COLLUSIVE BEHAVIOR IN PERMISSIONED BLOCKCHAIN

ABSTRACT

This paper identifies several collusive behaviors that businesses may engage within permissioned blockchain. It begins by explaining the key features of the blockchain technology. It is then followed by discussions regarding explicit collusion, concerted practice and anticompetitive foreclosure and the application of EU competition law. Through analyzing the scenarios in light of Art. 101 & 102 TFEU, the paper argues that the existing law is sufficient to deal with the challenges posed by the technology. The purpose of this paper is to identify the antitrust pitfalls in permissioned blockchain, so that users will understand the competition legal risks of the technology.

Author: Victor Chan

TABLE OF CONTENTS

INTRODUCTION

Blockchain is one of the buzzwords in recent years. Their best-known use is for cryptocurrency such as Bitcoin, which its unexpected rise and fall has led to increased public interest in digital currencies in general and their underpinning technology.[1] While commentators remain skeptical about cryptocurrency's long-term viability, it is well recognized that the technology underpinning Bitcoin – Blockchain – has potential for far broader applications. It has been suggested that "the way blockchain-based currency transactions create fast, cheap and secure public records means that they also can be used for many non-financial tasks".[2] Consequently, some have already been investigating the possibility of applying the technology in areas such as e-voting, land registry, and the supply chains. While some of these initiatives are government-led, most of them are funded by private companies.

Indeed, there is a growing number of firms working together to develop commercial applications using the technology. It is increasing popular for firms to form blockchain consortia, i.e. a group of companies that join together, seeking to develop and deploy business solutions based on blockchain technology. It has been estimated that currently there are more than 40 blockchain consortia globally, some of which are formed by industry leaders.[3] An example is Digital Trade Chain (DTC), a blockchain consortium formed by 8 leading European banks including HSBC, Société Général, UniCredit, and Banco Santander that aims at facilitating domestic and cross-border commerce for European companies by leveraging the blockchain technology.[4] Relatively recently, the consortium announced the establishment of a joint venture company, we.trade, that will be responsible for managing the DTC blockchain network.[5] Another example is the R3 blockchain consortium. Launched in 2015, over 80 of the world's largest financial institutions, such as HSBC, Bank of America, and Merrill Lynch, and central banks come together for the purpose of developing blockchain applications to address specific business challenges in different industries, including shipping, healthcare, insurance and financial services. As such, it seems there is a trend that firms are "banding together for blockchain".[6]

---

[1] BBC, 'Bitcoin falls below $6,000' (BBC News, 6 February 2018) <https://www.bbc.co.uk/news/technology-42958325> last accessed 14 August 2018

[2] European Parliamentary Research Service, *How Blockchain Technology Could Change Our Lives* (Science and Technology Options Assessment 2017) 4

[3] Deloitte University Press 'Banding Together for Blockchain: Does It Make Sense for Your Company to Joint a Consortium?' (Deloitte University Press 2017) 2

[4] KBC Group, 'KBC and Cegeka Trial Ground-Breaking Blockchain Application for SMEs' (KBC Group, 12 July 2016) <https://newsroom.kbc.com/kbc-and-cegeka-trial-ground-breaking-blockchain-application-for-smes> last accessed 14 August 2018; The eighth bank, Banco Santander, joined in 2017

[5] KBC Group, 'Digital Trade Chain Consortium Launches we.trade, Announces Joint Venture and Welcomes Santander' (KBC Group, 17 October 2017) <https://newsroom.kbc.com/digital-trade-chain-consortium-launches-wetrade-announces-joint-venture-and-welcomes-santander> last accessed 14 August 2018

[6] Deloitte University Press (n 3) 2

While in general the emergence of blockchain consortia is a good idea in the sense that everyone is contributing to release the full potential of the blockchain technology, the fact that firms, especially industry leaders, are now "assembling together" for blockchain may seem odd for antitrust regulators.[7] As with any new technology, competition authorities are paying close attention to the development of the blockchain technology. Indeed, two aspects of the technology may raise competition concerns. Firstly, blockchain as a digital distributed ledger. From a competition law perspective, particularly when several competitors are found sharing the same blockchain network, such functionality may be regarded as a mechanism to coordinate collusive behavior because members of the blockchain network may share sensitive information that is capable of reducing the strategic uncertainty in the market. Secondly, the 'decentralized' nature. One of the key characteristics of the technology is that multiple parties may interact with each other directly without the presence of a trusted single entity. In enabling this, there are mechanisms in place that help members of a blockchain network to reach consensuses before making collective decisions. However, such mechanisms could also be exploited by members of a blockchain network such that certain members could no longer use the network effectively. As such, it is at least theoretically possible that firms may engage in some conducts in blockchain that may go against competition law principle.

This paper aims to identify the antitrust pitfalls in permissioned blockchain and discuss the applicability of EU competition law in this regard. While the relationship between permissionless blockchain and competition law is equally interesting, this paper focuses only on permissioned blockchain. Moreover, the focus of the paper is on competition issues that arises from the architecture of blockchain technology. In other words, competition concerns that are unique to blockchain. As such, other antitrust considerations, such as standard setting and unilateral conduct by a dominant firm, will not be discussed.

The paper is divided into four chapters. After this Introduction, an overview of the blockchain technology will be provided. In Chapter Two, it explores explicit collusion in the context of permissioned blockchain. Chapter Three discusses how members of a blockchain network may share information on a blockchain. Chapter Four focuses on anticompetitive foreclosure that take place in a permissioned blockchain. Before ending with a conclusion, the paper explores other areas that are worth to conduct further research.

[7] Adam Smith once famously said: "People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivances to raise prices […] But though the law cannot hinder people of the same trade from sometimes assembling together, it ought to do nothing to facilitate such assemblies, much less to render them necessary"; Adam Smith, *The Wealth of Nations* (Book IV, Chapter VIII, W.Strahan and T. Cadell 1776) 660

CHAPTER ONE: BLOCKCHAIN

This Chapter provides an overview of the blockchain technology. In general, the technology presents five key characteristics which can be understood in terms of (a) distributed ledgers, (b) shared control of data, (c) participation criteria, (d) consensus protocols, and (e) immutability. These features will be outlined in turn below. The Chapter concludes by providing a summary of the operation of a typical blockchain network.

Distributed Ledgers

At its simplest, blockchain are digital ledgers that combine certain cryptographic technologies.[8] Blockchain can be utilized to record every type of transaction involving value, including money, goods and property. In the case of Bitcoin, the technology is being used to store the details of every transaction in order to stop the same Bitcoin from being 'double spent'. However, rather than being maintained and stored by a central entity, this digital ledger is 'distributed' to all members of the network. In essence, information that is stored in a blockchain network will be automatically replicated and shared among the users of the network. In other words, blockchain enable sharing of data.

Shared Control of Data

In fact, the technology of 'sharing of data', whether users need to have data access in real-time or not, has been resolved prior to the invention of blockchain. Consider Cloud Storage. In general, it enables users to upload data to a network of remote, connected servers, which can then be accessed, modified and shared across multiple devices by the users. The technology here typically does not involve the blockchain technology. Therefore, although similarly blockchain can share data, this is not unique.

What is fascinating about blockchain is that it enables 'shared control of data'. This is a new notion. In the past, data on a digital database is controlled by a single entity.[9] As such, at technical level, the stored data can be modified only when the controlling authority executes the request. For example, in Cloud Storage, although users seemingly have control over their own data, the stored data is ultimately controlled by the entity which maintains the severs, although its activities will be constrained by legal and contractual obligations. In other words, when a user 'modifies' his/her own data, the changes are actually made by this single entity. In other words, we typically rely on a trusted authority to maintain our records.

Rather than putting control on the hands of a single entity, blockchain enable data to be jointly controlled by the parties according to a set of pre-agreed rules, known as 'consensus

[8] In other words, while blockchain are a form of distributed ledgers, it is not true that all distributed ledgers are blockchain. To qualify as a blockchain, a distributed ledger must deploy certain technologies, in particular the hash function.

[9] Amazon Web Services (AWS), 'Cloud Storage' (AWS, 2018) <https://aws.amazon.com/what-is-cloud-storage/> last accessed 14 August 2018

protocols'. In general, consensus protocols are sets of rules that facilitate members of a blockchain network to reach consensus regarding how data should be handled, in particular whether a proposed transaction should be appended to the blockchain. Accordingly, control is shared in the sense that the power of how data should be dealt with is not vested in a single entity, but on the hands of all members of the network.

Participation Criteria

In general, there are three types of members in a blockchain network.[10] Firstly, the 'miners'. These are members who assemble data (e.g. transactions) into blocks and propose blocks to be added on the blockchain. Secondly, the 'nodes'. These members are responsible for storing the ledger and validating new blocks. Lastly, the 'users', who are the end users of the functionality of the blockchain technology.

There are two main types of blockchain, namely permissionless and permissioned.[11] The only difference between these models relates to who can participate in what. In the permissionless model, everyone is free to join the network, free to propose new blocks, and free to maintain the ledger. In other words, such model is completely open such that anyone can be a miner, a node, or a user. An example of the permissionless model is Bitcoin.

The permissioned model on the other hand can be understood as a closed platform with a defined number of participants. Typically, only authorized parties can join the network. Therefore, members in the network are usually known and trusted by each other. Permissioned blockchain can be configured to impose further restraints on the power of the members. Depending on the set-up of the blockchain, it is possible to limit the power of proposing new blocks and the power of storing the ledger to a smaller number of parties.

Consensus Protocols

As mentioned, how data should be handled on blockchain is based on 'consensus'. In general, before a miner could propose a new block to be added on the blockchain, he must demonstrate some sort of 'faithfulness' to show that the proposed block represent the 'true version' of the information and he is not malicious. The nodes will then verify the proposed block individually and decide whether this block should be appended on the blockchain. Should the nodes validate the block, it will be added on the blockchain. Otherwise, it will be rejected and sent back to the pool of blocks. The precise rules of a consensus protocol vary according to the needs of the members of a particular blockchain network, although

[10] Jean Bacon and others, 'Blockchain Demystified' [2017] Queen Mary University of London, School of Law, Legal Studies Research Paper No. 268/2017, 20 – 21

[11] Ramesh Gopinath, 'Checking the Ledger: Permissioned v.s. Permissionless Blockchain' (IBM, 28 July 2016) <https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-blockchain/> last accessed 14 August 2018

consensus protocols such as 'proof of work', 'proof of stake', and 'practical Byzantine fault tolerance' are commonly used by the blockchain community.

Immutability

Blockchain are immutable in the sense that the content and sequence of the stored data cannot be altered without being easily detected by other parties in the blockchain. Two elements are key here.

First, hash function. It is a software that converts digital inputs (e.g. a block of transactions) into a string of digits. This string of digits is known as hash value and is unique to that data item. In other words, the hash value is effectively the fingerprint of that data item. Importantly, hashing is 'one-way' in the sense that it is not possible to recreate the original input from its hash value. Moreover, if the input data is being modified even in the slightest, its hash value will be changed as well.

Secondly, blocks. As suggested by its name, data are stored in a blockchain in blocks. Each block thus contains a bundle of data (e.g. transactions records). However, in addition to data, each block also contains the hash of the previous block. In other words, the fingerprint of the previous block is included and forms part of the subsequent block. As a result, this fixes all existing blocks and a tamper-evident chain of blocks is formed – contents within a block cannot be altered without changing the hash value of the block. However, any attempt to 're-hash' the block will break the chain between itself and the subsequent block as the latter contains the original hash value of that block. Therefore, any tampering will be obvious to a viewer. Furthermore, as the blockchain technology enables the ledger to be replicated and stored in multiple locations, this means that all copies of the chain will need to be changed in the same way.

Lastly, it is important to note that data on blockchain is by default not encrypted. Especially when the set-up of the blockchain requires nodes to certify new blocks, the nodes will need access to the content in the blocks in order to cross-check with its own local copy of the ledger.

Conclusion

A typical blockchain network runs as follows:

1. After being authenticated, users of a blockchain network may submit a request to the blockchain network.
2. The message will be picked up by miners who will pack several transactions together into a block. Miners will then broadcast this block back to the network and propose it should be added on the blockchain

3. Upon the receipt of the suggested block, the nodes will verify whether the block contains the valid transactions and references by hashing the correct previous block on their chain.[12]
4. If the nodes come to an agreement that they are satisfy with the block, they will add the block to the blockchain. Otherwise, the proposed block will be discarded.

CHAPTER TWO: EXPLICIT COLLUSION

This Chapter examines explicit collusion in the context of blockchain. The Chapter will first provide the definition of 'explicit collusion'. After that, it discusses three forms of explicit collusion, namely information exchange, Smart Contracts & IOT, and collective boycotts. It is then followed by an analysis of these scenarios under the EU competition law.

Explicit Collusion

Explicit collusion occurs where "undertakings collude, collectively, to exploit their joint economic power and to improve their profitability".[13] Explicit collusion may take the form as an anticompetitive agreement or an anticompetitive concerted practice. Central to the notion of 'explicit collusion' is that there must be direct communication between the undertakings with the intention to coordinate and/or monitor each other's actions for the purpose of raising profits above competitive levels.

Of all explicit collusion arrangements, cartels are seen as the "supreme evil of antitrust".[14] Cartels are explicit attempts to eliminate competition in the market without producing any pro-competitive effects. Firms to a cartel typically employ means such as price fixing, allocation of production quotas, or sharing of geographic markets or product markets for the purpose of transferring wealth from consumers to themselves. These conducts undermine the free market economy and thus provoke hostile reactions from competition authorities.

Because of the strong attitude of competition authorities towards cartels, it is almost impossible to identify cartels nowadays. On the bright side, this shows that competition authorities have successfully created a competition culture, thereby firms are deterred from engaging in conducts that would severely harm the competition landscape of a market. However, it may also be argued that cartels nowadays are working in secrecy, thereby avoiding being detected by the authorities. Therefore, theoretically, cartels still exist, and it is likely that they are evolving as well. Blockchain is a buzzword in recent years. As such, one

[12] Konstantinos Christidis and Michael Devetsikiotis, 'Blockchain and Smart Contract for the Internet of Things' (2016) 4 IEEE Access 2292, 2293
[13] Alison Jones and Brenda Sufrin, *EU Competition Law: Text, Cases, and Materials* (6th edn, OUP 2016) 650
[14] *Verizon Communications, Inc. v Law Offices of Curtis V. Trinko,* 124 S. Ct. (2004) [879]

could imagine seeing firms exploit the technology for the purpose of facilitating their collusive behavior.

Cartel and Information Exchange

The successful operation of a cartel depends on various factors, including effective mechanisms for coordination.[15] After parties have agreed on the course of action that will be be taken on the market, it is then for them to implement the agreement. In doing so, there is a concern that firms in a cartel may cheat on the agreement, knowing that, according to the prisoners' dilemma,[16] it will profit the most if it charges a low price while its competitors are charging a high price. Hence, cartels would design measures to monitor output and prices of individual members in order to detect cheating. In some cases, however, cheating may be seemingly detected but in fact it is the market condition that affects the result.[17] Building trust among members is therefore difficult for cartels as, at the least, it may be hard to tell whether or not someone is cheating. As such, it is essential to have effective mechanisms to facilitate coordination among the firms.

Blockchain may represent a solution for cartels. The idea is that a blockchain may be employed solely for the purpose of exchanging strategic information. In the context of explicit collusion, members of a cartel may first agree on the course of action that will be taken on the market. This will then be followed by creating a permissioned blockchain to exchange sensitive information, such as prices and sales. Information exchange in blockchain will be discussed in detail in the next chapter in relation to concerted practice.

For cartels, the use of permissioned blockchain may enhance coordination between members. First, only authorized persons would be able to access to a permissioned blockchain. This then satisfies the need of secrecy for cartels. Moreover, in blockchain, information is shared directly between members without the presence of a middleman. Consequently, this reduces the possibility of miscommunication or tampering by third parties. Furthermore, blockchain are transparent in the sense that all information would be available to all members in the network in real-time. It is believed this would promote trust among members and reduce the incentive to cheat on the cartel agreement.

Cartels, Smart Contract, and Internet of Things

Alternatively, cartels may combine the blockchain technology with smart contracts and Internet of Things to run a cartel more effectively. Automate process will be enabled if a smart contract and Internet of Things are placed on a blockchain.

---

[15] Margaret Levenstein and Valerie Suslow, 'What Determines Cartel Success?' (2006) 44(1) Journal of Economic Literature 43, 45

[16] ibid.

[17] Ibid. 71

A smart contract is "a computerized transaction protocol that executes the terms of a contract".[18] In other words, contractual clauses are translated into computer code which will then be placed on a computer program that allows it to self-execute. In fact, computer codes that enable automate processes is not a new concept – we have been doing this ever since computers are invented. One example is the monthly direct debit out of a bank account. However, modern smart contracts may take such coding, and combine it with the potential of the blockchain technology.

Placing a smart contract on a blockchain means this set of computer code will run on an interoperable and incorruptible computer program. In essence, the computer code executes independently and automatically on every node in the network in parallel once the predetermined terms and conditions are met, in particular when the triggering and output events have been checked and verified by the participants.[19] As such, the execution of the smart contract is not controlled by a single entity. Instead, multiple parties are jointly responsible to update the computer code in order to trigger the automate process and to approve whether the process should be triggered. Moreover, the computer code is replicated and shared among all members, rather than within the hands of a single entity. This does not only allow authorized parties to see the computer code, but more importantly any attempts to modify the computer code will be visible by other participants in the network. Therefore, should anyone wish to alter the computer code, this must be done jointly by the members of the blockchain network.

The Internet of Things (IOT) is another technology that is becoming increasingly popular. In essence, IOT can be understood as "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data".[20] This network of interrelated electronic devices is typically employed for the purpose of collecting data in its surrounding area, monitoring remotely, or even interacting with other similar devices and making decisions without human intervention.[21] The blockchain technology may further enhance the functionality of IOT in two ways. Firstly, by placing IOT on a blockchain, IOT users may then have a verifiable, immutable, and secured method of recording data processed by these devices. The activities of these devices will also become visible to users. Secondly, it is possible to link blockchain-based smart contracts by the IOT, thereby enabling automated processes, for example large scale remote systems management.

---

[18] Nick Szabo, 'The Idea of Smart Contracts' (Nick Szabo, 1994) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> last accessed 14 August 2018

[19] Konstantinos Christidis and Michael Devetsikiotis (n 13) 2296

[20] Jon Wood, 'Blockchain of Things – Cool Things Happen When IOT & Distributed Ledger Tech Collide' (Medium, 20 April 2018) <https://medium.com/trivial-co/blockchain-of-things-cool-things-happen-when-iot-distributed-ledger-tech-collide-3784dc62cc7b> last accessed 14 August 2018

[21] Margaret Rouse, 'Internet of Things (IOT)' (IOT Agenda, June 2018) <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT> last accessed 14 August 2018

It is argued that the combination of the above technologies may be particularly appealing to cartels. If a blockchain-based smart contract is being used by cartels, firms not only can share information more efficiently, but they could also codify the cartel agreement into the technology. As a result, where punishment mechanisms are agreed into the agreement, the blockchain-based smart contract enables firms to enforce the punishment more effectively.[22] More specifically, when certain conditions indicate that some members deviate from the agreement, the inserted punishment mechanisms will be triggered, and compensation from the cheating members will be automatically made to the cartel. As the smart contract is implemented on a blockchain, there will be no single source of control in relation to cartel agreement. Therefore, unless all other members approve, the cartel agreement cannot be modified. Consequently, the credibility of the punishment is increased and the incentives to cheat is deterred. Furthermore, with IOT being connected to a blockchain-based smart contract, cartel members' behavior can be monitored by its fellow members remotely and directly through these smart electronic devices, rather than relying on each other's self-reporting. When these devices collect data that signifies that certain members are cheating, such data may trigger the smart contract to impose punishment on these members. As such, for cartels, the combination of IOT, smart contracts, and blockchain ensures members commit to the agreement and improves the accuracy of information in relation to members' behavior.

Collusive Boycott

Beyond cartels, explicit collusion in permissioned blockchain may also take the form of collective boycotts. A collective boycott can be understood as an agreement between a group of competitors to "exclude an actual or potential competitor".[23] In blockchain, a firm may be excluded by other members of the network via the consensus protocols.

Central to the blockchain technology is the idea of 'shared control'. As such, whether a transaction can be settled depends on whether members of the blockchain network agree that the transaction should be settled. In blockchain language, when a miner proposes a new block to be appended on the blockchain, the block in question will need to be verified by the nodes independently. The block would only be added onto the blockchain if the nodes reach a consensus regarding its validity. The question is then how much consensus is required. Normally, in permissioned blockchain, a consensus is reached if 2/3 of the nodes agree on the same matter[24]. In other words, a unanimous decision is not required. Accordingly, it is argued that some firms may utilize this 1/3 'buffer' to exclude their competitors. More specifically, these firms may agree among each other that they would not verify certain members'

[22] Harrington observed that enforcing punishment in cartels may not be as straightforward as first thought. In some cases, some firms may be reluctant to make compensation; Joseph Harrington, 'How Do Cartels Operate?' (2006) 2(1) Foundations and Trends in Microeconomics 1, 59

[23]European Commission, 'Guidance on Restrictions of Competition "By Object" for the Purpose of Defining Which Agreements May Benefit from the De Minis Notice' (SWD(2014) 198 final) 11

[24] The mechanisms of consensus protocols in permissioned blockchain will be discussed in detail in Chapter Four

transactions. If they are not the nodes of the network, they may instruct the nodes to do the same.

EU Competition Law Application

Explicit collusion falls within the scope of, and is prohibited by, Art. 101 TFEU.[25] In general, the provision prohibits certain joint conduct between two or more undertakings "which have as their object or effect the prevention, restriction, or distortion of competition".[26] While the blockchain technology, along with smart contracts and IOT, are relatively new concepts, it is argued that the existing laws remain applicable to these cases where new technologies are involved.

The notion of 'agreement' in EU competition law has been broadly construed. In *Bayer,* the Court summarized the notion of 'agreement' as emanated in EU case law and suggested that the notion "centers around a concurrence of wills between at least two parties, the form in which it its manifested being unimportant so long as it constitutes the faithful expression of the parties' intention".[27] As such, the notion of agreement is rather non-formalistic. This then allows competition authorities to utilize the notion in more imaginative ways. For example, in *AEG-Telefunken*, the Court confirmed that an agreement existed even if it was imposed by one party on another unilaterally.[28] Crucial to the notion of 'agreement' is therefore not the form taken by an agreement but a joint intention to behave in a way that would restrict competition.

In blockchain context, it then seems firms may 'accidentally' 'agree' into an anticompetitive collusion in various ways. For example, the mere fact that a firm agree to participate in a network that aims to facilitate an anticompetitive agreement may satisfy the element of 'agreement'. In *Cement,* it was held that "it is sufficient for the Commission to show that the undertaking concerned participated in meetings at which anti-competitive agreements were concluded, without manifestly opposing them, to prove to the requisite standard that the undertaking participated in the cartel […] The principles […] also apply to participation in the implementation of a single agreement".[29] Putting this into a blockchain network, it appears that where a firm joins a blockchain network that is set up for the purpose of conducting some anticompetitive collusive activities, such firm may be deemed as one of the participants to that agreement simply because it became one of the members of the blockchain network even if it actually has no intention to put the agreement into effect. This remains true even if the firm is capable of adducing evidence showing that its behavior does not reflect the terms of the agreement, and thus arguing that it has never participated in that agreement. Another

[25] Article 101 of the Treaty on the Functioning of the European Union
[26] ibid.
[27] Case T-41/96 *Bayer v Commission* [2000] ECR II-3383 [69]
[28] Case 107/82 *AEG-Telefunken v Commission* [1983] ECR 3151
[29] Cases C-204, 205, 211, 213, 217, and 219/00 *P, Aalborg Portland AS v Commission* [2004] ECR I-123 [81] – [83]

scenario concerns the situation where firms are already in a blockchain network but the anticompetitive agreement emerges subsequently. A collective boycott case may illustrate this scenario. For example, a blockchain which contains 9 firms is launched for facilitating normal business operations. Five of the firms decide to boycott three other members of the network with the remaining firm has not indicated whether or not it would participate in this collective boycott. According to *Cement*, it would appear that the mere fact that the firm remains in silence is sufficient to establish that it is one of the participants to the agreement as it "has given the other participants to believe that it subscribed to what has decided there and would comply with it".[30] As such, firms must not only be careful not to explicitly agree to participate in anticompetitive agreements, they must also be mindful of falling into what is known as "passive mode of participation".[31]

Where it is established that firms are engaging in an explicit collusion, the use of blockchain would not afford any defense. Inherently, blockchain are merely distributed ledgers. As such, no matter how transformative it may seem, a blockchain is not capable of self-learning. Therefore, humans, instead of the technology, remain as the 'master-mind' of the collusive behavior in question. Where firms exploit the technology to run the cartel more effectively, a blockchain is simply being used as an 'extended arms' of the firms in the sense that "cartel members program the computers to help effectuate the cartel, and monitor and punish any deviation from the cartel agreement".[32] This is to be contrasted with the "Digital Eye" scenario, whereby "the machines, through self-learning and experiment, independently determine the means to optimize profit".[33] In other words, computers in the latter scenario is capable of engaging in 'collusive behavior' automatically on behalf of humans. However, in the blockchain context, humans, as opposed to artificial intelligence, remain to be the main actors, and are responsible to make decisions. This is still the case even where IOT is involved as these electronic devices are involved just for the purpose of monitoring any deviation, thereby ensuring the success of the cartel in question. As such, it is believed that competition authorities will have no difficulty in relying on the established case law and the general framework of Art. 101 TFEU to prove its case.

Conversely, a blockchain may in fact become a useful evidence for competition authorities to strengthen its case. Blockchain' immutability means that all information that is stored on the network, most notably records about prices, sales, data collected by IOTs, and the cartel agreement which is embedded on the blockchain via smart contracts, will be in theory permanently available in the network. Accordingly, when competition authorities gain access to the blockchain network, a ledger which shows the entire history of the cartel in question

[30] ibid. [82]
[31] ibid. [84]
[32] Ariel Ezrachi and Maurice Stucke, 'Artifical Intelligence & Collusion: When Computers Inhibit Competition' (2016) 2017(5) University of Illinois Law Review 1776, 1784
[33] ibid. 1783

would be resurfaced. The recovered information will then be critical for the purpose of assessing the scope of the agreement and its competitive outcomes

CHAPTER THREE: CONCERTED PRACTICE

This Chapter primarily concerns information exchange that take place in a blockchain network. The Chapter will start by discussing the relationship between concerted practice and information exchange. The next section explores how members of a blockchain network may share information and the type of information that is typically shared. The last section analyzes information exchange in blockchain under EU competition law.

Concerted Practice & Information Exchange

Information exchange can take place in different context. In general, there are three main scenarios: (a) Information exchange as part of an agreement, (b) information exchange as part of a cartel, and (c) pure information exchange.[34] Information exchange that is ancillary to an agreement or a cartel will be assessed in the context of the agreement or cartel in question.[35] As far as pure information exchange are concerned, such information sharing between undertakings is 'stand-alone' in the sense that it is not dependent on a cartel or an agreement. The focus of this chapter will be pure information exchange. From the outset, it is important to note that the law in this area is rather controversial and thus there is no clear rules for firms to adhere to.

Pure information exchange are typically assessed as concerted practices under Art. 101 TFEU. The term 'concerted practice' can be understood as a 'catch-all' provision that aims to capture undertakings which seek to evade the application of Art. 101 TFEU by colluding in a way that fall short of an 'agreement'. The classic definition of 'concerted practice' can be found in *Dyestuff,*[36] in which the Court held that it is "a form of coordination between undertakings which, without having reached the stage where an agreement properly so-called has been concluded, knowingly substitutes practical cooperation between them for the risks of competition".[37] Far from requiring an actual plan to be worked out, the Court in *Suiker Unie* held that it would be sufficient if there had been "any direct or indirect contact between operators, the object or effect whereof is either to influence the conduct on the market of an actual or potential competitor or to disclose to such a competitor the course of conduct which they themselves have decided to adopt or contemplate adopting in the market".[38] As

[34] Organization for Economic Co-operation and Development, 'Roundtable on Information Exchanges Between Competitors Under Competition Law' (DAF/COMP/WD(2010)118 3

[35] ibid.

[36] Cases 48, 49, and 51–57/69, *ICI v Commission* [1972] ECR 619 [64]

[37] ibid. [61]

[38] Cases 40-48, 50, 54-56, 111, 113 & 114/73, *Suiker Unie* [1975] ECR 1663 [174]; The rationale behind this decision is that the notions of 'coordination' and 'cooperation' within the definition of 'concerted practice' must be understood in the light of a traditional concept that is inherent in EU competition law, that is each

'concerted practice' does not require an actual plan, it appears all that is required is the existence of a "reciprocal cooperation or a joint intention to conduct themselves in a specific way, disclosed through direct or indirect contact, designed to influence the conduct of an actual or potential competitor or to reveal to them the course of conduct that will or may be adopted on the market".[39]

As such, reciprocal information exchange may constitute a mechanism for substituting practical cooperation between the undertakings involved for the risk of competition. The concept of 'reciprocal' is however a broad one. In *Cimenteries,* it was held that the condition is met "where one competitor discloses its future intentions or conduct on the market to another when the latter requests it or, at the very least accepts".[40] As such, the concept of information exchange encompasses cases where undertakings have discussed and communicated their future plans in the market, as well as cases where the conveyance of information does not involve an express endorsement on the part of all the participants.[41] The Court in *Tate & Lyle* took this one step further by holding that the condition would be met even where "the participation of one or more undertakings in meetings with an anticompetitive purpose is limited to the mere receipt of information concerning the future conduct of their market competitors".[42] Stretching this decision further, it would appear that the requirement would be satisfied even if an undertaking receives an unsolicited email or fax from its competitors disclosing their future intention. Therefore, information sharing between undertakings would be prohibited where it eliminates "the risks of competition and the hazards of competitors' spontaneous reactions".[43]

Information Exchange in Permissioned Blockchain

At its core, a blockchain is a distributed ledger. It is therefore natural for members of a blockchain network to store information on it and share the same across the network. In permissioned blockchain, only trusted nodes will be authorized to store copies of the blockchain. These nodes may or may not be the users of the blockchain network. Where a node is a user at the same time, it should be able to see the stored information anytime it wants. Otherwise, where a user is not a trusted node, it would have to access the blockchain through a node. In general, new information will be available as soon as the block carrying the said information has been verified and added to the blockchain. In some permissioned blockchain, such process could be dealt with within seconds.[44] In other words, new

---

economic operator must determine the policy that it intends to adopt on the market in the future independently.

[39] Alison Jones and Brenda Sufrin (n 13) 153

[40] Cases T-25, 26, 30–32, 34–39, 42–46, 48, 50–71, 87, 88, 103, and 104/95, *Cimenteries CBR v Commission* [2000] ECR II-491 [1849]

[41] Albertina Llorens, 'Horizontal Agreements and Concerted Practices in EC Competition Law: Unlawful and Legitimate Contacts Between Competitors' (2006) 51(4) The Antitrust Bulletin 837, 859

[42] Case T-202/98, T-204/98 & T-207/98 *Tate & Lyle plc v Commission* [2001] ECR II-2035 [57] – [59]

[43] *ICI v Commission* (n 31) [119]

[44] More details will be provided in Chapter Four.

information could be available to all users of a blockchain network almost immediately after a new request is submitted to the network.

However, it may also be argued that certain users could acquire new information even earlier. As will be explained in more detail in Chapter Four, it is common to see permissioned blockchain feature a 'leader' whose responsibility is to propose blocks to be verified and added on the ledger. Similarly, such leader may or may not be a user of the blockchain network. Where the leader is a user of the blockchain network at the same time, he may acquire information as soon as when he is required to verify the proposed transaction. In fact, the idea that blockchain are encrypted may be a misleading thought. This is because, as mentioned in Chapter One, parties that are responsible to certify transactions would require access to at least a subset of information that is stored in the blocks so that they can cross-check the proposed blocks against their records in order to verify the transactions. Therefore, it seems unlikely that users of a blockchain network would encrypt the entire transaction before submitting a request on the network. As such, leaders may obtain certain information during the transaction verification process and disclose it to other members of the blockchain network. Alternatively, leaders may add comments, known as 'noise' in blockchain language, to blocks during the verification process, although such comments are unlikely to be useful to others and are not necessary for the blockchain to function.[45] Nodes may then acquire certain information from these comments when they are asked to confirm these blocks. It is argued that the presence of these two mechanisms allow members of a blockchain network to gain information before the nodes have updated their local copies of the ledger.

As mentioned, blockchain can be programmed to record virtually everything of value. Currently, blockchain are mainly used by businesses to record commercial transactions. This entails information such as parties to the transaction, transaction history between the parties, payment, amount, etc. could be found within a block and, depending on the degree of encryption configured by the parties, such information may be visible to members of the blockchain network.[46] Where however a smart contract is being placed on a blockchain, a wider variety of information may be found in the blocks. In particular, parties to such a blockchain network would store information regarding what has occurred, thereby triggering the automated process. As such, what is actually contained in a blockchain depends on how it is being set-up and how the parties intend to use the blockchain for.

EU Competition Law Application

[45] Kiran Desai, 'Blockchain and Competition Law' (Law Alert, Ernst & Young LLP 2018) 2

[46] https://www.blockchain.com/btc/block/0000000000000000062e8d7d9b7083ea45346d7f8c091164c313eeda2ce5db11 shows a Bitcoin blockchain. This provides an insight regarding that is typically stored in a blockchain.

Pure information exchange in itself may be sufficient to establish a violation of Art. 101 TFEU by object. In *T-Mobile*, it was held that information exchange is tainted with an anticompetitive object "if the exchange is capable of removing uncertainties concerning the intended conduct of the participating undertakings" and facilitating, directly or indirectly, the fixing of selling prices or any other trading conditions.[47] In its Guidance Paper, the Commission summarized information that is capable of reducing certainty in the market as 'strategic data', and such data includes information relating to prices, customer data, sales figures, individual output.[48] As such, where such information is stored on a blockchain, it seems that the very use of this blockchain network is susceptible to antitrust scrutiny. In particular, competition authorities may deem the sole purpose of setting up this blockchain network is to coordinate anticompetitive collusive behavior.

Where information exchange is not found to have its object the restriction of competition, it may still fall foul of EU competition law if the effect of such exchange is likely to have restrictive effects on the market. In assessing whether the sharing of information may restrict competition by effect, the Commission considered that the test is to compare the "likely effect of the information exchange with the competitive situation that would prevail in the absence of the specific information exchange".[49] For this purpose, regards will be given in relation to "the economic conditions on the relevant markets and the characteristics of information exchanged".[50] As far as market characteristics is concerned, the Commission stated that certain market conditions would render it easier to sustain coordination. In particular, information exchange will be more likely to restrict competition in markets which are "sufficient transparent, concentrated, non-complex, stable and symmetric".[51] As for the characteristics of information, the more strategic the information the more likely the Commission will find the exchange restricts competition. In assessing the strategic nature of the information involved, the Commission will consider factors such as age of the information, aggregation of the information, market coverage, frequency of the exchange, and the venue where the exchange of information took place.[52]

Applying the above to the blockchain context, it is argued that, even if strategic data is not exchanged, where several competitors are found to be sharing the same blockchain network, it is highly suspicious in the eyes of competition authorities. Concluding from the previous section, it seems that currently information that is stored on blockchain primarily relates to firms' past and current behavior. Although firms' future intentions are normally not found in a blockchain network, competition authorities may argue that the existing information may

[47] Case C-8/08 *T-Mobile* [2009] ECR I-4529 [37], [43]
[48] European Commission, 'Guidelines on the Applicability of Article 101 of the Treaty of the Functioning of the European Union to Horizontal Co-operation Agreements' (2011/C 11/01) 19
[49] ibid. 16
[50] ibid.
[51] ibid. 17
[52] Para. 19 – 21

nevertheless provide the firms a 'focal point' at which they can "reach a common understanding about the terms of coordination".[53] Moreover, such information may also "facilitate stability of collusion by enabling monitoring of deviations".[54] Accordingly, where the existence of parallel conduct between undertakings is established, competition authorities may argue that such conduct is the result of coordination based on the information exchanged on a blockchain network. In other words, blockchain may well become a 'plus factor' for competition authorities to conclude that the parallel conduct in question is the result of coordination.

Where a blockchain network is held to be a mechanism that facilitates coordination between undertakings, whether it is by effect or by object, it is argued that the leader will be held liable as well even if he is not a member of the cartel. EU competition law precludes any direct or indirect contact between undertakings which aims at influencing each other's conduct on the market. Therefore, any indirect exchange of information between undertakings (the 'spokes') that take place through an intermediary (the 'hub') is also prohibited. For example, in *JJB Sports plc,*[55] it was held that a concerted practice in the context of 'hub and spoke' arrangements may be established where (a) a retailer intended that the information be passed on by the supplier, (b) another retailer knew that the information had been provided by the first retailer, and (c) the second retailer used that information in setting its conduct in the market.[56] In the blockchain context, nodes or users of a blockchain network will be regarded as the spokes, whereas the leader will be deemed as the hub. Where a case of 'hub and spoke' arrangement is established, the hub may be held liable as well.[57]

However, there are two areas that competition authorities must pay attention to when proving the existence of a concerted practice in the context of an online system, which arguably includes the blockchain technology. First, while the concept of 'reciprocal' is widely defined and clearly covers the sharing of information in blockchain context, it nonetheless has limits. The case *Eturas* concerned an allegation of coordination that was taken place via an online travel booking system used by more than 30 travel agents in Lithuania.[58] The Court was asked whether the fact that a message, which concerns the capping of the level of online discounts which the travel agents should grant to customers, was sent via a personal electronic mailbox on the online system is sufficient to establish that its addressees became or should have become aware of its content and by fail to oppose the application of such a discount restriction they acquiesced in a way that would be held liable for engaging in

[53] Organization for Economic Co-operation and Development (n 29) 2 – 3
[54] ibid.
[55] *JJB Sports/ All Sports v Office of Fair Trading* [2006] EWCA Civ 1318
[56] ibid. [91]
[57] In Case AT. 39861 Yen Interest Rate Derivatives, the Commission sanctioned ICAP as one of its borker facilitate the cartel in question by serving as a conduit for collusive communications
[58] Case C-74/14 *Eturas UAB v Lietuvos Respublikos konkurencijos taryba* EU:C:2016:42

concerted practices.[59] Central to this case was the contention by the applicants who argued as they had not opened and read the message they could not be presumed to have been aware of the message and so could not have engaged in a concerted practice. In its response, the Court suggested that "infringements of competition law are subject to the presumption of innocence".[60] Accordingly, where there is no evidence that the applicants have actually read the message, competition authorities are precluded from inferring that they ought to have been aware of the content of the message simply from the mere dispatch of the message. As such, it seems that one lesson can be learnt from this case is that 'actual awareness' is one of the essential elements to demonstrate whether information exchange has taken place. Applying this in the blockchain context, it is argued that, in order to show that parties to a blockchain network have shared information, competition authorities must show the users have actually read their local copies of the ledger. This is particularly true where a user could only access to the blockchain through a node.

Another area competition authorities must pay regards to is the line of case law relating to Business-to-Business (B2B) e-marketplaces. B2B e-marketplaces are "software systems that allow industrial buyers and sellers to transact business online over the Internet through a central node".[61] While B2B e-marketplaces increase communication and transparency in the market, the flipside of the coin is that it is susceptible to being exploited as a platform for exchanging strategic data between competitors. Nonetheless, the Commission recognizes the pro-competitive effects of such marketplaces and has largely accepted that such platforms do not infringe Art. 101 TFEU. For example, in *Volbroker*, the Commission cleared the creation of an electronic brokerage service for trading foreign currency options after the founding firms gave several undertakings to the Commission which aimed at "building 'Chinese walls' between the joint venture operating the exchange and the parent companies which are active as market participants".[62] As such, it seems that the Commission is in principle not against the use of e-marketplaces as long as the anticompetitive concerns had been dealt with. Perhaps more guidance could be found in *Covisint.*[63] After clearing the establishment of an automotive e-marketplace, the Commission commented it is satisfied with the potential competition concerns had been eliminated, particularly because the platform is "open to all firms in the industry on a non-discriminatory basis, is based on open standards, allows both shareholders and other users to participate in other B2B exchanges […]".[64] It is argued that the Commission's approach regarding e-marketplaces may to some extent reflect where the law will stand in relation to blockchain networks. The blockchain technology largely produces the

[59] ibid. 25
[60] Ibid. 23
[61] Joachim Lücking, 'B2B E-Marketplaces: A New Challenge to Existing Competition Law Rules?' (Paper Presented at the Conference "Competition Law and the New Economy" at the University of Leicester 2001) 1
[62] ibid. 7
[63] Comp/38.064, IP/01/1155 Covisint Automotive Internet Marketplace
[64] EU Commission, 'Commission Clears the Creation of the Covisint Automotive Internet Marketplace' (Comp/38.064, IP/01/1155 2001) <http://europa.eu/rapid/press-release_IP-01-1155_en.htm?locale=en> last accessed 14 August 2018

same pro- and anti- competitive effects as B2B e-marketplaces do: On one hand, it enhances communication and transparency, improves efficiency, and reduces costs. On the other, it may be exploited to facilitate collusion. As such, it is believed information exchange that is taken place in the context of blockchain networks may not rise competition concerns as long as the Commission is satisfied that the anti-competitive concerns have been eliminated, especially those as set out in *Covisint*.

CHAPTER 4: ANTICOMPETITIVE FORECLOSURE

In this Chapter, we will see how anticompetitive foreclosure can take place in a permissioned blockchain. The first part of this Chapter explores the notion of 'consensus' in the context of blockchain. It will then be followed by a detailed explanation of Consensus Protocols. The final two sections discuss how firms could be effectively excluded in a blockchain network and the applicability of EU competition law.

Consensus in Blockchain

Consensus is the heart of the blockchain technology. The notion of 'consensus' can be understood as a state of agreement on which all or a majority of people agree. The lack of trust inherent in blockchain is particularly relevant to the notion. In a blockchain network, all authorized parties can propose a transaction to be added to the ledger. While parties to permissioned blockchain are in theory more collaborative, the possibility that some may betray their counterparts and disrupt the blockchain operation cannot be precluded. It is therefore necessary for the nodes of a blockchain network to evaluate and agree on the transactions before they are permanently incorporated into the blockchain. As such, the notion of consensus plays a key role in determining whether the blocks store the 'true version' of a group of transactions. Here, it is important to note that the concept of 'truth' as applied to blockchain does not refer to the traditional understanding of the word. It merely means that the nodes are in agreement or consensus that the transaction or event in question has happened. Accordingly, what has been agreed as valid by the nodes does not necessarily mean that it has actually taken place. As long as an agreement is reached among the nodes, a block could be appended to a blockchain. To some extent, this shows the process of adding blocks to a blockchain "may be arbitrary or even controlled by an adversary".[65] In any case, the notion of consensus enables multiple untrusted parties in a blockchain network to directly interact with each other without the presence of a trusted intermediary. Achieving consensus in such a distributed system however is not an easy task. For this purpose, a pre-agreed set of rules, known as 'consensus protocols' in blockchain language, must be designed.

[65] Shehar Bano and others, 'SoK: Consensus in the Age of Blockchain' (arXiv:1711.03936v2 [cs.CR], 2017) 4

Consensus Protocol in Permissioned Blockchain

Currently, there are three main consensus protocols: (a) Proof-of-Work (POW), (b) Proof-of-stake (POS), and (c) Practical Byzantine Fault Tolerance (PBFT). POW and POS are usually used in permissionless blockchain, although it is also possible to employ these protocols in permissioned blockchain. In general, POW and POS require miners to demonstrate some proof before proposing a valid block.[66] Miners in POW protocols must invest resources to find the answer to a computationally difficult puzzle, whereas for POS they must show a 'stake' in the system, such as the number of coins held by the miner. Requiring miners to 'work' in order to gain the right to propose new blocks means a high level of security is ensured as miners who invest resources into updating the blockchain can be seen as demonstrating good faith. However, this would also result in a low transaction speed. For example, the Bitcoin protocol, which adopts POW, automatically adjusts the difficulty of the puzzle.[67] Currently, a new block can be added to the ledger only every ten minutes.[68] This is perhaps not ideal for businesses which prefer instant settlements.

It is more common to find permissioned blockchain employ PBFT protocols rather than POW or POS. Derived from the Byzantine Generals' Problem, PBFT is a solution for distributed computer networks to operate as intended and correctly reach consensus despite the disruption of malicious or failing nodes.[69] PBFT aims to mitigate the negative consequences of these dishonest participants have on the right consensus that is reached by the honest parties. In blockchain context, PBFT protocols allow the signing of a block even when 1/3 of the participants in the network fail or act maliciously.[70] The flip side of the coin however is that, for the protocol to work, the amount of dishonest nodes in the network cannot exceed 1/3 of the overall nodes in the system at any point of time (the 'assumption'). In general, instead of requiring miners to prove or demonstrate something to gain the right of proposing blocks, PBFT protocols usually feature a predefined validator (or 'leader') who is primarily responsible for such task. Accordingly, the leader would perform an initial computation after it receives a message from blockchain users. It would then multicast the result to all other nodes and ask them to confirm whether the result is valid in turn. The leader then awaits $f + 1$ (f = the number of 'dishonest' nodes) replies from different nodes with the same result.[71] Assuming the amount of malicious nodes is less than 1/3 of the overall nodes in the blockchain network, this $f + 1$ replies should be the decision of the honest nodes. After validation, the predetermined validator would then broadcast the decision to the network, so that all nodes can update their local copies of the ledger. As such, comparing to POW and POS protocols, it

[66] Jean Bacon and others (n 10) 15
[67] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009) 3
[68] Jean Bacon and others (n 10) 14
[69] Miguel Castro and Barbara Liskov, 'Practical Byzantine Fault Tolerance' (Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999) 1
[70] Christian Cachin and Marko Vukolić, 'Blockchain Consensus Protocols in the Wild' (IBM Research – Zurich, 2017) 6
[71] Brian Curran, 'What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide' (Blockonomi, 11 May, 2018) <https://blockonomi.com/practical-byzantine-fault-tolerance/> last accessed 14 August 2018

can be said that PBFT protocols are more centralized. This allows higher transaction speed however scarifies the requirement of 'trustless' to some degree. Hence, it is not suitable for permissionless blockchain which typically involve dynamic, large scale of unknown participants.

Moreover, PBFT's centralized nature enables the blockchain to return to the traditional synchronous protocols. In such protocols, nodes would "agree on a total ordering of the accepted blocks by adding agreed blocks one at a time".[72] More specifically, they would "ensure every node has updated its copy of the [blockchain] before moving on to the next block". [73] Contrasting with the asynchronous model typically used by permissionless blockchain, the former is better at ensuring consistency between the copies held by nodes.

Consensus is the backbone of a blockchain. As such, consensus protocols, which manifest how members of a given blockchain intend to reach consensus, is capable of shaping the characteristics of the blockchain. Permissioned blockchain normally employ PBFT protocols and synchronous protocol. This then explains the common features of such blockchain model, which include: (a) few number of participants, (b) static number of participants, (c) operated by known entities, and (d) a level of trust exists among the participants.

Foreclosure in Permissioned Blockchain

It is argued that the use of PBFT protocols may lead to foreclosure risk, which may be manifested in two forms: (a) access refusal, and (b) prioritization.

It is likely that access to a permissioned blockchain will be restricted by members of the blockchain consortia in question. PBFT protocols perform better when there are few nodes and they are known to each other due to its centralized nature. Similarly, synchronous protocols work better where there is only a limited number of nodes.[74] As such, members of a blockchain network that adopt such protocols would want to set up the blockchain in a way that only authorized parties can join and participate in the network. In competition law language, such access which is controlled by existing members of the blockchain consortia is known as gating, and in certain circumstances such conduct may fall foul of EU competition law.

Even if a firm is given authorization to join the network, original members may engage in certain conducts such that the firm is effectively being precluded from using the technology. For example, they may configure the blockchain so that the new entrant only has limited permission to store the blockchain and add new blocks. Moreover, since PBFT protocols require merely 2/3 members come to an agreement for the purpose of signing new blocks

[72] Jean Bacon and others (n 10) 13
[73] ibid.
[74] Some suggested that a few tens of nodes is the maximum; Jean Bacon and others (n 10) 13

instead of unanimous consensus, it would also be possible that a firm's proposed transactions will be rejected by other members without objective cause. As such, while a firm may be granted access to the blockchain network, original members of the network may still constructively refuse certain parties, thereby preventing them from participating in the blockchain network meaningfully. To some extent, these conducts can also be seen as collective boycott.

Foreclosure in permissioned blockchain may also take the form of prioritization. In essence, prioritization can be understood as certain members' transactions are given precedence over the others. The issue of 'prioritization' in blockchain, in some way, resembles the net neutrality debate. The EU described net neutrality as "a non-discrimination principle, requiring that all electronic communication passing through an internet service provider (ISP) network is treated equally".[75] In other words, without net neutrality, ISPs would be free to offer varying levels of connectivity to content providers at different price range. Naturally, a multi-tiered Internet system may emerge, and this would create competition concerns. For example, start-ups that could not afford for the 'best connection' service would have to resort to the 'standard connection' which in turn may lead to poorer accessibility and speed of access to its products.

Similarly, 'prioritization' in a blockchain would create at least a two-tiered system, whereby certain members' transactions would be dealt with more efficiently. In PBFT protocols, it is necessary for a predetermined validator or leader to first verify the proposed transaction before broadcasting the results to other nodes for confirmation. When working in conjunction with the synchronous protocol, this would mean that transactions can only be verified one at a time in order to ensure new blocks would be added to the blockchain in the same logic. As a result, a 'queue' for transactions verification would be formed. Depending on the precise set-up of the blockchain, the leader may be given discretion in determining whether any of such transactions should be given priority. It would then be possible that the leader may work in an unfair or bias way, for example favors corporate affiliations over the others, so that the clearance of transactions of certain members would always go first. Alternatively, certain members of the blockchain network may collude with the leader in order to ensure their transactions are given preferences over the others. In any event, distinguished from the collective boycott situation as discussed in Chapter Two, all transactions in this case would be verified, although some may be processed later than the others. Consequently, members whose transactions are inferior to the others would feel that they are being placed at a competitive disadvantage position.

[75] Tambiama Madiega, 'The EU Rules on Network Neutrality: Key Provisions, Remaining Concerns' (European Parliament Research Service 2015) 1

EU Competition Law Application

Traditionally, anticompetitive foreclosure is dealt with by Art. 102 TFEU. However, it is argued that the provision may be ineffective for blockchain. Competition authorities must therefore seek alternate recourses.

It is clear that the Commission intended to prohibit anticompetitive foreclosures by Art. 102 TFEU.[76] In its Guidance Paper, the Commission described foreclosure as "a situation where effective access of actual or potential competitors to supplies or markets is hampered or eliminated as a result of the conduct of the dominant undertaking".[77] Importantly, EU competition law targets not just 'foreclosure' but 'anticompetitive foreclosure', thus it requires such exclusion of competitors to have "an adverse impact on consumer welfare".[78] Considering the wordings used by the Commission, in particular 'dominant' and 'conduct', it can be said that the definition fits more comfortably with Art. 102 TFEU, which was designed to prohibit unilateral abusive conduct of undertakings in a dominant position. Therefore, for the purpose of establishing anticompetitive foreclosures under Art. 102 TFEU, two elements are crucial: (a) abuse, which in this case would be the anticompetitive foreclosure, and (b) a dominant position. However, it may be problematic to demonstrate the element of 'abuse' in the context of blockchain.

Abuse

The conducts identified in the previous section can be analyzed under a line of EU case law known as "refusal to supply". In general, where a dominant undertaking refuse to supply its products or services or grant access to its facilities it may infringe Art. 102 TFEU. Moreover, the notion of refusal to supply includes constructive refusals, i.e. where the supply, known to the supplier, is unacceptable or unduly delayed.[79] Although EU competition law does not impose a duty to dominant undertakings requiring them to supply products or services to whoever requests them to do so, in certain situations a refusal to supply constitutes an 'abuse'. Of relevance here is the situation of 'essential facility' doctrine.

At its simplest, the concept of 'essential facility' denotes the situation where a competitor needs access to something that is owned or controlled by a dominant undertaking in order to provide products or services to its customers. In *B&I/Sealink*,[80] the very first case that saw the expression 'essential facility' being used, the Commission, after defining 'essential facility' as "a facility or infrastructure without access to which competitors cannot provide services to their customers",[81] stated that where a dominant undertaking refuses its competitors access

[76] Article 102 of the Treaty on the Functioning of the European Union
[77] European Commission, 'Guidance on the Commission's Enforcement Priorities in Applying Art. 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (2009/C 45/02) [19]
[78] ibid.
[79] *Napier Brown/ British Sugar* [1998] OJ L284/41
[80] IV/34.174, Sealink/B&I Holyhead: Interim Measures 11 June 1992
[81] ibid. [41]

to such facility or grants access to them only on less favourable terms "thereby placing the competitors at a competitive disadvantage" infringes Art. 102 TFEU.[82] The principle was then applied in several subsequent cases decided by the Commission. It is argued that, with hindsight, the doctrine was in fact used in even earlier cases. For example, the Commission in *London European/ Sabena* decided that Sabena's refusal to grant London European access to its Saphir system, an online system which "streamlined the procedure of travel agents to consult flight schedules, fares and seat availability of airlines included in the system, and to make reservations", constitutes an abuse of its dominant position in the relevant market.[83] To some extent, the online system in this case is similar to a blockchain network in the sense they are both 'online platforms' in the broadest sense. Thus, it can be argued that the Commission would have no difficulty in concluding a blockchain network is an 'infrastructure' for the purpose of satisfying the 'essential facility' test.

The 'essential facility' doctrine represents a powerful intrusive measure for competition authorities such that it can force dominant undertakings to share its valuable assets or resources where necessary. Unsurprisingly, as it may severely interfere an undertaking's rights, the Court halted the expansion of the doctrine. In *Bronner*, the Court held that access to a facility would be ordered only in very limited circumstances.[84] In particular, such order would only be permitted where the refusal is likely to "eliminate all competition" in the market on the part of the person requesting the service or product and that the access must be "indispensable to carry on that person's business, inasmuch as there is no actual or potential substitute in existence" for it.[85] As such, *Bronner* sets a high hurdle for invoking the 'essential facility' doctrine: the refusal has to be likely to 'eliminate all competition', but not merely leading it 'more challenging' to compete; the access must be 'indispensable', but not merely 'desirable'.

While a blockchain could be regarded as a 'facility' for the purpose of 'essential facility', it is argued it would be difficult to invoke the doctrine as a whole. The following example may provide an illustration. Several European banks, including one major bank, form a blockchain consortia for the purpose of facilitating interbank payments. The traditional way of clearing interbank payments remains available, although in comparison it would be much slower and costly. Accordingly, being a member of the blockchain consortia may be necessary if a bank wants to be competitive in the market in question. If its access to the blockchain is being refused, it appears this constitute an abuse. Here, the blockchain seemingly represents an important facility without access to which the bank may not be able to effectively provide services to its clients. However, according to *Bronner,* the 'essential facility' test may not be satisfied. Having access to the blockchain is merely desirable for the bank but not

[82] ibid.
[83] *London-European/ Sabena* [1988] OJ L317/47
[84] Case C-7/97 *Oscar Bronner GmbH & Co KG v Mediaprint* [1998] ECR I-7791
[85] ibid. [41]

indispensable as the traditional way of settling payments is still available. The fact that the traditional way is much slower and costly does not mean that all competition has been eliminated. On the contrary, it is just more difficult for the bank to compete with its rivals. As such, it is argued that it would be a daunting task for competition authorities to prove a blockchain is an 'essential facility'.

Similar conclusion can be made in relation to the issue of 'prioritization'. The problem of 'prioritization' is also a case of a refusal to supply in the sense that the blockchain is set up in a way that some of its member is denied having access to prioritized services. Slightly different from the scenario of 'access refusal' as discussed above, what is at stake here is the ability to have access to prioritized services. Nonetheless, *Bronner* remains to be applicable: prioritization is not indispensable as there is an alternative method being available, namely non-prioritized transaction verification; the presence and availability of non-prioritized transaction verification means that competition is not eliminated in its entirety. Accordingly, it is almost certain that, under the current law, dominant undertakings are not prohibited from providing prioritized services.

Collective abuse

Even if the element of 'abuse' is seemingly established, it may not amount to an abuse of a collective dominant position. It is settled law that 'one or more undertakings' in Art. 102 TFEU can refer to economically independent undertakings which together hold a 'collective dominant position' in the market, provided that they are "united by […] economic links".[86] The notion of 'economic links' must be understood broadly such that "from an economic point of view they present themselves or act together on a particular market as a collective entity".[87] In other words, the form of 'collaboration' between such undertakings is irrelevant. Rather, as long as they hold themselves out as a collective entity and act together independently of their competitors, the requirement of 'collective dominance' will be satisfied. Given this broad view of the links required to establish a finding of collective dominance, it is argued that the presence of undertakings within the same blockchain network may represent as a plus factor for competition authorities to demonstrate that a collective entity indeed exists. The question is then whether this collective entity holds a dominant position. If this is answered in affirmative, then it would be necessary to consider whether the requirement of 'collective abuse' is satisfied.

Central to the issue of anticompetitive foreclosure in the context of blockchain is that the exclusion is conducted by multiple parties collectively, yet the case law on what amount to abuse by collective dominant entities is underdeveloped. For example, in *TACA* the Court simply held that, on the facts, the Commission failed to demonstrate that the undertakings

[86] Cases T-68, 77, and 78/89, Società Italiano Vetro SpA v Commission [1992] ECR II-1403 [357]

[87] Joined cases C-395 and C-396/96P*, Compagnie Maritime Belge Transports SA and others v. Commission ('Cewal'), [*2000] ECR I- 1365 [36]

could induce potential competitors wishing to enter the market to join the TACA by the measures in question without further explaining the legal rationale behind.[88] It is therefore uncertain whether a collective decision to refuse to supply an undertaking in general would be deemed as an abuse of collective dominance. However, if the 'essential facility' doctrine is successfully invoked, it is possible that refusing to grant access to a blockchain network could amount to abuse. This is because in such scenario, given all competition has been eliminated, it is arguable that the exclusionary conduct engaged by the firms would "hinder the maintenance of the degree of competition existing in the market or growth of that competition", thereby strengthening the collective dominant position.[89] However, as mentioned, it would not be an easy task to invoke the doctrine. Accordingly, it seems questionable whether the concept of abuse, which has been primarily developed in the context of individual dominant firm, is the ideal mechanism for the propose of prohibiting practices that may facilitate or stabilize a collusive strategy engaged by several undertakings in the market.

In any case, it seems difficult to explain a collective decision to refuse to supply to an undertaking without considering the element of collusive behavior. For example in both *Compagnie Maritime Blege* and *TACA* the Commission had found that the parties did engage in some liner conferences before embarking the alleged abusive conducts. Moreover, in proving these cases, the Commission in essence simply recycled the facts of the Art. 101 infringement to demonstrate a violation of Art. 102 TFEU. As such, it is argued that, to a large extent, cases that involve collective abuse overlaps with Art. 101 TFEU. Against this backdrop, it appears that Art. 101 TFEU may be more relevant when it comes to anticompetitive conducts in blockchain context. Indeed, in Chapter Two, the paper showed that the notion of 'agreement' in fact capable of encompassing far more conducts that one thought, including unilateral conduct by one firm to another; in Chapter Three, the paper stated that the notion of 'concerted practice' must be understood broadly, in particular it seems the only way for firms to escape from being scrutinized by competition authorities under the application of concerted practice is to demonstrate that they had decided their future conducts in the market independently. Accordingly, these broad and liberal definitions allow competition authorities to apply Art. 101 TFEU to capture all sort of loosely formalized forms of cooperation. It is therefore argued that Art. 101 TFEU is perhaps the better venue to prove anticompetitive foreclosures in permissioned blockchain.

[88] Cases T-191 and 2120214/98 *Atlantic Container Line v Commission* [2003] ECR II-3275
[89] C-209/10 *Post Danmark I* EU:C:2012:172 [24]

FURTHER RESEARCH

Before moving on to the conclusion, this paper would like to highlight its limitation and recommend an area for further research.

This paper has primarily focused on the *ex post* regulation of blockchain networks. Indeed, competition law is typically regarded as an *ex post* market regulation tool in that competition authorities react only after the emergence of anticompetitive practices. In blockchain context, as can be seen, Art. 101 and potentially Art. 102 TFEU would be invoked after the formation of blockchain network and after anticompetitive conducts are observed. The question is then whether competition authorities would regulate these networks prior to their establishment?

Beyond Art. 101 and 102 TFEU, European Merger Control Regulation (EUMR) may be deemed by the regulators as a useful tool to regulate blockchain network *ex ante.* In general, the current EUMR prohibits 'concentrations' with an EU dimension that would impede effective competition in the internal market or a substantial part of it. In other words, the purpose of EUMR is to prevent changes in market structure that would have a negative impact on the competition landscape in the internal market. As far as the notion of 'concentration' is concerned, it has been widely defined in order to cover mergers, acquisitions of control, and the creation of full-function joint ventures.[90] Of relevance to blockchain is the last point – joint ventures. Art. 3(4) EUMR provides that a joint venture will give rise to a concentration where the following conditions are met: (a) its parent companies reserve joint control on the joint venture, (b) lack of autonomy in the joint venture, and (c) the joint venture is not intended to operate on a lasting basis.[91] As mentioned in the introduction, firms, including market leaders, are now working together for the purpose of developing the blockchain technology for commercial applications. Some blockchain consortium, such as the Digital Trade Chain, have even emerged into joint ventures that operate in the reality. As such, where the joint venture is in essence a sham for the firms to strengthen their dominant positions in the market, it may appear that the EUMR may be applicable in blockchain context, enabling competition authorities to adopt pre-emptive measures on blockchain networks.

However, the application of EUMR in blockchain context may not be as straightforward as first thought. Art. 2(3) EUMR requires that competition authorities to demonstrate that the concentration would "significantly impede effective competition in the common market or in a substantial part of it, in particular as a result of the creation or strengthening of a dominant position".[92] This then entails that competition authorities must make an assessment in the market in question, in particular it must decide what the market in question is and the market power of the firms is involved. Similar assessment has to be done under Art. 102 TFEU and it has been proven that this may be a tricky task. The question is then whether the fact that

[90] Article 3(1) and (4) European Merger Control Regulation
[91] Article 3(4) European Merger Control Regulation
[92] Article 2(3) European Merger Control Regulation

blockchain technology is employed would make this assessment easier or even more difficult. As such, there are a number of gaps in our knowledge around blockchain and merger control and thus it is believed that further research focusing on this area would be beneficial.

CONCLUSION

This paper has examined how firms may exploit the architecture of blockchain in order to participate in certain collusive behavior. Two features of the technology are particularly relevant. First, blockchain as a distributed ledger. Secondly, blockchain' consensus protocols, in particular the PBFT protocol.

In Chapter Two, the implication of the blockchain technology on explicit collusion is discussed. It is suggested that the technology, along with Smart Contracts and Internet of Things, may offer an efficient way to enforce an explicit agreement with an anticompetitive intention, for example cartel agreements. Outside the context of cartels, the paper considered that firms may agree to boycott their competitors collectively via the consensus protocols so that the affected undertakings could not participate in the blockchain network meaningfully. It is argued that these issues should not pose any difficulty for competition authorities as parties to these agreements remain to be the main actors and the blockchain are merely tools for these parties to facilitate their agreements.

In Chapter Three, the paper discussed how firms may share information between themselves on a blockchain. Central here is blockchain' core functionality: distributed ledger. Accordingly, in blockchain, information is exchanged simply when firms store records on the blockchain as these records will be replicated and shared automatically among all members once being put on the network. Under EU competition law, information exchange is usually assessed as concerted practice as, according to one of the inherent competition principles in EU law, firms must formulate their future conduct in the market independently. It is recognized that the law is this area is not settled and currently there is no bright-line rule for reference. As such, while it is argued that EU competition law is largely applicable to the situation, competition authorities or professional advisors may need to take two lines of case law into account, namely the requirement of 'awareness' in relation to information available on various online platforms and B2B e-marketplaces.

Chapter Four focuses on anticompetitive foreclosure. The paper suggested that the notion of 'consensus' is the heart of the blockchain technology, and the way how the firms intended to reach consensuses will be codified into a consensus protocol. In most permissioned blockchain, the protocol that is being commonly used is known as the PBFT protocol, which is a protocol that allows firm to tolerate 1/3 indifferent results. This could be deemed as a loophole such that firms could exploit it to exclude certain members in blockchain network. Traditionally, under EU competition law, anticompetitive foreclosure is a topic that is assessed

under Art. 102 TFEU, which is a provision that has been primarily developed to sanction unilateral conducts performed by individual dominant firms. It is argued that Art. 102 TFEU could not comfortably deal with antitrust issues that arise from permissioned blockchain, a technology that emphasize the notion of 'shared control'. However, collective abuses are inherently creatures of collusive behaviors. Accordingly, this entails that Art. 101 TFEU should be available for tackling the issue of anticompetitive foreclosures, despite this is a topic that is typically assessed under Art. 102 TFEU.

Immediately before this conclusion, this paper has suggested that further research in relation to the relationship between blockchain and competition law could be made in the area of merger control. As firms have acquired more understanding regarding the blockchain technology, it is increasingly popular for firms to form joint venture to put the concept into reality. It therefore appears that there is an imminent need for competition authorities to investigate the applicability of EUMR on blockchain.

Overall, EU competition law, in particular Art. 101 and 102 TFEU, is applicable to blockchain uses. As such, when firms, especially competitors, are sharing a blockchain infrastructure, they must be mindful of the implication of the antitrust rules in this regard. In particular, firms must be careful of what information they are sharing with the other firms and they must not engage in conducts such that other members in the blockchain network are prevented from using the facility.

BIBLIOGRAPHY

Legislation

Art. 101 Treaty on the Functioning of the European Union

Art. 102 Treaty on the Functioning of the European Union

Article 3 European Merger Control Regulation

Article 2 European Merger Control Regulation

Cases

Case 107/82 *AEG-Telefunken v Commission* [1983] ECR 3151

Cases T-191 and 2120214/98 *Atlantic Container Line v Commission* [2003] ECR II-3275

Case T-41/96 *Bayer v Commission* [2000] ECR II-3383

Cases T-25, 26, 30–32, 34–39, 42–46, 48, 50–71, 87, 88, 103, and 104/95, *Cimenteries CBR v Commission* [2000] ECR II-491

Cases C-395 and C-396/96P*, Compagnie Maritime Belge Transports SA and others v. Commission ('Cewal'), [*2000] ECR I- 1365

Case C-74/14 *Eturas UAB v Lietuvos Respublikos konkurencijos taryba* EU:C:2016:42

Cases 48, 49, and 51–57/69, *ICI v Commission* [1972] ECR 619

Case C-7/97 *Oscar Bronner GmbH & Co KG v Mediaprint* [1998] ECR I-7791

Cases C-204, 205, 211, 213, 217, and 219/00 *P, Aalborg Portland AS v Commission* [2004] ECR I-123

C-209/10 *Post Danmark I* EU:C:2012:172

Cases T-68, 77, and 78/89, Società Italiano Vetro SpA v Commission [1992] ECR II-1403

Cases 40-48, 50, 54-56, 111, 113 & 114/73, *Suiker Unie* [1975] ECR 1663

Case T-202/98, T-204/98 & T-207/98 *Tate & Lyle plc v Commission* [2001] ECR II-2035

Case C-8/08 *T-Mobile* [2009] ECR I-4529

Comp/38.064, IP/01/1155 Covisint Automotive Internet Marketplace

London-European/ Sabena [1988] OJ L317/47

Napier Brown/ British Sugar [1998] OJ L284/41

Sealink/B&I Holyhead: Interim Measures 11 June 1992

Case AT. 39861 Yen Interest Rate Derivatives

JJB Sports/ All Sports v Office of Fair Trading [2006] EWCA Civ 1318

Verizon Communications, Inc. v Law Offices of Curtis V. Trinko, 124 S. Ct. (2004)

Books

Smith A., *The Wealth of Nations* (Book IV, Chapter VIII, W.Strahan and T. Cadell 1776)

Jones A. and Sufrin B., *EU Competition Law: Text, Cases, and Materials* (6th edn, OUP 2016)

Journal Articles

Bacon J. and others, 'Blockchain Demystified' [2017] Queen Mary University of London, School of Law, Legal Studies Research Paper No. 268/2017

Bano S. and others, 'SoK: Consensus in the Age of Blockchain' (arXiv:1711.03936v2 [cs.CR], 2017)

Cachin C. and Vukolić M., 'Blockchain Consensus Protocols in the Wild' (IBM Research – Zurich, 2017)
Castro M. and Liskov B., 'Practical Byzantine Fault Tolerance' (Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999)
Christidis K. and Devetsikiotis M., 'Blockchain and Smart Contract for the Internet of Things' (2016) 4 IEEE Access 2292
Ezrachi A. and Stucke M., 'Artifical Intelligence & Collusion: When Computers Inhibit Competition' (2016) 2017(5) University of Illinois Law Review 1776
Harrington J., 'How Do Cartels Operate?' (2006) 2(1) Foundations and Trends in Microeconomics 1
Levenstein M. and Suslow V., 'What Determines Cartel Success?' (2006) 44(1) Journal of Economic Literature 43
Llorens A., 'Horizontal Agreements and Concerted Practices in EC Competition Law: Unlawful and Legitimate Contacts Between Competitors' (2006) 51(4) The Antitrust Bulletin 837

EU Publications

European Commission, 'Guidelines on the Applicability of Article 101 of the Treaty of the Functioning of the European Union to Horizontal Co-operation Agreements' (2011/C 11/01)
European Commission, 'Guidance on the Commission's Enforcement Priorities in Applying Art. 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (2009/C 45/02)
European Commission, 'Guidance on Restrictions of Competition "By Object" for the Purpose of Defining Which Agreements May Benefit from the De Minis Notice' (SWD(2014) 198 final)
EU Commission, 'Commission Clears the Creation of the Covisint Automotive Internet Marketplace' (Comp/38.064, IP/01/1155 2001) <http://europa.eu/rapid/press-release_IP-01-1155_en.htm?locale=en> last accessed 14 August 2018
European Parliamentary Research Service, *How Blockchain Technology Could Change Our Lives* (Science and Technology Options Assessment 2017)
Tambiama Madiega, 'The EU Rules on Network Neutrality: Key Provisions, Remaining Concerns' (European Parliament Research Service 2015) 1

Articles

Deloitte University Press 'Banding Together for Blockchain: Does It Make Sense for Your Company to Joint a Consortium?' (Deloitte University Press 2017)
Joachim Lücking, 'B2B E-Marketplaces: A New Challenge to Existing Competition Law Rules?' (Paper Presented at the Conference "Competition Law and the New Economy" at the University of Leicester 2001)

KBC Group, 'KBC and Cegeka Trial Ground-Breaking Blockchain Application for SMEs' (KBC Group, 12 July 2016) <https://newsroom.kbc.com/kbc-and-cegeka-trial-ground-breaking-blockchain-application-for-smes> last accessed 14 August 2018
KBC Group, 'Digital Trade Chain Consortium Launches we.trade, Announces Joint Venture and Welcomes Santander' (KBC Group, 17 October 2017) <https://newsroom.kbc.com/digital-trade-chain-consortium-launches-wetrade-announces-joint-venture-and-welcomes-santander> last accessed 14 August 2018
Kiran Desai, 'Blockchain and Competition Law' (Law Alert, Ernst & Young LLP 2018)
Organization for Economic Co-operation and Development, 'Roundtable on Information Exchanges Between Competitors Under Competition Law' (DAF/COMP/WD(2010)118
Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009)

Websites and Blogs

Amazon Web Services (AWS), 'Cloud Storage' (AWS, 2018) <https://aws.amazon.com/what-is-cloud-storage/> last accessed 14 August 2018
Curran B., 'What is Practical Byzantine Fault Tolerance? Complete Beginner's Guide' (Blockonomi, 11 May, 2018) <https://blockonomi.com/practical-byzantine-fault-tolerance/> last accessed 14 August 2018
Gopinath R., 'Checking the Ledger: Permissioned v.s. Permissionless Blockchain' (IBM, 28 July 2016) <https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-blockchain/> last accessed 14 August 2018
Rouse M., 'Internet of Things (IOT)' (IOT Agenda, June 2018) <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT> last accessed 14 August 2018
Szabo N., 'The Idea of Smart Contracts' (Nick Szabo, 1994) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> last accessed 14 August 2018
Wood J, 'Blockchain of Things – Cool Things Happen When IOT & Distributed Ledger Tech Collide' (Medium, 20 April 2018) <https://medium.com/trivial-co/blockchain-of-things-cool-things-happen-when-iot-distributed-ledger-tech-collide-3784dc62cc7b> last accessed 14 August 2018

Newspaper Articles

BBC, 'Bitcoin falls below $6,000' (BBC News, 6 February 2018) <https://www.bbc.co.uk/news/technology-42958325> last accessed 14 August 2018