Blockchain and competition law

Pat Treacy*

Alex Latham**

Blockchain; Competition law; EU law

1. Introduction

Arguably the technological buzzword of our times, according to many, blockchain is a revolutionary force that will change the face of commerce as we know it. Whilst the underlying technology itself is not novel, most of us only came into contact with the idea of blockchain when the meteoric rise of bitcoin caught international attention in late 2017, prompting many commentators to draw comparisons with Dutch Tulipmania in the seventeenth century. Originally conjuring up images of basement crypto-anarchists using the untraceable currency for nefarious purposes, over time the excitement around blockchain has led to extensive corporate interest and discussion of a myriad of potential uses. This article aims to provide a broad overview of blockchain technology and of the surrounding potential competition law issues.

Section 2 below provides a high-level breakdown of the fundamentals of blockchain technology and looks at the key internal mechanisms that drive it. Section 3 reviews the areas in a blockchain ecosystem where power might collect and assesses the potential for that power to be exercised in anti-competitive ways. Section 4 addresses how blockchain might interface with competition law as it currently stands and Section 5 examines the enforcement issues that agencies may face.

2. Introduction to blockchain

The section below provides a brief primer on the fundamentals of blockchain technology, the contrast between public and private blockchains and a short explanation of consensus algorithms and forking.

2.1 The fundamentals

Blockchain technologies securely store transactional records in multiple locations with no centralised ownership.[1] They are repositories of data that are tamper-proof because all nodes in the peer-to-peer system the blockchain creates each contain a record of all transactions across the network to that point.[2] Users transact with each other as peers rather than via a centralised hub and the record of that transaction is recorded as a new "block" in the chain. The block will be validated against the existing "ledger" already contained within each record, for example, in a payment system an individual cannot transact to spend more units than they are recorded to have been given. Each block contains a unique "hash" which acts as a digital fingerprint. Once a block is synthesised, its hash has been calculated and tampering with the data inside the block will mean that the contents and the hash no longer match. This makes tampering immediately evident. Each block also contains the hash of the previous block in the chain, identifying the transaction immediately preceding the one that has taken place. Because of this linkage, if the hash of a single block were to change, it would invalidate all the blocks subsequent to it.

Once a block is added to the chain it is then distributed amongst the peer-to-peer network so that everyone has a record of the new transaction. This creates an immutable, tamper-proof data file, as in order to corrupt one block in the chain it would be necessary to concurrently change all the blocks subsequent to it, as well as taking control of over 50% of nodes in the decentralised network in order to form a consensus and become accepted by the ecosystem in general. Blockchains therefore allow for the removal of any third party validation or tracking of transactions (such as that historically provided by banking institutions) and creates what has been called "frictionless transfer of value".[3]

2.2 Public open blockchains

Blockchains can be public (permissionless) or private (permissioned). A public blockchain can be used by anyone and its participants are anonymous save for unique user identifiers. Any user can add blocks to the chain and can transact with other users at will. By contrast, private blockchains are operated in a similar way as private servers currently: a defined set of host users have access and authority to control all aspects of the chain. Private 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.

"Open" in this sense refers to the open-source nature of the underlying code upon which the blockchain is built. Open-source blockchains allow for coders with the requisite level of skill to make changes to the chain, shifting certain parameters and presenting alternatives to the current rules which govern its operation.

* Senior Partner, Bristows LLP.
** Trainee Solicitor, Bristows LLP. With thanks to Myles Jelf for his suggestions and technical expertise.

[1] M. Mainelli and S. Mills, "The Missing Links in the Chains? Mutual Distributed Ledger (aka blockchain) Standards" (Z/Yen Group, November 2016) longfinance.net, *https://www.longfinance.net/media/documents/The_Missing_Links_In_The_Chain_Mutual_Distributed_Ledger_aka_blockchain_Standa_DMN9ulM.pdf* [Accessed 2 October 2020].

[2] M. Saad, J. Spaulding et al, "Exploring the Attack Surface of Blockchain: A Systematic Overview" (Cornell University, 6 April 2019), *https://arxiv.org/abs/1904.03487v1* [Accessed 2 October 2020].

[3] K. Malinova and A. Park, "Market Design with Blockchain Technology" (26 July 2017), *http://dx.doi.org/10.2139/ssrn.2785626* [Accessed 2 October 2020].

2.3 Consensus algorithms and forking

Blockchains use consensus algorithms so that everyone can trust the state of the ledger. In essence, these are a set of rules that apply to everyone, with certain pre-conditions governing the mechanism for how blocks are added to the chain. Arguably the most well-known consensus algorithm is Proof-of-work (PoW), the algorithm used in the cryptocurrency Bitcoin.[4] This involves special nodes in the system known as "miners" who compete against each other to solve a computationally expensive mathematical challenge.

In Bitcoin, miners listen for broadcasts of transactions that should be added to the blockchain. They then aggregate these broadcasts into a block of transactions which is combined ("hashed") with the solution to a complicated cryptographic puzzle. The global network of miners are trying to solve the next step in the puzzle so that it can be used to verify ("frank") the last set of transactions that have taken place across the Bitcoin network. If the miner solves the cryptographic puzzle first, then the miner broadcasts the new block across the network and is rewarded with newly minted Bitcoin.[5,6] In Bitcoin's case, the system is set up so that on average the global computing power presently engaged in mining will find a new solution (and so can create a new block recording the latest transactions) every 10 minutes.[7,8] As computational power increases, the network will dynamically adjust the difficulty of the challenge to ensure that the block time remains constant.

Controls like the one illustrated above have divided opinion and with open-source blockchains dissenting programmers have the power to alter the code and change the rules of the consensus algorithm, imposing new, more favourable conditions. This creates a fork in the chain (see fig.1) as the new version will no longer be compatible with the previous chain and will not receive the necessary software updates.

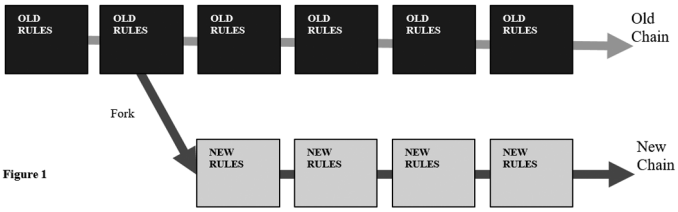

Figure 1

Some more well-known incidences of this are the offshoots of Bitcoin; Bitcoin Cash and Bitcoin Gold which split in August 2017[9] and October 2017[10] respectively. Participants could easily convert currency for both of these forks, initially one Bitcoin equalled one of the new units so there were low switching costs in both cases.

3. The new regime – power structures within blockchain

Before exploring how competition law maps onto blockchain technologies it is first sensible to investigate where power may collect within such a system and the potential creation of concentrated areas of power that could pose a threat to competition.

3.1 Founders and core developers

Blockchain founders and core developers are the original designers of the software and are responsible for implementing the rules of the blockchain as they are originally laid down.[11] Once live, public blockchains are evolving and consensus driven systems so core developers remain influential only through reputation and understanding of the technology. As a computer-based network technology driven by software, blockchain is not a static creation and will require updates in the forms of new software releases. One operational risk of blockchain is that only a few people truly understand how this software works. Whilst founders and core developers no longer have active control over the blockchain, those using the technology must place their trust in this small

[4] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), *https://bitcoin.org/bitcoin.pdf* [Accessed 2 October 2020].
[5] T. Wan Kim and A. Zetlin-Jones, "The Ethics of Contentious Hard Forks in Blockchain Networks with Fixed Features" (Frontiers in Blockchain, 28 August 2019) frontiersin.org, *https://doi.org/10.3389/fbloc.2019.00009* [Accessed 2 October 2020].
[6] The Bitcoin system was very cleverly set up so that the reward for solving the puzzle and creating a new block halves every 210,000 blocks (about four years at a block every 10 minutes)—originally it was 50 bitcoin, then 25 and 12.5, dropping to 6.25 on 11 May 2020. Ultimately this means the number of Bitcoin that will be created is effectively finite at about 21 million, with each transaction confirming block only leading to 0.2 new Bitcoins by 2040. That in itself has implications for the real-world value of Bitcoin and for the economics of Bitcoin mining needed to validate the entire system.
[7] The system was (also very cleverly) set up so that the difficulty of solving the mathematical problem at the heart of the arrangement is adjusted every 2,016 blocks, based upon the total computing power—or net hash power—available in the system. It is that ratcheting up of difficulty, together with the greater and greater computing power dedicated to the pursuit, which has made it increasingly onerous and expensive to create new blocks and so earn new bitcoin.
[8] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008).
[9] G. Jenkinson, "Forks in the Road: 2017 Bitcoin Forks" (CoinTelegraph, 3 January 2018) cointelegraph.com, *https://cointelegraph.com/news/forks-in-the-road-2017-bitcoin-forks* [Accessed 2 October 2020].
[10] A. Hertig, "Bitcoin Gold: What to know about the Blockchain's next split?" (Coindesk, 23 October 2017) coindesk.com, *https://www.coindesk.com/bitcoin-gold-know-blockchains-next-split* [Accessed 2 October 2020].
[11] T. Schrepel, "The Theory of Granularity: A Path for Antitrust in Blockchain Ecosystems" (14 January 2020), *http://dx.doi.org/10.2139/ssrn.3519032* [Accessed 2 October 2020].

group of individuals with the expertise to make desirable policy choices and implement them accurately into the underlying code.[12]

Large public blockchains are, therefore, in effect operated by an amorphous group of ever-shifting members with no one definitively in charge. Historically, updates to blockchain have been made voluntarily by a small group of skilled individuals invested in the underlying decentralised ethos of the technology. The dispersed nature of those making the updates means that when core developers feel there needs to be a change in the underlying software (i.e. modifying the block time or total number of Bitcoin) there must be a consensus in developers (and subsequently a consensus in users) to adopt the technology. The lack of centralised power means that as no one is directly responsible for the code, voluntary core developers may be vulnerable to exploitation and the lack of a guiding force behind most of the technology means that extraneous operators could pay to influence the underlying rules of the chain. Centralised private blockchains have someone in charge of management and repair, whilst this sacrifices a degree of freedom it does mean that risk management and policy decisions are attributable to someone and therefore can be monitored and improved.

3.2 Miners

Competition involving miners is present on a single blockchain (i.e. competition amongst miners) and also across several blockchains in multi-cryptocurrency systems (competition for miners).[13]

The competition amongst miners on a single blockchain is a fundamental aspect of the mining process.[14] It is the competition for the transactional incentive that drives the addition of blocks to the chain and maintains the underlying integrity of the blockchain.[15] As incentives grow, competition for the reward of appending blocks will increase. The key economic decision taken by miners is how much computational power to invest in search of the reward. From a game theory perspective, the decision to participate as an active miner is dependent on the cost margin between generation of computational power and economic reward gained from appending blocks to the chain. In this theoretical model, mining itself is monopoly-proof, as you cannot exclude a competitor by cutting down costs—profits will always be positive regardless of the margin obtained by other competitors.[16] Realistically this does not work as mining is not an independent system, the resource commitment necessary to mine a block, outside systems and transactional costs all play into mining decisions. As blockchain mining has become an increasingly lucrative venture, the energy required to solve the computational puzzles has grown in parallel and competition amongst miners is fierce, with miners now needing specialised hardware to compete effectively and large "mining pools" sharing resources to spread their processing power over networks of miners.[17]

Mining pools introduce a consolidated aspect into a blockchain's supposedly decentralised system.[18] As miners have pooled their risk and organised, the computational power and number of mining pools has grown, pools now account for almost 100% of all Bitcoin mining activity.[19] Maintained by a pool manager, who takes a cut from miners' rewards as a fee, miners participate in a fee contract which apportions how miners' computational contribution maps onto their final reward. Reassuringly, while some pools have gained significant market share, none of these large pools retained this over time, possibly signalling an economic system with factors that suppress dominance.[20] Underlying mining technology may also change the balance of power, application-specific integrated circuits (ASICs) are chips designed for mining a specific cryptocurrency and increase the efficiency of those who use them. If pools can leverage economies of scale to shape the competitive landscape through technology then this may raise significant competition concerns and could lead to a call for mandatory licensing.

In a multi-cryptocurrency ecosystem, blockchains are competing against each other for computational power. Large mining pools wield considerable power as they have the potential to make or break a new blockchain by choosing to mine for it. In future, migration of miners across platforms may be subject to significant scrutiny by competition authorities, particularly if certain blockchains are allowed to fail or are deliberately bypassed by an exploitative mining pool (see section 4.1).

3.3 Users

Users generate the transactions that are recorded in the blockchain; the power that they exercise is the decision to participate in the blockchain. Aside from simple supply and demand, such as a greater number of users driving up the value of Bitcoin in relation to fiat currency, the blockchain with the most users will add blocks to the end of the chain more quickly and therefore be more

[12] A. Walch, "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk" (2015) 18 NYU *Journal of Legislation and Public Policy* 837.
[13] E. Altman, D. Menasche et al, "Blockchain Competition Between Miners: A Game Theoretic Perspective" (Frontiers in Blockchain, 17 January 2020) frontiersinorg, *https://doi.org/10.3389/fbloc.2019.00026* [Accessed 2 October 2020].
[14] N. Dimitri, "Bitcoin mining as a contest" (2017) 2 *Ledger* 31.
[15] As someone seeking to subvert the integrity of the system would need to control 51%+ of the net hash power in order to achieve a consensus legitimising some revised version of the chain.
[16] Dimitri, "Bitcoin mining as a contest" (2017) 2 *Ledger*.
[17] Wan Kim and Zetlin-Jones, "The Ethics of Contentious Hard Forks in Blockchain Networks with Fixed Features".
[18] L. Cong, Z. He, and J. Li, "Decentralized Mining in Centralized Pools" (George Mason University School of Business Research Paper No. 18-9, 1 November 2019), *http://dx.doi.org/10.2139/ssrn.3143724* [Accessed 2 October 2020].
[19] Cong, He, and Li, "Decentralized Mining in Centralized Pools".
[20] Cong, He, and Li, "Decentralized Mining in Centralized Pools".

trustworthy. More users can also be leveraged for transaction fees, should these be present on the specific blockchain, and like digital platforms, can add value by developing new compatible programs.[21]

One user-related dynamic specific to blockchain is how they attract users compared to traditional digital structures.[22] Successful digital platforms benefit from network externalities i.e. the usefulness of the service increases as the number of users increases. As Amazon recruits more products to its website, the more useful it becomes to individual consumers. Similarly, as more consumers use Amazon, the more useful the platform becomes for businesses looking to sell products to as many consumers as possible.[23] Blockchain scales in an inverse way due to its token offering system.[24] Where a blockchain issues tokens to represent a scarce asset, initially there is a high incentive for users to join as they can amass tokens more easily and will be rewarded disproportionately highly for mining efforts. As more users join and the blockchain stabilises with a critical mass of participants, tokens are harder to obtain as there is a larger community of users. In this way blockchains incentivise different patterns of behaviour because of the reversed economic incentives. The blockchain incentive structure prevents entrenchment and promotes early adoption, opening the door to the prospect of shifting power in a competitive marketplace.

As referenced in the previous section, users as well as miners choose whether a blockchain will fork through their choice to follow the new system of rules or to stick with the existing one. The threat of possible forks in the chain, coupled with the low switching cost, means that there should be competitive pressure from users and miners on open-source blockchains to efficiently manage the interests of the various nodes active in its ecosystem.

3.4 Other forces

The increasing computational power of mining pools necessarily leads to an arms race where any addition of power which raises the global processing power imposes a negative effect on other pools as the blockchain compensates by raising the difficulty of the problem being solved.[25] This arms race of mining has a real world cost due to the vast reserves of energy now needing to be consumed—at the moment aggregate electricity devoted to Bitcoin mining alone exceeds 70 TWh per year, roughly the annual energy consumed by Chile in 2018.[26] This may give rise to issues involving the underlying energy companies, it is not beyond the realms of possibility that we could see arrangements between energy companies and mining pools, possibly with built in blockchain related remuneration structures. Energy costs may also be driving the geographic location of mining activity, with some 70% now understood to be taking place in China because of the low local cost of the dedicated ASIC processors and of electricity.[27]

Considerations arising from all the above could give rise to a whole host of subsidisation or state aid arguments which competition authorities must be alive to. Another future point to consider is the concern surrounding some cryptocurrencies, namely bitcoin, regarding the deflationary aspect of the currency due to its finite supply. As mentioned at FN6, Bitcoin is in effect a finite resource. As the reward miners gain for processing the 10 min ledger chunks of transactions diminishes, the existing system of decentralised validation will no longer function and with no centralised authority to step in, alternative solutions must be found. One mooted solution is that transaction fees can be introduced which eventually rise to a level sufficient to keep mining profitable. The structure and quantum of these transaction fees may raise future competition law concerns.

4 Direct interaction with competition law

Those involved in blockchain technology will have potential interactions with both arts 101 and 102 of the TFEU. The technology presents a number of issues including: the potential for information sharing and co-ordination; possible abuse of dominance; and the difficulty of applying current legal presumptions to blockchain.

4.1 Horizontal information exchange

As explained above, the essence of blockchain technology is that it provides a decentralised ledger, accessible to all in the network. Coupled with the anonymous nature of blockchain, this presents a tempting opportunity for firms to collude.[28] If competitors within a market use a single blockchain then it provides an opening for an art.101[29] arrangement or what some have called "cartel management for groups that don't trust each other".[30] It has been suggested that the transparency and trust derived from the operation of a cartel via a specific blockchain with identifiable users presents the opportunity for firms

[21] Schrepel, "The Theory of Granularity: A Path for Antitrust in Blockchain Ecosystems".
[22] T. Schrepel, "Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox" (2019) 3 Geo. L. Tech. Rev. 281.
[23] J. Rochet and J. Tirole, "Platform Competition In Two-Sided Markets" (2003) 1 *Journal of the European Economic Association* 990.
[24] Schrepel, "Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox" (2019) 3 Geo. L. Tech. Rev. 281.
[25] Cong, He, and Li, "Decentralized Mining in Centralized Pools"; the blockchain is structured this way to prevent well-resourced entities being able to easily control more than 51% of the net processing power and so subvert the integrity of the system.
[26] "Bitcoin Energy Consumption Index" (August 2020), digiconomist.net, *https://digiconomist.net/bitcoin-energy-consumption*, "*Breakdown by country (TWh)*, yearbook.enerdata.net, *https://yearbook.enerdata.net/electricity/world-electricity-production-statistics.html* [Accessed 2 October 2020].
[27] "Why so much Bitcoin Mining is Concentrated in China" (18 September 2017) coinbureau.com, *https://www.coinbureau.com/analysis/much-bitcoin-mining-concentrated-china/* [Accessed 2 October 2020].
[28] OECD, "Blockchain Technology and Competition Policy—Issues Paper by the Secretariat" (26 April 2018) one.oecd.org, *https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf* [Accessed 2 October 2020].
[29] [2008] OJ C115/88.
[30] I. Kaminska, "Exposing the 'If we call it blockchain perhaps it won't be deemed a cartel?' tactic" (11 May 2015) *Financial Times*.

to identify deviations by cartel participants and punish them using smart contracts, or to identify on which terms collusion is most suitable.[31]

If market-wide blockchains are set up then the potential for unmonitored tacit co-ordination may increase. As blockchain is still at its core merely a record of ownership, some have suggested that a pragmatic effects-based approach is preferable.[32] The potential for anti-competitive effects depends on the quality and type of data stored on the blockchain, as well as the market structure of the industry using the technology. Use of a blockchain itself can be competition-neutral, it is the abuse of the technology that leads to monitoring and information sharing. As such, any effects based analysis will need to weigh the potential benefits of the technology against its potential for collusion. Adding a regulatory node into the chain to observe and collect information, especially for private blockchains, may be the answer. Another solution could be ex ante regulation that institutes compulsory regulatory involvement in protocol design (the underlying rules of a blockchain) and could enable agencies to retain access to certain encrypted information broadcasted to participants.[33]

Given that blockchain technology is built on consensus and information sharing, if anti-competitive collusion is identified, it will also be very hard for undertakings to avoid "decisive influence"[34] decisions against them as all undertakings involved in the chain were party to the same data, any "public distancing"[35] will also be technically complex.[36] It is also plausible that third party operators of a blockchain used to disseminate sensitive information may be subject to "hub and spoke"[37] claims against them.

The case of *UnitedCorp v Bitmain*[38] in the US gives us a window into another possible collusive practice, one akin to more familiar litigation involving market manipulation. In December 2018 UnitedCorp, a diversified technology company, sued Bitmain, the largest Bitcoin mining pool, over an alleged anti-competitive scheme. UnitedCorp alleged that a number of investors and mining pools colluded to support a specific fork of bitcoin over an alternative and as a consequence caused the price of the forks to fall, causing damage to UnitedCorp's investments. This draws obvious parallels with litigation concerning uneconomic bids from energy traders or false quotes from LIBOR traders that caused those markets to artificially deviate from their economic fundamentals. Whilst the case did not progress, it raises interesting questions around the concept of harm[39] and the difficulty of proving a practice is anti-competitive in a complex blockchain ecosystem.[40]

4.2 Vertical information exchange

Where a blockchain consists of vertically related parties, applications such as smart contracts give rise to concerns that an upstream undertaking may maliciously use the chain to regulate its downstream buyers. Automated contracts or shared access to data may facilitate practices such as resale price maintenance or selective distribution systems, a particularly relevant issue post-*Ping & Coty*.[41] One strategy to combat this may be to separate usage of the blockchain into distinct groups, for instance, users and record keepers or buyers and sellers, in order to prevent access to the aggregate-activity information that drives the behaviour.[42] Separation methods like this compromise the core decentralised nature of blockchain and set the stage for the centralisation v decentralisation debate regulators and industry must have if blockchains are to be widely implemented.

4.3 Dominance

One major issue regarding dominance will be the approach to assessing how the operation of a blockchain could give rise to dominance. There are several metrics that could be used to assess this; number of users, recorded transactions, market power, participation of key industry players and governance structures will all inform the approach that competition enforcement agencies take.[43] If a blockchain is deemed to be a necessary service or is classified as dominant with regard to the factors above then art.102 TFEU[44] could bite.

It is important at this point to return to the distinction between private and public blockchains. Many of the problems that may arise from dominance do not apply to the latter. Exclusionary abuses like "refusal to deal" require gatekeeping built in to the underlying code of the blockchain and are therefore irreconcilable with the "public" aspect. Tying and predatory pricing models are also difficult to implement due to the decentralised consensus model, if software updates with additional obligations or higher transaction fees were implemented then they would only be adopted if users controlling 51%

[31] OECD, "Blockchain Technology and Competition Policy—Issues Paper by the Secretariat".
[32] R. Nazzini, "The Blockchain (R)evolution and the Role of Antitrust", King's College London Dickson Poon School of Law, *Legal Studies Research Paper Series: Paper No. 2019-20*.
[33] L.W. Cong and Z. He, "Blockchain Disruption and Smart Contracts" (2019) 32(5) *The Review of Financial Studies* 1754.
[34] *Akzo Nobel NV v European Commission* (C-97/08 P) EU:C:2009:536; [2009] 5 C.M.L.R. 23.
[35] *Toshiba Corporation v European Commission* (C-373/14 P) EU:C:2016:26; [2016] 4 C.M.L.R. 15.
[36] F. Schoning and M. Tagara, "Blockchain: Mind the Gap! Lessons learnt from the net neutrality debate and competition law related aspects" (2018) 3 *Concurrences*.
[37] *Argos Ltd v Office of Fair Trading* [2006] EWCA Civ 1318.
[38] *UnitedCorp v Bitmain Inc. et al.*, Case number 1:18-cv-25106, in the US District Court for the Southern District of Florida.
[39] Did the devaluation hurt UnitedCorp as an investor because it decreased the sales of its offerings or did it lower its profits as miner because the forking controversy limited the number of transactions or lowered the fees payable to miners?
[40] K. Stylianou, "What can the first blockchain antitrust case teach us about the crypto-economy" (26 April 2019) Jolt Digest, *Harvard Journal of Law & Technology*.
[41] *Ping Europe Ltd v Competition and Markets Authority* [2020] EWCA Civ 13; [2020] 4 C.M.L.R. 13; *Coty Germany GmbH v Parfümerie Akzente GmbH* (C-230/16) EU:C:2017:941; [2018] 4 C.M.L.R. 9.
[42] Cong and He, "Blockchain Disruption and Smart Contracts" (2019) 32(5) *The Review of Financial Studies* 1754.
[43] Schrepel, "The Theory of Granularity: A Path for Antitrust in Blockchain Ecosystems".
[44] [2008] OJ C115/89.

of the global processing power were convinced to implement them. In a predatory pricing model this would require a blockchain to first lower its fees to attract users and then somehow convince the 51% to agree voluntarily to adopt a price increase. Similarly, due to low switching costs across blockchains, exploitative abuses are unlikely, as any exploitative behaviour would lead to migration of users across to a different blockchain. Discriminatory abuses covered under art.102(c) could occur, however, as everyone has access to the record of transactions, any such abuses would be visible to all and instantly detectable.[45]

The potential for abuse grows considerably if a private blockchain becomes truly essential. If a blockchain requiring permission to enter became "indispensable for competing in a market"[46] then this brings refusal to access issues to the fore.[47] Many of the abuses listed above could arise in the context of private blockchains in the same way that they may apply to dominant technology companies at the moment. Access to data is a topic being explored by many agencies at the moment and the suspicion surrounding Big Tech is an indication of how authorities might view private permissioned blockchains that monitor and store data whilst still retaining centralised control. In the case of dominant blockchains, one remedy open to competition authorities might be to introduce mandatory forks. This would involve the authority creating an alternative competing blockchain that forked off the existing dominant chain, analogous to a forced break up of companies. This approach would not be without its challenges as the fork would require different parties to co-ordinate in their uptake of the new technology in order for it to become competitive.

5. Problems with enforcement

Public open blockchains present a problem for law enforcement due to the evidentiary quality of the records held within them. In conventional record keeping, records have a physical signature and date and are placed in proximity to other records like them, this means that the perpetrator of an act is identified as soon as the practice is recognised. With blockchain determining the genuineness of the author, and therefore the legal entity to pursue, enforcement is challenging as there is no explicit and stable link between a transacting user and a real world legal entity.[48] There have been efforts to implement tracking services on large blockchains,[49] however, as is the case with the many digital technologies, clandestine techniques can often develop in concert or faster than the efforts to detect them.[50] Furthermore, blockchain platforms cannot simply be closed or shut down as the decentralised nature of blockchain means that there is no central entity to target and therefore enforceable remedies are challenging.

Current techniques are not completely defunct; if users who transact know each other's identity in real life then they can whistleblow to agencies if they are being subjected to an anti-competitive practice and then directly identify the entity behind the transactions. Another solution may be to directly implement legal requirements into the code of the blockchain itself.[51] Whilst lawmakers will wish to be careful to avoid stifling the nascent technology, built-in regulation would provide a channel into the blockchain through which the law can act. Any such system would need to be fair, and may involve legal or tax advantages to induce core developers to include regulatory mechanisms, but such a proposal does provide one example of how authorities can penetrate the barriers that blockchain currently presents.

6. Conclusion

Blockchain is a revolutionary technology with the potential to radically transform how users of digital commerce transact with each other. Prompted by its potential to circumvent traditional enforcement methods, some may see this as a chance to implement the sort of ex-ante regulation that some think should have been applied to the current digital giants before they grew into the colossi of today. Conversely, it is also vitally important to safeguard innovation and prevent the law from stifling this transformative technology.

This article has highlighted some of the aspects of the blockchain ecosystem which are of interest from a competition law perspective. The decentralised nature of public blockchains leaves core developers vulnerable to exploitation and the lack of a guiding force behind most of the technology means that extraneous operators could pay to influence the underlying rules of the chain. Mining pools represent the greatest threat as potential silos of power. However, as yet, the top pools seem unable to maintain their market share over time. This may change if certain mining technology becomes essential and is owned by a single pool or, perhaps less likely, if pools strike anti-competitive deals with energy providers.

Regarding information exchange, collusion remains a significant issue for all types of blockchain given the shared nature of the data within the system. The ability to have certainty of transaction across a clandestine private network potentially presents a golden opportunity for cartel collaboration and therefore opens the door to misuse. Whilst public blockchains are less likely to give rise to an abuse of dominance, private blockchains present many of the same issues that agencies are faced with

[45] Schrepel, "Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox" (2019) 3 Geo. L. Tech. Rev. 281.
[46] *Oscar Bronner GmbH & Co KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG* (C-7/97) EU:C:1998:569; [1999] 4 C.M.L.R. 112.
[47] Schoning and Tagara, "Blockchain: Mind the Gap! Lessons learnt from the net neutrality debate and competition law related aspects" (2018) 3 *Concurrences*.
[48] V.L. Lemieux, "Blockchain and Public Record Keeping: Of Temples, Prisons, and the (Re)Configuration of Power" (2019) 2 *Frontiers in Blockchain* 9.
[49] M. Hrones, "Yes, Your Bitcoin Transactions Can Be Tracked—And Here Are The Companies That Are Doing It" (28 June 2018) bitcoinist.com, *https://bitcoinist.com/yes-your-bitcoin-transactions-can-be-tracked-and-here-are-the-companies-that-are-doing-it/* [Accessed 2 October 2020].
[50] P. McGee, "How VW's cheating on emissions was exposed" (11 January 2017) *Financial Times*.
[51] Schrepel, "Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox" (2019) 3 Geo. L. Tech. Rev. 281.

today in other contexts. The counter-point is that the centralised power present in these private blockchains would make it easier to include mandatory regulatory nodes, software updates and monitoring if regulation were thought appropriate, and also much easier to enforce a competition law regime if necessary. Whose remit this would fall under remains to be seen, it is possible that units like the UK's new digital markets task force[52] will take up the challenge. However, with the level of specialist knowledge required, agencies may need dedicated blockchain units to truly tackle these issues.

Despite the anonymous decentralised nature of permissionless blockchains, underlying market conduct is still driven by human operation. This means that those involved are susceptible to conventional measures such as whistleblowing if any of the other operators in the system know their real-world identity. As noted above, some public blockchains may require inducement to accommodate regulatory oversight mechanisms directly into their software if that is considered to be necessary or desirable. Given the technology's government-sceptic roots, achieving this may prove challenging. One thing is certain, tools need to be developed and tested whilst the technology is still in its nascent stages as if regulators and agencies fall too far behind, it may be too late to catch up without very significant effort.

[52] "Digital markets taskforce: terms of reference" (11 March 2020) gov.uk, *https://www.gov.uk/government/publications/digital-markets-taskforce-terms-of-reference/digital-markets-taskforce-terms-of-reference--3* [Accessed 2 October 2020].