collusive agreements (which discipline and stability, by definition, cannot be provided by the law) under the headings of the "visibility effect" and the "opacity effect". The "visibility effect", which applies to colluders themselves, describes colluders' enhanced ability to monitor and/or police one another's behaviour that is provided by the chain/smart contract, by which governance of the agreement, and in particular the identification of deviant behaviour, is automated. The visibility effect strengthens the cohesion of the anti-competitive agreement. The "opacity effect", which applies to non-colluders, describes the enhanced secrecy that the chain provides with respect to the information on the chain from the perspective of outsiders, in particular relevant regulators and enforcement agencies, protecting colluders from detection.[357]

The first blockchain competition case

What is widely recognised as the first blockchain competition/antitrust case, United American Corporation v Bitmain Incorporated and others (Case No. 1.18-cv-25106), first came before the Court of the Southern District of Florida in December 2018. In March 2021, the Court granted the Defendants' motion to dismiss the Plaintiff's First Amended Complaint (with prejudice) under Federal Rule of Civil Procedure 12(b)(6), on the basis that the Plaintiff had failed to state a claim on which relief could be granted under §1 of the Sherman Act, which (comparably to Article 101 TFEU) provides that: "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal." With the claim having been dismissed at such an early stage, it is difficult to draw many general conclusions as regards how courts will deal will allegations of collusion in a blockchain context and/or undertake enforcement action against colluders in the future. However, the following brief comments can be made.

The facts and allegations in the Bitmain case centred upon a 'hard fork' in the Bitcoin Cash blockchain that took place in November 2018. Bitcoin Cash is a public/permissionless blockchain originally derived from Bitcoin Core, the first Bitcoin cryptocurrency. 'Forks' are periodic updates to blockchains. Whereas 'soft' forks enable users who elect not to go through the relevant update to continue to communicate on the same network (because the existing software is compatible with the updated version). In a hard fork, users must update in order to continue to participate: after a hard fork, the old rules will be incompatible with the new rules.[358] Different proposals for updates relating to the same chain may compete with one another, i.e. in a "hash war", where the mining servers[359] participating in a blockchain network "vote" on which set of rules

[355] CMA Decision in Case 50233, Online sales of posters and frames (12 August 2016), available here: https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf.
[356] See in particular: Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", pp. 117-166.
[357] Thibault Schrepel, "Collusion by Blockchain and Smart Contracts", pp. 143-151.
[358] United American Corporation v Bitmain (Case No. 1.18-cv-25106), §I.B.2. The judgment is available here: https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc/
[359] Mining" refers to the process by which "Consumers – that is, individuals or individuals that operate servers – compete to "mine" virtual currencies by using computer power that solves complex math puzzles. The computer servers that first solve the

or protocol they prefer, and "the rules set mined with the most computer hashing power would prevail and continue the … blockchain going forward.[360] The November 2018 update to the Bitcoin Cash chain concerned two competing proposals, the "Bitcoin ABC" protocol and the "Bitcoin SV" protocol.

The Plaintiffs, United American Corporation ("UAC"), backed Bitcoin SV in the hash war, and lost to the Defendants, who all backed Bitcoin ABC. UAC alleged that all of the Defendants (whom the Honorable Kathleen M. Williams in her judgment grouped into the Mining Defendants, the Exchange Defendants and the Developer Defendants) colluded in a two-part scheme: (i) first, to determine that Bitcoin ABC was the winning protocol in the hash war by increasing their mining capacity in the short term as a way of influencing the "vote"; and (ii) second, to secure the benefits of their win by implementing a "checkpoint" on the resulting Bitcoin Cash ABC blockchain, which allowed anyone with 51% hashing power (based on mining power) to cement centralised control of the chain by ensuring that they would prevail in any future disputes regarding the consensus rules on the chain. UAC pleaded losses in the form of losses to the value of Bitcoin SV and a decrease in the value of both currencies created by the fork. Those allegations were pleaded under §1 of the Sherman Act as both a per se violation (analogous to an "object" infringement of Article 101 TFEU) and a "rule of reason" violation (analogous to an "effects" infringement of Article 101 TFEU).[361]

The Defendants succeeded on their motion to dismiss due to a "multitude of pleading deficiencies" on the Plaintiff's part, among which three stand out for comment.[362]

First, the judge found that UAC had failed to plead conspiracy, which is the first essential element in a §1 Sherman Act claim. In particular, the judge found no express allegation in UAC's pleading that all of the Defendants had entered into an agreement (whether horizontal, vertical, or "hub-and-spoke") to undertake the impugned conduct. As the judge observed, the allegation regarding the relocation of hashing power prior to the fork would in any event have related only to the Mining Defendants, and not to the Developer or Exchange Defendants. Even then the pleaded allegations were not strong enough to suggest an agreement as opposed to independent action. As regards the "checkpoint" implemented by the Developer Defendants, UAC did not allege that those Defendants implemented it by agreement with any of the other Defendants.[363] Moreover the judge was unconvinced that the "checkpoint" was, as UAC alleged, implementing with the purpose of centralising cementing control of the ledger for anyone with adequate hashing power: "It may be equally plausible that checkpoints serve another purpose, instead of centralising a cryptocurrency market, such as providing security for the blockchain or as an efficiency measure."[364]

Second, UAC failed adequately to plead that the "Bitcoin Cash market" was a distinct relevant product market for the purpose of a rule of reason analysis (the judge accepted that the relevant geographic market was global). At its highest, UAC's case was that Bitcoin Cash was "'unique' because of its utility for peer-to-peer daily transactions" and was "the most widely adopted form of cash-like cryptocurrency".[365] However the judge noted that that plea merely "leaves us hanging": she had been told nothing that would allow her to discern the extent to which consumers preferred Bitcoin over other cryptocurrencies, or why Bitcoin Cash would be a market of its own as opposed to being in the same market as similar cryptocurrencies primarily used for transactions. Further, UAC had made no factual

puzzles are rewarded with new cryptocurrency, and the solutions to those puzzles are used to encrypt and secure the currency" United American Corporation v Bitmain, §I.B.1.

[360] United American Corporation v Bitmain, §I.B.5. "Hashing power" refers to the computing power that is used to solve the relevant puzzles, see: United American Corporation v Bitmain, §I.B.1 and §I.B.5.

[361] The judgment is available here: https://www.courtlistener.com/docket/8382061/united-american-corp-v-bitmain-inc/

[362] United American Corporation v Bitmain, §II.B.

[363] United American Corporation v Bitmain, §II.B.2, and subsections.

[364] *United American Corporation v Bitmain*, §II.B.2.d.(3)

[365] United American Corporation v Bitmain, §II.B.3.a.(2).

assertions which were capable plausibly of demonstrating whether or not there was cross-elasticity of demand (i.e. a measure of demand-side substitutability that suggests that two products are part of the same market) between the market for Bitcoin Cash and the market for Bitcoin Core or other cryptocurrencies.[366]

Third, UAC was unable adequately to plead that there had been actual or potential harm to competition as a result of the alleged conduct. UAC alleged that the "quality" of the Bitcoin Cash market had been harmed by the introduction of the checkpoint (the core allegation was that for the blockchain to remain "secure and trusted" its processes needed to remain "distributed and decentralised"), but: (i) there was no allegation that any change in price, output, or any other particular change had harmed competition; (ii) no facts were pleaded to explain how and why competing developers would be unable to propose innovations to improve upon software protocols used to mine Bitcoin Cash; and (iii) in any event the allegation of harm to the "quality" of the market through the introduction of the "checkpoint" rested on the allegation of agreement between all of the Defendants (particularly the Miners and Developers) which could not be made out.[367]

Due to the foregoing and other fatal shortcomings in its pleading, UAC could not make out its case on a rule of reason violation. The judge found that UAC had also failed to plead a per se violation: the alleged conduct could not be categorised (as was pleaded) either as something "in the nature of bid rigging" (because not all of the Defendants were competitors and there was no agreement between competitors to co-ordinate bids/prices to a third party) or as a "group boycott" (again because not all of the Defendants were competitors, so there could be no agreement among competitors to withhold services from a third party).[368]

In all, what is immediately striking about the judgment in the Bitmain case is that there is nothing exceptional about the way in which the judge disposed of it. Simply, she considered pleaded facts in the light of an existing legal framework and found that those facts did not give rise to a cause of action. Furthermore, and crucially, UAC's claim was dismissed not because the existing legal framework was inadequate to test complex facts relating to competition on blockchain networks but because there was no properly pleaded case on the fundamentals of conspiracy/agreement, the relevant market, and harm to competition. Shortcomings of that kind can apply in any competition case involving allegations of covert unlawful agreements: in that regard, there is nothing special about blockchain.

The most significant feature of the Bitmain case might be that following the judge's request that the parties give her a "tutorial" on the core concepts at stake in the complaint, the lawyers on both sides "strived to make… a neutral presentation to the court".[369] It may be that UK courts can use the existing provisions of the CPR on concurrent expert evidence (PD35 paras 11.1-11.4) to similar effect in future competition/blockchain cases.

"Cartel management for groups that don't trust each other"?

In 2015, a Financial Times journalist observed with regard to blockchains that "what the technology really facilitates is cartel management for groups that don't trust each other".[370] Although blockchain technology may facilitate cartel management, and other anti-competitive harms falling within the scope of Article 101/the Chapter I Prohibition, that is not necessarily so. Renato Nazzini has underlined the point forcibly: "Blockchains… could be an electronic means of setting up a cartel. If this were the case, it would not be the blockchain itself or its operation or application [that was unlawful], but the use that the parties make of it to give effect to their unlawful agreement."[371] As regards uses of blockchains that do not amount to cartels or infringements of Article

[366] United American Corporation v Bitmain, §II.B.3.a.(2).
[367] United American Corporation v Bitmain, §II.B.3.b.
[368] United American Corporation v Bitmain, §II.B.4.a-b.
[369] Transcript of discussion available here: https://www.jonesday.com/en/insights/2021/06/jones-day-talks-takeaways-from-a-landmark-cryptocurrency-antitrust-case
[370] Izabella Kaminska, 'Exposing the "If we call it a blockchain perhaps it won't be deemed a cartel" tactic, Financial Times (11 May 2015), available here: https://www.ft.com/content/bb7f42ec-a049-3739-b74d-131e9357694c
[371] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", p. 8.

101/the Chapter I Prohibition by object, Nazzini has further advocated in favour of a robust effects analysis : *"It will be essential to balance any potential anti-competitive effects against the benefits of the technology and the need that information is to [be] shared for such benefits to accrue. There can be no blockchain without a degree of transparency. The question is how much transparency is required for the blockchain application under review to work, and how much information can, instead, be securely blacked out. And all will be a matter of degree."* [372]

2. Potential harms within Article 102 / Chapter II

Article 102 TFEU and the Chapter I Prohibition in UK competition law (s.18 of the Competition Act 1998) prohibit abuse of a dominant position. The scope for abuse of dominance or collective dominance (i.e. by blockchain consortia)[373] in the blockchain context is at present limited. There are only two obviously dominant undertakings in this space: Bitcoin and Ethereum. Though, as these platforms rely on public/permissionless blockchains, the likelihood of unilateral abuse is insignificant for the reasons discussed above.

However, that is not to say that conduct in breach of Article 102 TFEU / Chapter II CA 1998 is unlikely to occur in future. In the same way that tech giants saw remarkable growth in their market power alongside the rise of the internet via "network effects", the same may well be true for blockchain-based services. To this effect, the OECD has commented how *"in cases where blockchain-based business models successfully disrupt non-blockchain models, the cross-platform network effects might be expected to give one blockchain a degree of market power"*; and that *"we might expect that there would be particularly strong network effects in the increasing number of 'industry' blockchains that are being formed by consortia of upstream and downstream firms that serve a certain market (see for instance those in shipping or diamonds) or that serve a broader set of markets (for example in the case of Libra)"*.[374]

Another key concept here is that of "single source" information or data – i.e. that permissioned blockchain owners are likely over time to build up unique historic datasets on the chain which only they have access to – such as transaction data or medical records history. The richer the historic datasets, the harder it will be for newer rivals to compete. This dynamic increases the likelihood that blockchain-based markets become "winner takes all" markets.

Finally, it is important to note that undertakings may establish dominance in the blockchain space by lawfully or unlawfully leveraging dominance in other markets.[375] For example, in the context of payment activities, the French competition authority has commented that "data collected by Big Tech in the context of their core business activities could give them a significant advantage in the payments industry and, conversely, the data collected via the payment services they offer could allow them to make their respective platforms more attractive".

Once undertakings begin to establish dominant positions, there is likely to be ample opportunity for permissioned blockchain owners to engage in uncompetitive conduct. As the founder of Etherum has considered: "The consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc."[376] Whilst it all possible manifestations of abuse of dominance in the blockchain context cannot be predicted, the most likely can be grouped as follows: i. abuse that is designed to increase market share of a dominant blockchain owner; ii. refusing or limiting access to a blockchain with the effect of market foreclosure; iii. predatory innovation; and (iv) exploitative abuse.

[372] Renato Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", pp.8-9, insertion added.

[373] The Chapter II Prohibition and Article 102 both refer to abuse "by one or more undertakings".

[374] Pike and Capobianco, 'Antitrust and the trust machine' (2000), p.8; available at http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

[375] See Opinion 21-A-05 of 29 April 2021 on the sector of new technologies applied to payment activities, p.5; available at https://www.autoritedelaconcurrence.fr/sites/default/files/attachments/2021-06/21-a-05_en.pdf.

[376] Buterin, On Public and Private Blockchains, Ethereum Fondation Blog (2015); available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

i. Abuse intended to increase market share

In ‘winner takes all’ markets, characterised by network effects and single source information, there may be significant commercial incentives to engage in abuse that directly increases customer numbers. There are two clear types of abuse that could be implemented with this in mind: abuses on the market on which the blockchain services are offered (so-called “own market abuses”), and abuses on related markets that entrench dominance in the blockchain market.

The classic example of an own-market abuse is predatory pricing. This is where an undertaking charges prices at levels that have no economic purpose other than to eliminate or weaken competition. In the blockchain context, the most obvious form of predatory pricing is where a blockchain owner reduces transaction fees to artificially low levels in order to foreclose the market. Whether or not prices are “predatory” is fact-specific. Though applying the predatory pricing doctrine in digital markets comes with various conceptual challenges.[377] For example, Lina Khan has argued that “[t]he fact that Amazon has been willing to forego profits for growth undercuts a central premise of contemporary predatory pricing doctrine, which assumes that predation is irrational precisely because firms prioritize profits over growth”.[378] It may therefore be challenging to distinguish the dividing line between conduct which builds up a customer base (i.e. “loss leading”) and conduct which eliminates rivals. That challenge is particularly pronounced where predation in one market can be cross subsidised by a firm’s dominance in related markets.

Another type of own-market abuse is the imposition of exclusive purchasing agreements, where dominant blockchain owners provide services on condition that customers abandon any rival products it may be using.[379] Relatedly, the blockchain owner might also give loyalty rebates: for example, blockchain owners looking to foreclose a financial transactions market might grant significant rebates to important financial services customers. The incentive to ensure exclusivity may be particularly pronounced if the customer has an ability to “port” historic data stored on the blockchain to other chains. Both exclusivity purchasing agreements and loyalty rebates may be objectively justified. Though, as with the predatory abuses considered above, particular evaluative challenges are posed in digital markets.

The second type of abuse designed to attract customers is where a dominant undertaking leverages dominance in other, related markets to foreclose the market on which the blockchain operates. Although some of the abuses considered above may also apply, the most obvious “leveraging” abuses in the blockchain context are tying and bundling. This is where the dominant undertaking requires customers using a “tying product” in a different market to acquire a “tied product” (i.e. the blockchain-based product). For example, a dominant retail business might require companies it buys products from, or sells products on behalf of, to use its own blockchain-based platform for completing the transaction and tracking delivery. Whilst a dominant digital wallet application provider might ensure its application is only compatible with one type of blockchain-based payment option. Such practices may be capable of objective justification. Though, as above, it may be challenging to distinguish between conduct that seeks to eliminate competition and conduct that generates network effects that are beneficial for consumers.

ii. Refusing or limiting access

Once a blockchain owner becomes dominant in a given market, there is clear scope for abuse in either refusing to deal or providing access to the chain on unfair or discriminatory terms.[380]

[377] See OECD, ‘Abuse of dominance in digital markets’ (2020), pp.31 et seq.; available at https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf. https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf page 32

[378] Khan, ‘Amazon’s Antitrust Paradox’, Yale Law Journal, 126 (2017), p.44; available at https://ssrn.com/abstract=2911742.

[379] Note that Exclusivity may be contractual or de facto.

[380] On this issue, see Opinion 21-A-05, pp.120 et seq.

Refusal to supply constitutes an abuse of dominance where, in essence, an undertaking refuses to supply (or supplies on unacceptable terms – i.e. constructive refusal to supply[381]) without objective justification, products or services which constitute an "essential facility" or "objectively necessary" input. This will be the case where the input cannot be duplicated or can only be duplicated with significant difficulty (i.e. it would not be economically viable) in the foreseeable future. Although this doctrine was initially developed in the context of access to physical infrastructure, it has since been applied to less tangible inputs, such as computerised airline reservations systems,[382] cross border payments systems,[383] and intellectual property rights.[384] The EU Commission's Article 102 Enforcement Priorities state that "an input is likely to be impossible to replicate … where there are strong network effects or when it concerns so-called 'single source' information".[385] As discussed, both factors are likely to arise in relation to blockchain. In this context, essential input arguments are likely to focus on the economic viability of setting up a rival blockchain and attracting a critical mass of customers. This will clearly vary from case to case. However, commentators have pointed out that *"there are several features of blockchain that clearly distinguish it from other inputs and services to which the essential facilities doctrine has previously been applied – most notably the fact that the source code underpinning the design of a blockchain is largely publicly available and is readily accessible to competing developers"*.[386] Where a refusal to supply results in foreclosing of the market, a dominant undertaking may still be able to objectively justify that conduct in the blockchain context. For example, access may be refused to users with inadequate cybersecurity practices which pose a threat to the operation of the blockchain.

Due to the incentive to generate networks effects and single-source information, blockchain owners may generally wish to grant access where possible. Refusal to deal situations may be less common than situations where blockchain owners provide blockchain-based services on terms that are discriminatory or not objectively justified. Even if this falls short of a constructive refusal to supply, it may still fall foul of Article 102 / Chapter II. Both provisions specifically prohibit dominant undertakings from "applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage". Though it is important to note that differential conduct is not per se unlawful where it can be objectively justified. For example, when it comes to price discrimination, the courts have recognised that different prices can be applied to different categories of buyer; in particular that newer entrants to the market can be incentivised through lower prices.[387] Another example of differential conduct is the operation of "dual speed blockchains" (as already de facto exist with Bitcoin) – i.e. different transaction speeds depending on how much the user is willing to pay. As a general rule, the more the market share of the blockchain owner increases, the harder it will be to justify differential treatment.

To address access issues, regulators and courts may turn to existing competition law principles from the licensing of Standard Essential Patents (SEPs). Where intellectual property constitutes an essential input, dominant firms are required to license access on terms that are fair, reasonable, and non-discriminatory (FRAND). Those terms are standardised regardless of what a customer is willing to pay and are set with reference to the true value of the SEPs licensed.[388] Courts have been willing to set FRAND prices in appropriate cases.[389] There is no reason in principle why this approach could not be applied in the blockchain context. Less clear is the extent to which these principles are

[381] For an example of constructive refusal to supply, see Case T-486/11 Orange Polska v Commission.

[382] See London European-Sabena, OJ [1988] L 317/47.

[383] Commission Notice on the Application of the Competition Rules to Cross-border Credit Transfers, OJ [1995] C 251/3.

[384] Discussed below.

[385] Communication from the Commission, 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings', fn.58; available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52009XC0224%2801%29#ntc52-C_2009045EN.01000701-E0052.

[386] Leahy and Davis, 'Innovating for the greater good: how to design a competition law compliant blockchain' (2020); available at https://technologyquotient.freshfields.com/post/102g0n8/innovating-for-the-greater-good-how-to-design-a-competition-law-compliant-blockc.

[387] See Attheraces v British Horseracing Board [2007] EWCA Civ 38.

[388] See Unwired Planet International Ltd v Huawei Technologies Co. Ltd & Anor [2020] UKSC 37, para 114.

[389] Most notably, in Unwired Planet v Huawei [2017] EWHC 711 (Pat), where Birss J said at para 169 that "courts all over the world have now set FRAND rates. I am sure the English court can do that as well." This judgment was later affirmed by the Court of Appeal and Supreme Court.

capable of applying to the licensing of other proprietary information, especially large datasets stored on a blockchain; although there is a growing consensus that such datasets can constitute an essential input in digital markets and may be required to ensure interoperability and competitive tension.[390] To take a practical example, a joint Competition Commission of India and Ernst & Young paper on blockchain and competition considers a hypothetical blockchain application which records regular data from IoT devices installed in cars. The report considers how "[t]his data could be used by insurance providers to determine the car insurance premium based on the risk profiles developed from the historical data. If a new insurance company is denied access to this hypothetical blockchain application, it is possible that it may not be able to compete effectively in the market."[391]

iii. Leveraging dominance in the blockchain-based market

The third category of abuse is what has been described as "predatory innovation". This is an emerging theory of harm which has been primarily considered by Schrepel. He defines this harm as "the alteration of one or more technical elements of a product to limit or eliminate competition".[392] As Schrepel recognises, identifying predatory innovation may be difficult in practice. However, he has commented that "predatory innovation remains one of the most anticipated and dangerous anticompetitive strategies that can be implemented on private blockchain". The basis for Schrepel's conclusion is as follows.[393]

> *"First of all, predatory innovation on blockchain is cheap as it can be implemented at no cost. Its implementation can also be very fast, in fact, interactions/validations via blockchain only take a few seconds or minutes at most. Although transactions and modification are not invisible on public blockchain, they can be on private blockchains — the access to information and the history of the blockchain can be limited to some users. And predatory innovation on blockchain can have a radical effect: it will produce immediate effects by excluding a targeted user which also is a competitor. Lastly, predatory innovation practices can take different forms with multiple effects, beyond the mere exclusion from the blockchain. A company that owns a private blockchain can indeed modify its governance design so that a user's access is purely and simply denied, or, to a lesser extent, that the user can no longer read all the information on the blockchain, register transactions or take part in the block validation process."*

iv. Exploitative conduct

The fourth and final category of harm is so-called "exploitative" abuse. This is where undertakings abuse dominant positions "to reap trading benefits which it would not have reaped if there had been normal and sufficiently effective competition".[394] Whilst this type of abuse has traditionally been directed towards the charging of excessive prices, there is an emerging theory of harm concerned with the exploitation of user data; something of particular relevance in the blockchain context given the likelihood of network effects and single-source data. For example, in 2019, the German competition authority decided that Facebook had abused a dominant position in the way it collected, merged and used user data because this exceeded what was necessary for Facebook to operate its platform and consumers had

[390] See, for example, the French and German competition authorities' joint report, 'Competition Law and Data' (2016), pp.17-18; available at https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=821DE929A6BEF735EF2B0EE63D4A9B25.1_cid362?__blob=publicationFile&v=2. See also Brinsmead, 'When does information become an essential facility?', fifteen eightyfour; available at http://www.cambridgeblog.org/2021/05/when-does-information-become-an-essential-facility/.

[391] CCI and EY, 'Discussion paper on blockchain technology and competition', p.43; available at https://www.cci.gov.in/sites/default/files/whats_newdocument/Blockchain.pdf.

[392] Schrepel, 'Predatory Innovation: The Definite Need for Legal Recognition', SMU SCI. & TECH. L. REV (2018); available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997586.

[393] Schrepel, comments to the European Commission for its conference on competition policy in the era of digitization, in particular the panel entitled "Digital Platforms' Market Power" (2018), p.8; available at https://ec.europa.eu/competition/information/digitisation_2018/contributions/thibault_schrepel.pdf.

[394] Case C-27/76, United Brands v Commission, para 249.

no ability to opt-out of the processing activities.[395] Theories of harm of this kind are still being shaped in UK and European law, where it has belatedly been recognised that the use and abuse of data is not merely a matter for privacy law and data regulators, but is a concern for competition lawyers (in that privacy standards may impact on the quality of a service offering). However, similar reasoning may in future be applied to the exploitation by blockchain owners of transaction data and other user data. If this data is processed in a way that strikes an unreasonable balance between the blockchain owner's interests and that of the blockchain participants, this may be unlawful.

3. Potential enforcement problems for competition regulators

Issues with competition enforcement in a blockchain context appear to hinge on two factors: the degree of transparency on the blockchain and the concentration of power in the hands of the blockchain owner(s). With this in mind, we consider enforcement of two types of blockchains: "decentralised" blockchains (permissioned or permissionless blockchains, that are characterised by more transparency and less concentrations of power) and "centralised" blockchains (permissioned blockchains characterised by less transparency and greater concentrations of power). Though it should be flagged that these concepts are somewhat artificial and are not separated by any clear dividing line.

Regulating "decentralised" blockchains

The first problem regulators are faced with is the detection of anti-competitive practices that may be perpetrated through encrypted means within a particular blockchain network, and the identification of the perpetrators of those competitive harms. As has been noted: "The pseudonymity of transactions on the blockchain, combined with the anonymity of the nodes on the chain create obstacles in terms of enforcement. Thus the distributed network architecture of blockchain constitutes a real barrier to competition law enforcement."[396]

In addition, where blockchain is used as part of a decentralised network, there is no single target of blocking action – there being no single server to target – like there would be in relation to an identifiable company conducting anti-competitive practices through their own identifiable servers. For the same reason, there is no single, central person against whom a regulator might seek an injunction or to apply sanctions or in respect of whom remedial orders might be made (or at least certainly not on a public or permissionless blockchain). The notion of a dawn raid against a particular participant and the seizing of their computer will be entirely ineffective for the same reason that a hacker seeking to amend the chain by hacking a particular node and amending a single particular transaction will be revealed by the history of the transactions on the chain to be an incorrect outlier. The problems surrounding the taking of enforcement action multiply when many of the network's constituent users operate in other jurisdictions.

In competition law terms, who is the undertaking or undertakings that may be targeted with enforcement action? Is it each individual participant in the network, or only those constituting the majority that adopted the practice (or amending the governance rules – most obviously on a private, permissioned blockchain) giving rise to the anti-competitive harm or effect[397]? Each individual is engaged in economic activity on the chain, albeit that the adoption of governance rules by a certain sub-section of individuals may constitute an agreement between an association of undertakings. Similar considerations apply where the blockchain is dominant on a particular market: there, is the fact that all participants on the chain are beneficiaries of the block's monopoly, such as to render them collectively dominant? Or would dominance only reside in those sub-set of users whose amendment of the governance rules or software protocols had led to the chain's position of dominance? Or only those users on the chain whose market power in the relevant markets

[395] See https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Meldungen%20News%20Karussell/2019/07_02_2019_Facebook.html. For the complex subsequent procedural history, see Heinz, 'Bundeskartellamt hits "don't like" button on Facebook', Kluwer Competition Law Blog (2019); available at http://competitionlawblog.kluwercompetitionlaw.com/2019/02/11/bundeskartellamt-hits-dont-like-button-on-facebook/.

[396] Schrepel, comments to the European Commission, p.3.

[397] At least on an open or public blockchain: private blockchains can modify their governance design anytime and do no need a majority to agree or acquiesce.

renders them dominant? Or indeed only those sub-set of users who have market power by reference to the chain's particular applications?[398]

In any event, the answer may be that in order to 'take down' the operation of a blockchain network that is found to be engaged in anti-competitive practices it will be necessary to encode disabling measures into the network's own internal system of governance. But if that encoding had not been undertaken from the outset, then again, one envisages that a competition regulator would need the power – as is being discussed in the context of the new Digital Markets Unit (DMU) – to undertake pro-competitive interventions by way of orders that would, in this case, lead to the re-coding of the blockchain itself. Again, that requires a regulator to know who to target in order to issue an enforceable order.

For open blockchains the governance rules are embedded in code. The protocol part of the software defines the consensus mechanism, being the mechanism by which governance rules might be altered. The software protocol also defines the consensus mechanism for private blockchains. However, as noted above, governance is always complemented by an ordinary agreement between participants through, in particular, cooperation agreements. The question will be whether that agreement constitutes an agreement between all participants for the purposes of the Chapter I prohibition. If that agreement is an agreement which, inter alia, provides for the pursuit of transactions on that blockchain by way of the governance rules and software protocols that may have an exclusionary effect, it is likely that all participants would be regarded as parties to an anti-competitive agreement. The CMA can use their powers to raise information requests to seek to ascertain the identity of participants, and recourse might even be had to Norwich Pharmacal Order, being a disclosure order available in England and Wales which allows information to be obtained from third parties who have become 'mixed up' in wrongdoing.

Moreover, if the blockchain is immutable, it just will be the case that visible transactions that constitute a competition law violation will remain on the permanent digital record, at least for all users of that chain to see. It may be a form of information sharing that cannot be deleted. The impact of the breach may dissipate as market conditions move on and insofar as that particular form of breach is addressed either through effective sanctions and/or remedial measures including recoding, the fact that the record of the previous competition law breach cannot be deleted or destroyed may therefore have no lasting impact.

Regulating "centralised" blockchains

As more economic activity is undertaken online, competition regulators have had to consider the extent to which the existing rulebook and enforcement toolkit continue to be sufficient to protect the process of competition, and thus the maximisation of efficiency and consumer welfare. That has led, in the United Kingdom, to the establishment of the DMU within the Competition and Markets Authority. The DMU – which currently operates on a non-statutory basis pending the anticipated passage of new legislation conferring on it new powers to promote competition on digital markets – will operate as a pro-competition regulator for digital markets and platforms, and in particular will "oversee a new regulatory regime for the most powerful digital firms, promoting greater competition and innovation in these markets and protecting consumers and businesses from unfair practices".[399] In that regard, the DMU will oversee and enforce the new pro-competition regime for digital firms with Strategic Market Status (SMS), meaning the activities of major tech companies where the risk of anti-competitive harm is greatest.

In July 2021, the Government published a consultation on proposals for the new

[398] Shrepel, Is Blockchain the Death of Antitrust Law? P 304
[399] https://www.gov.uk/government/collections/digital-markets-unit

pro-competitive regime that will apply to digital markets.[400] including in relation to the criteria to be applied to designate those with SMS. What is envisaged is a new agile approach to regulating big tech firms, where an evidence-based assessment will be used to identify those firms with substantial and entrenched market power, in at least one digital activity, providing them with a strategic position.[401] This includes situations where the effects of the firm's market power are likely to be widespread or significant. These firms will be designated with Strategic Market Status and will be subject to (i) a new enforceable Code of Practice which will be designed to shape firms' behaviour to prevent anti-competitive outcomes before they occur; and (ii) a range of potentially pro-competitive interventions by the DMU.

As matters stand, it seems likely that many online companies who adopt blockchain technology will not fall within scope of the new pro-competitive regime that will be enforced by the DMU, but will remain subject to existing competition law provisions. However, as discussed above, it seems likely that blockchain-based services will operate in markets characterised by network effects and single source information. Therefore, as these markets mature and dominant positions are established, companies may begin to fall within the DMU's remit.

Before that stage is reached, it seems likely that regulators will have to adapt in a piecemeal fashion. Whilst the existing analytical framework for evaluating competition harms seems more than adequate, the main concern is whether regulators will forever be playing 'catch-up'. In our view, getting ahead of the curve requires three main steps. First, regulators need to ensure they have the necessary technical expertise to understand exactly how relevant blockchain technologies operate. For example, in the same way 'algorithmic auditors' are starting to shed light on the implications of algorithmic coding, similar professionals will be needed in the blockchain arena. Second, regulators will need to ensure they oversee grey areas where traditionally siloed areas of law overlap. For example, when it comes to the interaction of competition and privacy / data protection law, the CMA's DaTa Unit and the Digital Regulation Cooperation Forum (which consists of the CMA, FCA and ICO) are both designed to address unique challenges posed by digital markets. Third, regulators should be willing to push the boundaries of competition law to ensure all forms of anticompetitive abuse are addressed. That may be easier said than done but is imperative to ensure blockchain technologies fulfil their promise of enhancing consumer welfare.

[400] https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets

[401] This will not require the DMU to undertake formal market definitions to precisely define the parameters of the market in which the activities of the undertaking in question take place (see para 54 of the Consultation)