Organisation for Economic Co-operation and Development

DAF/COMP/M(2018)1/ANN5/FINAL

Unclassified **English - Or. English**

12 November 2019

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Summary of Discussion - Blockchain and Competition Policy

Annex to the Summary Record of the 129th Meeting of the Competition Committee held on 6-8 June 2018

8 June 2018

This document prepared by the OECD Secretariat is a detailed summary of the discussion held during the 129th meeting of the Competition Committee on 8 June 2018.

More documents related to this discussion can be found at
http://www.oecd.org/daf/competition/blockchain-and-competition-policy.htm

Please contact Mr Chris PIKE if you have questions about this document.
[Email: chris.pike@oecd.org]

JT03454459

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Summary of Discussion on Blockchain and Competition Policy

By the Secretariat

The **Chair** of the Competition Committee introduced the topic of the roundtable discussion: blockchain technology. This general-purpose technology can be adopted in many circumstances but its capability to provide trust without the need for a trusted intermediary in transactions has the potential to disrupt a number of markets, creating both risks and opportunities for competition. The Chair noted the discussion would focus on blockchain technology's relevance to competition law enforcement, assessing both its risks and opportunities.

Before beginning the roundtable discussion, the Chair welcomed the expert panellists: Isabelle Corbett, the Regulatory Affairs Director at R3; Catherine Mulligan, co-director of the Imperial College Centre for Cryptocurrency Research and member of the World Economic Forum's expert panel on Blockchain Technologies; Mark Simpson, a partner at Norton Rose Fulbright; Thibault Schrepel, from Sorbonne University; Peter Ostbye, a special adviser to the Central Bank of Norway; and Ajinkya Tulpule, Senior Legal Counsel at Ferrero.

The Chair explained that the roundtable would be organised around two core topics: (1) the technological aspects of blockchain, such as the implications and opportunities for firms along with factors that may delay blockchain technology's adoption; (2) examining blockchain technology from the viewpoint of competition agencies as well as considering the risks, concerns and opportunities that may arise from its use.

Before giving the floor to the panellists, the Chair therefore raised three issues surrounding blockchain technology to prompt the discussion: (i) whether there are risks that it may be used by firms to collude; (ii) whether there are risks that its use may lead to the exclusion of rivals or to a softening of competition; and (iii) whether there are opportunities for competition authorities to use the technology to improve their effectiveness or the efficiency of imposed remedies.

The Chair then invited **Greg Medcraft**, Director of Financial and Enterprise Affairs (DAF) of the OECD, to take the floor.

Mr Medcraft explained that blockchain's potential is much wider than financial services. Mr Medcraft described the OECD's current and upcoming focuses in terms of blockchain technology. These ranged from tracking inputs in footwear and garment supply chains to tackling illicit trade in environmentally sensitive goods. He concluded that because blockchain technology is widespread and of growing interest, the OECD hopes to establish a Blockchain Centre to advise governments on policy making and encourage capacity building.

The Chair thanked Mr Medcraft then invited Isabelle Corbett to present an introduction of blockchain technology and the ways in which it could impact competition.

Ms Corbett defined blockchain and distributed ledger technology as two technologies that create records of agreement, with a secure audit trail, maintained and validated by several separate computers. She described how once consensus is reached and the agreement is recorded, the agreement is committed to the ledger and immediately viewable by the parties who have the right to view it. Ms Corbett emphasised that blockchain's significance is that it allows competing firms to collaborate and maintain one secure database, run software that communicates with their counterparts and enables a near instant update in their system without relying on intermediaries for conciliation, matching or manual fixes.

Ms Corbett then described R3 as an enterprise software consortium working with a large ecosystem of financial institutions, regulators, trade associations, professional services firms and technology companies. She explained that R3 offers two platforms: Corda, an open source platform, and Corda enterprise, a commercial license for major financial institutions. Although Corda has many similar features to distributed ledgers or blockchains, Ms Corbett pointed out that Corda does not have a full copy of the ledger replicated on each node. In a more traditional blockchain, there is a full copy of each transaction that has ever occurred on every node of the network. Corda has limited data sharing because it was designed for businesses and highly regulated institutions, but it is interoperable. Next, Ms Corbett briefly described some obstacles and roadblocks to blockchain technology's path to adoption such as privacy, how to protect the data, interoperability, governance and scalability. Finally, she concluded by noting the Corda Partner Network encompasses large institutions such as Microsoft, Amazon Web Services (AWS), Oracle and Intel.

The Chair noted that agreements, transparency, network effects and decentralisation are all issues dealt with in other circumstances. He then asked Ms Corbett to describe the elements of differentiation.

In terms of ledgers in the business and financial space, Ms Corbett explained four elements that emerge: the differences arising from how data is replicated; public versus private; the types of security being implemented because of their different security layers; and how agreement is reached. The Chair then asked Ms Corbett to expand on the topic of mining. Ms Corbett responded that mining is essentially a vast amount of computing power required for the calculation to ensure that transactions are what they are supposed to be.

The Chair gave the floor to **Australia** who asked about the importance of interoperability between various systems. Ms Corbett said that interoperability between systems was a large conversation about two and a half years ago. But that more recently it was less of a focus for some since the view was that firms did not want to waste time becoming interoperable with a dozen ledgers when only 3 will survive. She said that was not the view of Corda and that ultimately Corda, Ethereum, Fabric and Hyperledger eventually would have to become interoperable because it is in everyone's interests.

The Chair then turned to **Austria** who, after highlighting that one core feature of blockchain technology is transparency and data protection regulation, asked Ms Corbett how these two issues could be reconciled. On Corda, she explained that those who have the need to see data can see it, but there is not data transparency amongst all the nodes.

Next, the Chair asked Ms Corbett to clarify that if a regulator is part of a system, can he or she actually see the transactions that would be relevant for his or her regulation? Ms Corbett explained that a regulator can see needed information and has the right to see it on the ledger. If a regulator is on the ledger, and ultimately all of them are, they are receiving information not only on a rolling basis like in a regulatory reporting scheme, but also in an enforcement action like in an auditing enquiry. Therefore, the regulator can look back to the extent permitted per regulation and have a clear view of exactly what happened.

The Chair then gave the floor to **France** who asked about the possibility of limiting data to all the network members but at the same time respecting the principles of blockchain.

Would this imply horizontal validation and access of all members of the transaction network? France also asked if blockchain is a hybrid system where members maintain server capabilities for data that is not transmitted to the network. Finally, the French delegate inquired where and how critical data are validated that are not transmitted to network.

Ms Corbett explained that limited data sharing means that the data is shared between the parties to the transaction, notary and regulator nodes. There are different ways to design the network such as placing a node on the network that receives a copy of every single transaction. In the governance model, it could be a requirement that if a node were to go down, all of the parties who have information facing that node are required to put it back onto the node. Also, she said that the notary node could be a notary cluster, meaning it is not sent to one notary to validate it. Rather, there could be ten and the network could require that all ten be in agreement on the transaction before it can actually be committed, which increases replication. Overall, Ms Corbett explained that the users determine how to implement the network and also determine where on the scale they want to be. Do they want replication of each transaction 12 or 50 times? She concluded, "what is enough?" is usually the core question.

The Chair then turned to Japan who asked about the distribution of the data versus having the whole system as one related piece. The Japanese delegate asked how it works if there is a master copy where everything was put together or if it were split like in jigsaw puzzles. Ms Corbett replied that R3 is not the central piece of the ledger, meaning it does not hold a full copy of the ledger. Although the network operator is central, that also does not hold a full copy either. If a full copy of the ledger were strung together, the system would be like jigsaw pieces. Therefore, the data is only replicated to the extent that it needs to be and there is not a central authority holding the golden copy, unless the network is so designed.

The Chair thanked Ms Corbett then gave the floor to Greg Medcraft to explain an example from Australia where the regulator was on a blockchain and used that as a way to receive information in order to regulate. Mr Medcraft noted a particular case with the Australian Stock Exchange in which there was a regulator node that was operational and also scaled because it had several million accounts offering all the needed data. The regulator was able to monitor the market online in real time, which allowed for instant access to all transactions.

The Chair offered the floor to Catherine Mulligan for her complementary presentation covering the technology of blockchains, the nature of the firm and what factors may delay blockchain's adoption.

Ms Mulligan first discussed the ways in which blockchain technology might impact the boundaries of the firm. She explained that although fundamental economic theories regarding boundaries would probably not be changed, where the most efficient and effective boundary is in terms of the economy would be changing. She highlighted that even as cryptocurrency is a large aspect of blockchain technology, there are also assets such as contracts, data and the idea of the peer-to-peer economy. She then compared today's transactions, which have high error rates, with the concept of a shared ledger. She emphasised that the theory of the shared ledger introduces a dramatic reduction in paper-based systems and costs, a reduction of potential for fraud, but also an increased potential for collusion in some industries.

Next, Ms Mulligan defined the three main types of distributed ledger technology as permissionless, permissioned public and permissioned private. She highlighted that public permissioned systems are most interesting from the regulatory perspective because they have undergone detailed within-government use cases. In these systems, people can read and write from the network, but they also ensure that even if someone is not part of the network, they can have oversight of all the transactions. Ms Mulligan underlined this is where the regulator would come in and be able to see all of the transactions and make sure that there is no collusion or watch market prices to see if there is unusual activity.

When working in a consortium approach, Ms Mulligan said that rewards or incentives are interesting from a regulatory viewpoint. She explained that Corda is an excellent example of consortium approaches, even if there are many different types of consortia. She described one in the diamond industry that increases the exchange of information between companies and also creates the possibility for a micro supply chain. In this, individuals are dynamically delivering goods and services on demand without using the boundary of a firm. Instead, they are co-ordinating with other people, using distributed ledgers, and other types of digital technology to essentially create a company for ten minutes, or however long it takes, to deliver a particular good or service, and then they are disbanding it. Ms Mulligan emphasised this will have dramatic implications for the boundary of the firm because it has dramatic implications for labour and social protection laws.

Ms Mulligan then explained why blockchain is demanding a rethink of most business processes and of regulation. She cited an example of a micro supply chain in which edible flowers were being sold to Michelin star restaurants. In this case, a micro supply chain was created. Overall, Ms Mulligan said that the main question is, “When is it collusion?” For example, if many micro supply chains suddenly begin working together, is that considered collusion? Or is the fact that there is no boundary of the firm around them mean that it is not collusion?

The Chair thanked Ms Mulligan then gave the floor to Ms Corbett who commented that the presentation illustrated how broadly blockchain technology could be used and that the references to the different types of systems were a useful way to distinguish various solutions. She noted that there is not one ledger for everything but that each of these models has a place where it makes sense to deploy it.

The Chairman then turned to **Argentina** who asked about whether parties to this kind of transaction have a way to communicate and agree between themselves about commercial conditions, prices and transactions that nobody can see. Ms Mulligan replied that there are ways for them to communicate and exchange without recording on the ledger, as blockchain cannot stop people from having phone calls and conversations.

Next, the Chair gave the floor to **Canada** who asked Ms Mulligan to expand on the concept of a firm and what happens when the agreement is struck. Do the parties in the agreement have a state like a firm that is then disbanded after? Ms Mulligan explained that the definition for the economic boundary of the firm is Ronald Coase’s definition, which focuses upon where transactions are more effectively and efficiently delivered, and where they are not. She discussed that in her own work by looking at where the contract was actually created, they realized that some contracts put out towards the market would be more efficient if decentralised. In regard to the micro supply chain, she emphasised that these are individuals who are providing services similar to a traditional firm. However, when they come together to deliver a product or service to that supply chain, they are not falling under the boundary of a traditional firm. Traditionally, those transactions would have been managed within one firm, but now they are being managed across multiple firms.

Before giving the floor to **France**, the Chair noted that overall transaction costs are reduced and thus many transactions that would not have taken place or that would have been internalised in the firm could now be externalised.

France highlighted that the Court of Justice of the European Union (CJEU) has made distinctions between the collaborative economy and the classic business economy. Given the notions of microenterprise, micro supply chains etc., France asked if the blockchain in its purest sense could ultimately be reserved for the collaborative economy. Is there not a fundamental contradiction between the notion of blockchain and commercial services provided by a conventional contract? Ms Mulligan replied that there is a difference between the collaborative economy and the commercial economy. Also, in the platform economy, they are aggregating other people's assets, time and value, and making money off of that. With the digital economy, the slow erosion of the industrial economic system is being seen and blockchain does things like reduce the need for intermediaries.

Ms Mulligan then asked France to clarify if the second question was, "Does blockchain change the nature of the contract or the nature of the business process?" France clarified that the question was, "Can there be a blockchain that stores and makes available to everyone typical commercial transactions?" Ms Mulligan replied that there are ways to negotiate the contract and companies are working on that, specifically using things like AI. Theoretically it is possible, but not yet happening.

The Chair gave the floor to Ms Corbett who added that contracts can be negotiated on blockchain and that R3 is actually working on that with the International Swaps and Derivatives Association (ISDA).

The Chair thanked Ms Mulligan then asked a follow-up question on micro supply chains and the transitory nature of the firm. To better understand the traceability of the transitory firm in the real world, he inquired if it was possible for a regulator to gather information or initiate enforcement proceedings against one of these economic actors. Ms Mulligan replied that in theory, this would be possible but it would have to be on a public permissionless ledger so they would be able to see it.

Next, the Chair noted that it was time for the second part of the discussion focusing upon competition enforcement. He then gave the floor to Mark Simpson to discuss the risk of possible collusion or co-ordination through blockchain systems.

Mr Simpson began by sharing that his focus would be collusion out of collaboration, exploring what blockchain means for competition policy and competition law. Therefore, two elements of blockchain consortia were of concern: (1) looking at how collusion might or has been viewed as a concern in respect to the establishment of blockchain platforms and (2) thinking about some of the risks around the operation of the solution itself. Overall, he highlighted the core question as, "Are there new opportunities for collusion?"

Mr Simpson then explained that many of the known private blockchains that have been developed, or are in development, are consortia blockchains. Many of these applications involve competitors within industries such as automotive, trade finance or logistics getting together and then co-operating to develop the blockchain to solve a particular problem or improve a particular process. In recent years, these industries have been subject to high profile antitrust investigations where collusion has been found to exist. Mr Simpson also highlighted that the broader consortia, like R3's 200 members, involves even more competitors. He explained that competition policy and the law in many jurisdictions recognises that some degree of information sharing between competitors, or potentially involving competitors, is fundamental to ensure that markets can function effectively. Mr

Simpson cited the European Commission's horizontal co-operation guidelines as an example of this. Overall, there are incentives and risks in every situation in which the blockchain consortia and competitors are getting together.

Next, Mr Simpson said the pro-competitive objectives of the consortia and the potential blockchain application are increased consumer confidence, greater efficiency, lowering cost base, the ability to offer a wider range of services and providing for greater trust. He noted that the concern for regulators is the potential co-ordination of behaviour, therefore limiting competition between those involved. This could either result in a pure collusive action or reduce the overall system effects of the blockchain.

Mr Simpson then discussed some risks within competition law that are broadly collusion. First, he said there are the spillover risks or effects which mean that there might be a perfectly valid, pro-competitive reason for competitors to get together, and perhaps share information or co-ordinate behaviour in some way. However, perhaps that collaboration goes too far from one end of the spectrum and more information is shared than is necessary, which is not collusion in its purest sense. At the other end of the spectrum there is also a risk of naked collusion.

Mr Simpson suggested that there is nothing new about blockchain consortia and protecting against these risks. There are standard procedures that well-advised businesses go through when getting involved in joint ventures and collaboration, and blockchain consortia are no exception. The lawyers are there on day one. There are non-disclosure agreements, obviously. There has to be discussion about the scope of what the purpose of the blockchain might be. The consortia might first think about whether it is actually something that should be in the first instance preceded or taken forward with the view that there might be an outcome. In some cases, it might just be some initial conversations. The competition lawyers come in and advise that if any information is going into the consortia, to allow the development of the potential blockchain, that there should be information sharing protocols and clean teams; there should be vetting of the activities, ranging from the scope of the project through to the meetings themselves and the development of the rules, who can participate, how the rules should be finalised, and how they are ultimately operating. So, the spill-over risk is not anything new.

He also highlighted the risk of collective boycotts, which are also usually treated by authorities as agreements and hence as hard-core infringements. However, there is of course no obligation on the founders of a blockchain consortia to necessarily admit all comers. But, care does need to be given to whether when someone asks to be involved and they have been working on a competing technology, whether or not they can be excluded from the discussion of the consortia, and whether that might affect their ability to compete in a market. So, collective boycott is a concern, but that is very much an issue that has always been considered in standard setting environments. So again, this is not a new theory of harm here or a new risk, just a standard concern related to collective or collaborative actions that can result in the emergence of a new technology or new standard which might end up being the default standard or technology in a market.

Next, Mr Simpson underlined that the operation of the blockchain platform itself is a risk. Commonly, blockchain platforms involve a heightened risk of anticompetitive information exchange between participants. He highlighted that Ms Corbett and Ms Mulligan already commented on the ability to create technical solutions that permit sensitive data to be stored securely off the blockchain or off the ledger, rather than being publicly accessible to all, which lowers the risk. Mr Simpson noted that the key question is what information is visible on a ledger.

Mr Simpson also highlighted the potential of having too much competitively sensitive information on the blockchain, for example on future strategic decisions. However he suggested this seemed unlikely since firms would be aware of the risks of doing so. He explained there is perhaps a more credible risk that information is included in a private blockchain that provides too much market transparency, so that in the right market conditions, perhaps oligopolistic markets, tacit collusion could be facilitated. He also noted cryptocurrency manipulation as a risk for collusion.

In conclusion, Mr Simpson underlined that regulators should think carefully about what these technologies are and understand them. As for new rules or regulations, he did not recommend a need for a new block exemption regulation or amendments to existing block exemptions around topics like research and development, particularly within the European context. In his view the existing rules can be applied and it is just a question of understanding the context and the technology. However he suggested that regulators need to be open to having informal conversations with business and consortia founding members right at the start.

The Chair gave the floor to Mr Schrepel for his presentation.

Mr Schrepel asked delegates to imagine a large tech platform that is nervous about the threat posed by public blockchains to its business and which therefore develops its own private blockchain in anticipation of that threat. He asked delegates to imagine that the blockchain it develops is used by its rivals and hence he asked them to consider the possibility that it would seek to use the blockchain to engage in exclusionary conduct against those rivals. He explained that he would therefore focus upon three questions: (1) How to define dominance? (2) What abusive practices to expect? (3) What sanctions to impose or what remedies?

First, Mr Schrepel explained that dominance on a blockchain is a complex issue because as the blockchain is decentralised, it is not a legal entity. He asked whether the creators of a blockchain are liable for its behaviour, or whether its users might be, and said that to calculate dominance you should look at market shares based on the type of applications running on the blockchain. For example taking all the blockchains with applications which allow you to take a taxi. But he noted that there remains the issue of what shares to calculate - the number of users? The number of recorded transactions? The number of blocks? Also, geographical aspects? He suggested that blockchains with applications which allow you to take a taxi in Paris are not really a competitor to a blockchain doing the same kind of service in Hong Kong.

Next, Mr Schrepel discussed governance, which on public blockchains operates through a consensus protocol. There is therefore a question of whether there is a pilot on the plane. One answer is that the users are running the blockchain. However, he said that new governance models are being tested in public blockchains that allow small numbers of users to change the way the blockchain operates, in the same way that in private blockchains the blockchain is designed in the way that its owners want it to operate. In that case unilateral strategies are more likely. He also suggested that the consortium blockchain is not truly private because a number of users set up the rules for the blockchain.

Mr Schrepel then discussed the distinction between public and private blockchains. He suggested that the likelihood of anticompetitive unilateral practices on public blockchain is very low firstly because actions on public blockchains are visible, and secondly because it is very difficult to change to change the protocol. However, private blockchains have a higher risk because there are no visible effects and they are easier to control. He noted other concerns such as tying, refusal to deal, loyalty rebates and discounts, predatory pricing and margin squeeze as issues surrounding private blockchains. He then described predatory innovation as modifying the blockchain to eliminate their competitors. He then asked whether agencies are able to intervene when anticomepttive behaviour occurs. First he noted that pseudonymity makes it difficult to identify a user who does something anticompetitive on the blockchain. Second he noted that decentralisation means that competitively sensitive information shared over the blockchain cannot be deleted by every node of the network. Mr Schrepel then explained that smart contracts are transactions that are automatically implemented and can be designed so that they cannot be stopped. Hence even identifying the responsible party may not be sufficient to stop the harm taking place.

He therefore suggested that there be regulatory infiltration of the blockchain However, he outlined six founding principles that, in his opinion, should not be challenged by regulation: the distributed ledger system, peer-to-peer transmission, computational logic, blockchain consensus, data immutability and pseudonymity. Subject to these being respected however he said he could imagine two possibilities. The first is to publish the rules of good conduct, which is “well, if you design smart contracts, you need to design them in a way that competition agencies or regulators can enter the smart contract if necessary.” An alternative is to provide safe harbours which legal certainty for developers.

In conclusion, he reiterated that defining dominance remains complicated and that the focus should be on the application and not the blockchain. He said that governance is still a new topic, but his concern is much more on private blockchains.

The Chair thanked Mr Schrepel then gave the floor to Ms Corbett who offered some responses to the presentation. She said that most people agree that regulation of the technology itself is not the goal, but that regulation of the use of it is. She noted that blockchain technology makes it easier for competition authorities to see the history of transactions and pricing. However, she argued that a private blockchain does not facilitate collusion, nor is it inherently more prone to anticompetitive behaviour because it is actually just data and asset flow.

Ms Corbett said that in her view anticompetitive pricing cannot exist because the price is zero. She explained that Corda is a network available to anyone, and even though the network operator maintains it, there is a governance model in place. In regard to smart contracts, she said that in a permission system where the party is known to the contract, not only could it be stopped, but a governance model could also be added so if a smart contract is executing incorrectly it could be stopped. What matters is that the parties must agree to make that change.

The Chair gave the floor to Mr Simpson who noted that the rules around governance where there are multi-parties involved in setting up blockchain do take into account that individual players may look to leverage their involvement through the rules. He noted that there are very stringent rules around tying or any of the other abuses. On fortress concept, he questioned whether antitrust authorities do not already have the necessary tools to actually go in, whether using dawn raid powers or information requests, and obtain information on what has happened on the ledger. Overall, he opined that perhaps if the authorities do not have the necessary capability, such as their own computing power and expertise, the blockchain could allow for issues behind a curtain, which could lead to them never being discovered.

The Chair then turned to **Peter Ostbye** for his presentation, which focused upon cryptocurrencies. First, Mr Ostbye defined cryptography-based asset disposal as when users use cryptographic keys to dispose of their assets. Essentially, this makes them anonymous because the keys are addresses that are not linked to any private identities. He noted that this also facilitates some conditional asset disposals, which then facilitates the smart contracts. He identified the decentralised operation and governance as the most innovative part of a blockchain, as the users themselves validate transactions and maintain the distributed ledger.

Although not a new technology, Mr Ostbye explained cryptocurrencies can improve competition by creating something that can compete with traditional finance, even if regulation is needed. He noted that crime prevention and consumer protection are also needed, and that there is concern that cryptocurrencies could blossom into a new financial crisis. However, he opined that regulation should not necessarily restrict the door to competition. Next, he said that the relevant markets associated with cryptocurrencies such as a medium of exchange might provide a store of value or in the future be a unit of account. Mr Ostbye noted that cryptocurrencies are also separate payments and can be platforms for the intermediation of suitable services such as smart contracts, AI services, data storage and other services that are suitable for blockchain or a decentralised operation.

Mr Ostbye then discussed market power in cryptocurrency markets, highlighting that they can have various anticompetitive alliances and market power in the broader relevant markets where a cryptocurrency participates. Certain cryptocurrencies and blockchains may even gain a strong position in a relevant market because the stakeholders can engage in exclusionary or exploitative practices. Mr Ostbye highlighted that looking at stakeholders such as code developers, input providers and normal users can be important because they can restrict competition and exploit market power.

Next, he shifted to possible anticompetitive actions involving cryptocurrencies such as collusive agreements, explaining that collusion is possible between certain stakeholders for exclusion or exploitation. In these cases, collusion can occur between various stakeholders in different cryptocurrencies. Two cryptocurrencies can also co-ordinate with each other, maybe to not compete in each other’s markets or to not provide similar services. He noted that there can also be exclusive agreements between stakeholders in a cryptocurrency and third-party providers as well as some exclusive agreements between internet or communication providers and cryptocurrency stakeholders.

In terms of unilateral conduct, Mr Ostbye gave the example that certain exchanges or wallets could obtain a dominant position and discriminate against certain cryptocurrencies. For mergers, he highlighted the core issue as cross-ownership in cryptocurrencies. As an example, if there was proof of stake consensus, there could be certain stakeholders who hold a large stake in different cryptocurrencies and in that sense it could prevent cryptocurrencies from competing with each other. Banks, traditional payment services providers, or internet providers might acquire control over certain cryptocurrencies and associated platforms.

The Chair then turned to **Australia** who asked about pseudonymity, particularly in the context of cryptocurrencies. The Australian delegate was concerned with where problematic conduct was occurring even if private information was maintained.

Mr Ostbye explained that when it comes to permissioned blockchains, there are certain operators or stakeholders to focus upon. He gave R3 as an example, but also cited that it is difficult when it comes to pseudonymous open blockchains. However, criminal enforcers have their tools and Mr Ostbye opined that in terms of enforcement, there is optimism because most cryptocurrencies and blockchains will likely see the benefit of operating legally and have some sort of accountability. He said that those will also have the biggest impact on the economy. Overall, he highlighted that co-ordination is crucial so it is possible to be held liable even in large jurisdictions.

Mexico highlighted the importance of having interoperability among different platforms, not only inside each platform but also data portability to allow users to move from different platforms. As this would require effort to standardise data among platforms, the Mexican delegated asked if there is a spontaneous solution for this emerging or if there is a need for action by authorities.

The Chair then turned to **Italy** who asked whether a blockchain process could be patented as a business method, referring to the patentability of the technologies in themselves. The Italian delegate gave the example of technologies that are registered as standard essential patents (SEPs), if they meet the conditions.

Next, the Chair gave the floor to **Israel** who discussed the shifting balance in areas like auto parts where regulators have not had great access to data traditionally, but now have access to an enormous immutable database of transaction data. In those kinds of industries, the Israeli delegate asked how to balance the theory of harm of over transparency with the fact that all the transparency is also available for audit afterwards, which was not always the case.

The Chair turned to **Korea** who noted that in traditional competition law enforcement, safe harbours are normally set in terms of market share, and asked for the percentage of market share that would be appropriate compared to the brick and mortar industry? Korea also queried which criteria should be used to measure market share such as number of users, the volume of transaction, etc., or maybe combinations.

The Chair gave the floor to Mr Schrepel who asked Mr Simpson for his opinion on the development of new cryptocurrencies such as Monero and Zcash, which are oriented towards total anonymity. The Chair then invited Mr Tulpule to reply and present on the future of blockchain technology.

By presuming blockchain technology has been accepted by the market, Mr Tulpule said that there are a range of platforms, services, data analysis and other goods and services that are sold through regulated commerce on the blockchain platform. In the future, he asserted there should be a much wider acceptance than now, which will have impact on the regulators' work.

In terms of Israel's comment regarding the massive swathes of data, Mr Tulpule said that competition matters are fact-intensive. They involve collecting data, analysing data and drawing inferences from them. The more energetic the enforcement, there is a sense that the rigorousness of the analysis may drop because the same level of data may not be available in all the cases that you pursue. Mr Tulpule opined that with blockchain technology's pervasive use, the vigorousness of enforcement could be matched by the rigorousness of the analysis.

In terms of utility in enforcement, Mr Tulpule discussed key elements of blockchain: access to data; more informed and better decisions; an advanced level of granularity; and resolving the information asymmetry that is bound to exist between market participants involved in an anticompetitive act and the regulator who is going after them. He cited EC data of a study done on the timespan between the start of an investigation and the issue of a decision. Between 2001 and 2011, cases where the cartels were detected before the cartel was terminated took on average around 20 months longer. He then highlighted that in cases where a chief witness was available the decisions took 9.71 months shorter on average. Overall, such past statistics may not suggest whether more data will mean a shorter, faster process. However, he opined that should be true, because with blockchain technology the data is far more streamlined, organised and imputable. It is also difficult to remove, depending on the type of blockchain, and presuming it is a public blockchain. Therefore, blockchain should allow regulators to sift through data, get to the right type of data very quickly and then incorporate it into the analysis. This should lead to better information on the regulator side and better analysis.

Mr Tulpule then cited a case against Imperial Tobacco where the Office of Fair Trading (OFT) was involved in which there was a level of information asymmetry. He also noted a merger case at the EC level regarding Olympic/Aegean Airlines, which illuminated that the data needed to be a good indicator of the likely impact of future competition. Mr Tulpule highlighted that blockchain would not solve the previous point well, because merger analysis looks at what will happen further down the road.

Next, Mr Tulpule discussed how over the last 100 years, competition enforcement and theories of harm have become more complex because the data available for regulators to reach a certain assessment has become more complex. In the USA, China and Europe, cases that deal with merger control also experience longer clearance times because they are investigating more complex theories of harm, which are essentially far deeper and wider requests for information. With market definition, Mr Tulpule explained that even with more data to show there is price correlation, it is still not sufficient to demonstrate substitutabilty. As for presumptions, it could reduce the duration of a case, the amount of appeals or increase the number of appeals because along with the regulator, the market participants will also have access to much wider data. However, he noted that none of this is conclusive.

Mr Tulpule then discussed leniency applications, live data feeds and utility in compliance. He explained that with trade associations, even as information is gathered from member parties, it remains encrypted. The chairperson, which is usually a rotating member of participants, can only see the aggregated data, because everything else is given only to compliance people and legal counsel who are advising that relevant trade association. He then highlighted the possibility of live monitoring of market shares, which could help companies that are generally uncertain as to whether they are dominant, such as Microsoft or Coca-Cola, to verify if the level of sales received from the Nielson Scan data matches transactional data as it is happening in the real world. He opined this could lead to deeper engagement of in-house counsel because if there is better governance and control, in-house counsel will end up being a very good friend of the regulator.

Mr Tulpule suggested that blockchain could lead to more complex theories of harm, better information gathering and analysis, faster internal procedures and decision making for the regulators as well as stronger compliance protocols. In conclusion, Mr Tulpule discussed the impact on private competition enforcement. Assuming there are more complex theories of harm, he explained the impact that would have on a company trying to prove damages, especially in follow-on jurisdictions. Essentially, it would entail linking the complex theory of harm to the damages that company has suffered along with the evidence it may have to generate proof of that link. He cited the 2019 Roundwood case in Finland, in which a company provided millions of documents, yet failed to prove evidence of damages linking to competition infringement.

The Chair thanked Mr Tulpule for his presentation and noted that abundant and easily tradable data is positive in terms of both competition agencies' ability to intervene in a relevant way and the monitoring of compliance of firms.

The Chair then gave the floor to Mr Simpson who addressed Israel's question about the access to data on blockchains. He noted that there is a distinction between being able to access information using enforcement powers versus having it as a live feed. However, all regulators should have access to all information on a live basis, although perhaps as a node on every blockchain is going a few steps too far. Instead, he suggested that existing powers are sufficient. He noted that for agencies to obtain data they currently need reasonable cause to suspect an infringement. He argued that there was a danger in having antitrust regulators undertaking ex post assessments with the benefit of ex ante or live access to private data.

Ms Mulligan then took the floor to explain that in her opinion, there is no such thing as privacy in digital technologies. If people want access to specific data, they will be able to get access to that data, in particular police and law enforcement, even if it is complicated and technically expensive. From a technical perspective, she also underlined that interoperability is being worked on quite extensively. Finally, she said that the physical process of moving data from one system to the other does require some form of data standards, whether it is a blockchain standard or a data format standard, which ISO is working on.

Next, Mr Ostbye was given the floor to discuss the issue of standardization. He opined that the market must be allowed to evolve and that innovation must develop. As for patents, he explained that could be an issue when it comes to blockchains in the future and as Competition Agencies may have a role in patents. When it comes to anonymous currencies like Monero and SetCash, Mr Ostbye explained that all operate with some sort of coin mixing so that the receiver and sender of coins is blurred. They might be legitimate or not. Crime enforcers might not like them, but they do satisfy a need for privacy. Overall, he underlined that to stay legitimate they must adjust to regulations but it would be difficult for a legitimate firm to use them as an instrument for collusion.

Mr Schrepel then took the floor to answer Korea's questions. First, he explained that as far as the market shares to determine dominance, some markets may be on the blockchain only, whereas others might actually compete with brick and mortar so there is not a single answer. As for the criteria, the number of users, revenues and number of blocks could all be considered. He also opined they should probably be combined, but he did not think it possible to actually determine one methodology and say should always take this methodology into account. He concluded by asking if there is a blockchain antitrust paradox? He noted that, if competition law and antitrust is about being anti-trustees and that blockchain eliminates trustees because it is decentralized, is blockchain reaching what competition law was seeking for all those years?

The Chair then turned to Mr Tulpule who focused upon data and the ability to get quick data, by offering an example of the hash rate distribution for bitcoins, which is available on blockchain.info. He noted that the web portal shows the different mining pools and their market shares in confirming calculations thereby showing the type of data.

For the last comment of the roundtable, the Chair gave the floor to the **Netherlands**. The Netherlands offered an update on research done on blockchain by their country's competition authority that began in September 2017 until March 2018. The focus was on what blockchain means for the tasks of the Netherlands' consumers and markets authorities, which culminated in an internal document that aimed to increase the knowledge level of their organization on blockchain so they could better deal with issues once they arise. The paper looked at how blockchain works technically and practically in the Netherlands. This included a couple of case studies in the financial services sector on cryptocurrency, clearance and settlement, pensions and trade finance as well as the energy market. Overall, the paper showed that in the Netherlands blockchain could be used to replace existing processors with the goal to lower costs and reduce lead times but that only incidentally is blockchain being used to make third parties redundant. The exception to this was cryptocurrencies, which aimed at realizing an entirely alternative payment system. Otherwise, it was noted that when established market parties operated on private permission blockchains, this could possibly result in entry barriers. The Netherlands concluded that over the next two years their authority would continue to monitor and investigate blockchain.

The Chair concluded the roundtable by stating that it was clear that the nature of competition issues are not entirely different. He noted that there were two issues: the reduction in the cost of exchanging information and using information to provide services. The Chair also underlined how important the new generation of data through networks, private networks and competing networks, which creates for the enforcement of competition law both risks and opportunities because there are risks that some of this information could be used in certain cases to reduce competition.