Antitrust by Design - The prohibition of anti-competitive coordination and the consensus mechanism of the blockchain

Sebastian Louven[*] & David Saive[**]

Carl von Ossietzky University Oldenburg

ZRI Working Paper

Is the blockchain technology with its technical coordination mechanisms also posing new challenges to antitrust dogma? Are conventional principles transferable to platforms or do we need new approaches? This paper examines the applicability of the prohibition of concerted practises to blockchain issues and which requirements arise for a compliance-conscious design of new technologies.

I. Introduction

In the meantime, the Blockchain technology has arrived at the centre of the legal discussion. The focus of the legal analyses is primarily on the irreversibility of the database and the consequences for the users arising from that. From the perspective of competition law, however, another aspect of the technology is of much greater relevance, the so-called consensus mechanism of the blockchain.[1] New information is only added to the database if the majority of network participants, the 'nodes' agree to. In this respect, therefore, there is coordination between the parties involved. The following article examines whether and to what extent this voting behaviour is contrary to the prohibition of anti-competitive measures within the meaning of Art. 101 TFEU and shows which measures can be taken by design to make the blockchain compliant with competition law.

II. Legal background

1. Prohibition of anti-competitive concerted practices

Article 101(1) of the TFEU prohibits agreements, decisions and concerted practises which may restrict interstate trade and which restrict or intend to restrict competition within the internal market. In relation to the prohibition of abuse of a dominant position pursuant to Art. 102 TFEU and to the unilateral anti-competitive measures mainly covered by these measures, it is crucial that it involves restrictive collusion on the part of several companies involved. Section 1 German law against restraints of competition (GWB) provides for a similar regulation under German antitrust law. If collusive measures have the object of restricting competition, they are inadmissible per se. If the restriction of competition is not the object but merely the effect and if the parties' market share does not exceed 10%, the measure is considered to be of no concern. [2]

2. Exchange of information

Some typical cases of restrictions of competition are already listed in Article 101(1) TFEU. However, these are not final. Rather, various other case groups have emerged in antitrust practice. This includes

---

[*] Competition & Antitrust Lawyer; Research Associate at Carl von Ossietzky University Oldenburg; Research Fellow at the Interdisciplinary Centre for Law of the Information Society (CLI); Editorial board member at Telemedicus.

[**] Legal Scientist and Research Associate at Carl von Ossietzky University Oldenburg; Research Fellow at the Interdisciplinary Centre for Law of the Information Society (CLI).

[1] See also Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox* (forthcoming), (Jun. 11, 2018),https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576.

[2] Commission, Notice on agreements of minor importance which do not appreciably restrict competition under Article 101(1) of the Treaty on the Functioning of the European Union (De Minimis Notice), 8.

the anticompetitive exchange of information via so-called market information systems. [3] In this context, the parties do not directly impose so-called hardcore restrictions, such as price agreements, territorial or import restrictions. Instead, information is exchanged that would otherwise have remained undisclosed to the participating companies or the public. In some cases, public disclosure or selective disclosure of certain information may have a positive effect. For example, information that is aggregated in an objective way could contribute to greater price transparency so that customers can make more informed decisions, thus reducing search costs. Likewise, stakeholders and competitors can make their products and services compatible or interoperable, which could reduce switching costs.

On the other hand, however, disadvantages can also arise from the exchange of information. If competitors have information on the behaviour of other companies that has remained undisclosed to them so far, they could possibly anticipate other companies' strategic decisions. This could lead to conclusions about future pricing or sales strategies such as areas or production volumes. The company obtaining the information would thus be able to adjust its own behaviour with foresight by reacting to the expected price-strategic behaviour of a competitor with its own price adjustment or by adjusting its sales strategy accordingly. The Commission has already stated in its horizontal guidelines that companies cannot be denied the opportunity to adapt themselves '*intelligently*' to the existing or anticipated conduct of their competitors.[4] Furthermore, according to the special requirements of independence it does strictly preclude any direct or indirect contact between them to the extent that companies do so on their own initiative and on their own responsibility.[5]In any case, this prohibits companies from receiving market-strategic information as a result of an additional trust that is no longer justified in terms of competition. Against the background of recent technological developments and the associated better and faster possibilities for exchanging information, the first question that arises is to what extent the ban on collusive contact and the ban on anti-competitive confidence can be complied with. This applies in particular to technologies whose actual purpose is to improve trust.[6]

3. Allocation to platform participants

The prohibition laid down in Art. 101 (1) TFEU does not require any explicit agreement or even a legal or similar agreement. Instead, coordinated behaviour can be covered under the aspects mentioned above. This means that the existence of an anticompetitive and prohibited collision does not depend on an explicit or otherwise consistent act of will by the companies involved. Rather, mere participation in an inadmissible information exchange system can lead to the company's own liability. This applies in particular if information is not exchanged bilaterally, but centrally via a platform infrastructure.[7] This is similar to the hub-and-spoke constellation already developed for price coordination.[8]The platform (hub) is able to coordinate their behaviour due to its star-shaped agreements or other connections to

---

3 DANIEL ZIMMER, WETTBEWERBSRECHT, Art. 101 AEUV, 265 (Ulrich Immenga & Ernst-Joachim Mestmäcker ed., 5th ed. 2012).

4 Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 61.

5 VOLKER EMMERICH, WETTBEWERBSRECHT, Art. 101 AEUV, 87 ff. (Ulrich Immenga & Ernst-Joachim Mestmäcker ed., 5th ed. 2012).

6 See also Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox* (forthcoming), 8, (Jun. 11, 2018),https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576.

7 Eturas, ECJ C‑74/14 (ECLI:EU:C:2016:42, 2015).

8 Johannes Ylinen, *Digital Pricing und Kartellrecht*, NZKART 19, 19 ff. (2018); CHRISTIAN EWALD, HANDBUCH DES KARTELLRECHTS, § 7, Rn. 110 (Gerhard Wiedemann ed.3rd ed. 2016); Kim Manuel Künstner & Benjamin Franz, *Preisalgorithmen und Dynamic Pricing: Eine neue Kategorie kartellrechtswidriger Abstimmungen?*, K&R 688, 688 ff. (2018), Daniel Dohrn & Linda Huck, *Der Algorithmus als „Kartellgehilfe" – Kartellrechtliche Compliance im Zeitalter der Digitalisierung*, DB 173, 173 (2018); Jan-Frederick Göhsl, *Algorithm Pricing and Article 101 TFEU*, WUW 121, 121 ff (2018).

its participants (spoke). The anti-competitive coordination is therefore controlled centrally by an intermediary, although this intermediary coordinator is not mandatory. It is also possible, that a technical infrastructure itself maintains the coordination, which may lead to an abstract coordination of the parties involved.

This anti-competitive coordination system can also be attributed to the participating companies, as the ECJ recently demonstrated in its Eturas ruling.[9] In this case a booking platform had only allowed a certain discount amount by default in an update. Companies that had offered their services via this platform could initially only offer a discount of up to a specific per cent of the total price. On the one hand, the platform company thus restricted the pricing freedom of the companies involved in the vertical relationship. On the other hand, the star-shaped connections to its platform participants caused a price collusion on a horizontal level, which meant that only a limited range of discounts could be used. The other companies were technically able to circumvent this default setting. In the antitrust fine proceedings initiated as a result of this procedure, the responsible antitrust authority assumed that the participants were also liable if they accepted the discount default. This could also be done tacitly, which is why active resistance or a complaint to invalidate the official accusation would have been necessary. The ECJ agreed to this ruling.

4. Use of technology coordination

Another critical anti-competitive coordination situation may be that the companies involved agree on the use of a certain technology by participating in it, thus excluding or displacing competing technologies from the market. However, a vote on the use or specifications of a particular technology can in turn be unobjectionable from a competitive point of view under a rule of reason point if this vote is an expression of well-functioning competition. On the one hand, this can be at the purpose level if standardization or norming leads to significant improvements in the product or distribution channels. With blockchain technology, this could be the exclusion of intermediaries with corresponding commissions, advertising revenues or shares. Secondly, the Commission considers that standardising or normative voting in an open and transparent voting procedure does not raise competition concerns and that any interested party has access to this procedure.

III. Distributed systems and information exchange

However, the technical developments exceed the hub-and-spoke concept. The current discussion focuses on distributed network structures, most of which do not require a central instance. The aim of increasing decentralisation is to avoid intermediaries whose purpose is to establish confidence in the authenticity and integrity of the process in question. It is questionable how the exchange of information within such networks should be handled when it is necessary, particularly for the operation of the network, that an active exchange of information of all parties involved must take place.

1. Technical Background

a) Distributed systems

First of all, the term "distributed systems" needs to be examined in more detail. Distributed systems are network structures consisting of several individual components on different computers in order to pursue a common goal.[10] This can lead to the fact that the users of such networks acting completely without a central instance are both clients and servers. This means, on the one hand, that each user is

9 Eturas, ECJ C‑74/14, 42 ff. (ECLI:EU:C:2016:42, 2015).

10 ALEXANDER SCHILL & THOMAS SPRINGER, VERTEILTE SYSTEME, S. 4 (2012).

the owner of an image of the entire database and, on the other hand, that the communication between the users takes place directly. This is comparable to a P2P structure, in which communication or information exchange takes place directly between the individual participants. With a structure based on a P2P network, deployment can still be done from a central server.[11] Depending on the design of a distributed system within an increasingly decentralized operation, the intermediate instance e.g. agents or the platforms can be omitted.

b) Special case of blockchain technology

The blockchain technology is also a distributed system. The individual users, so-called nodes, also play a multiple role in the network and are both client and server.[12] The special feature in comparison to the general concept of distributed systems is that each individual node is also the owner of a complete image of the database stored inside the network, which is constantly updated. In addition, the nodes are responsible for the validation and inclusion of new information in the database. This is the quintessence of blockchain technology. New information is only added with the consent of the majority of nodes. Thereby trust in the integrity and authenticity of the database is established through a consensus mechanism, also called algorithm.[13] There is no longer a need for a central authority to monitor the validity of the information. Data that contradicts existing information in the data set is rejected by the nodes and cannot become part of the blockchain memory.

In addition, the use of asymmetric encryption ensures the authenticity of the nodes. Each node receives a pair of private and public key. The public key serves as a publicly visible address to which information can be sent. The information can only be decrypted with the associated private key. In addition, the sender of information can sign it with his private key and thus make his sender status visible to the outside world. The private key must be kept secret by the owner, similar to a password.

The term "blockchain" is derived from the concept of the storage process. The complex validation process, the so-called proof-of-work procedure, is not carried out for each individual piece of information. Rather, several individual information is combined in one block. Once the preset maximum amount of storable information has been reached, it is invariably entered into the database by a complicated cryptographic process, the actual proof of work. Each block contains a summary of the information of its predecessor. This creates, as in a knitting pattern, the interlinking of the blocks. Trust is thus strengthened through technical entanglement.

The irreversibility of the database results from the fact that the proof of work described above must be carried out every time the information stored within a block is changed. If the information of a block changes, this affects the immediate successor block in the chain, so that the proof of work must also be resolved again for the successor. In order to stick to the example of the knitting pattern, stitch by stitch must first be opened until one reaches the point where a correction or change must be made in order to close the loosened stitches again by the proof of work.[14]

The proof-of-work process though has a crucial weakness. If a node can combine more than 50% of the total network computing power, it can decide on its own whether to accept or reject it, the so-called 51% attack.[15] In addition, the associated electricity costs are enormous, which is why

---

11 JOCHEN DINGER, DAS POTENTIAL VON PEER-TO-PEER-NETZEN UND SYSTEMEN, 18 (2009).

12 David Saive, *Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG*, CR 186, 187 (2018).

13 It should be clear, however, that algorithms are neither something evidently new nor do they “replace people and their decisions" as partially assumed. Algorithms can also be represented by company-internal processes, and computer programs as well.

14 DANIEL DRESCHER, BLOCKCHAIN BASICS, 123 (2017).

15 ELFRIEDE SIXT, BITCOINS UND ANDERE TRANSAKTIONSSYSTEME, 105 (2017).

alternatives have been sought for some time. With the so-called proof of stake, it is no longer only the computing power that decides whether information is recorded or not. Rather, it depends - simplified - on the number of shares that a node holds in the network.[16] This eliminates the time-consuming calculation of the proof of work.

2. Platform coordination and blockchain

In order to approach the antitrust challenges of blockchain technology, a distinction must be made between the various forms of blockchain-based networks. The main difference in the technical design of blockchain networks is whether the number of participants is unlimited or whether only a certain group of users can join the network.[17] If only certain persons are entitled to use it according to predetermined criteria, which are coordinated and controlled by an authority, this is referred to as a private blockchain. The Public Blockchain, on the other hand, is open to an indefinite number of users in advance.

a) Platform coordination with central authority

With the first type of blockchain, the so-called private blockchain, access to the network is thus limited from the outset. A central instance decides which node may become part of the network. In the antitrust analysis, a distinction can therefore be made between the central instance and the respective nodes. For this constellation, the principles developed as part of the hub-and-spoke constellation and the previous approaches to coordination via platforms can be applied to the central instance.[18] Because this occurs similar to the operator of a platform by coordinating the fate of the blockchain and its users. Coordination is only executed at a different technical level. As with a platform, the central body is responsible for concrete coordination. Obviously, this role is played by companies that use blockchain technology and integrate it into their business.

However, this central instance does not have to be a node of the network itself. Rather, the organisational power of the Private Blockchain is already sufficient. Anyways, coordination by several operators is not excluded. In fact, being central instance or node is neither technically nor legally exclusive. This means that each instance can also be a node at the same time. If a node becomes overweight, it could coordinate in fact.

The so-called Genesis block, i.e. the first block of a blockchain-network, can also play a special role.[19] If the creator of the Genesis block is not the operator, but only the initiator of a subsequently released blockchain, he can nevertheless set the essential impulses for the subsequent coordination. It may therefore also be responsible for the vote based on its initiative, in accordance with traditional principles.

b) Abstract platform coordination through consensus mechanisms

In the other case, the so-called public blockchains, there is no centralized restriction mechanism that excludes user groups from the outset. The most famous application of the blockchain, the Bitcoin network, is based on this principle. Open design and free access to the network are necessary

---

16 Vitalik Buterin, *What Proof of Stake Is And Why It Matters*, BITCOIN MAGAZINE (Aug. 26, 2013, 11.37 AM), https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/.

17 David Saive, *Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG,* CR 186, 187 (2018).

18 Kim Manuel Künstner & Benjamin Franz, *Preisalgorithmen und Dynamic Pricing: Eine neue Kategorie kartellrechtswidriger Abstimmungen?*, K&R 688, 691 (2018); Jan-Frederick Göhsl, *Algorithm Pricing and Article 101 TFEU*, WUW 121, 121 (2018); Daniel Dohrn & Linda Huck, *Der Algorithmus als „Kartellgehilfe" – Kartellrechtliche Compliance im Zeitalter der Digitalisierung*, DB 173 (2018).

19 CHRIS DANNEN, INTRODUCING ETHEREUM AND SOLIDITY, 55 (2017).

prerequisites for alternative monetary systems. Only if as many users as possible can join the network the virtual "currency" may become established as alternative means of payment.

On the other hand, the nodes are only coordinated by the previously defined algorithm, which determines which syntactic requirements an information must fulfil and which requirements are placed on the validation of new information. This technically determined algorithm forms a consensus mechanism which, on the one hand, makes coordination possible in the first place and, on the other hand, provides information to the nodes involved. This means that coordination is not carried out by a central body in the form of at least identifiable companies. Instead, the central instance is abstracted by the algorithm. Coordination therefore does not take place directly through deliberate actions of the participating companies, but indirectly through the logical level of the blockchain. If coordination and associated exchange of information are to be seen as a closer contact, the established principles of the ban on cooperation can be applied. The "intelligent" technology is just as irrelevant as the externally responsible coordination behaviour of the co-ordinators.

IV. Impact

1. Reversal of processing transactions contrary to antitrust law

Companies that violate the prohibition of concerted practices may be required by the authorities or the courts to eliminate them. It would be difficult to reconcile with the objective of antitrust law if legally inadmissible transactions could not be fundamentally reversed. However, the strong technical interdependence of the parties involved in a blockchain and its associated irreversibility seems to make a reversal difficult or even impossible without jeopardizing the existence of the entire system and the associated legally harmless business models or without affecting those not involved in the vote.

The first principles can be derived from the Eturas ruling of the European Court of Justice. In the specific submission procedure, the mere use of the distribution platform should continue to be permissible for the participating companies if they either did not accept the specified antitrust measures, deliberately violated them or filed a complaint with the competent authority.[20] For price-related specifications, it can therefore be assumed that active disagreement is necessary instead of passive acceptance. This is problematic in the case of coordination on the basis of information that has merely been exchanged, since there will not be any option to not accept or just violate the information transfer.

a) Reversal information from the original consignor

On the one hand, the original sender of information could use a reversion information to name the previously entered information as no longer current. In the case of transaction-based information, such as in the bitcoin network, this would mean that the sender would re-execute the same transaction by changing the now legitimate recipient.[21] Only the owner of the corresponding private key can carry out the reversion transaction.

Firstly, this procedure is problematic if the unlawfulness of the transaction was only determined after some time. In these cases, the validation will have been carried out a long time ago. A simple reverse information would no longer be sufficient to resolve possible further entanglements within the blockchain. Instead, all blocks calculated since the relevant information has been stored within the database would have to be rewound via reverse information. This would be accompanied by the second objection to this approach. Both a cartel injunction and a removal order would have to be addressed to a specific addressee on the one hand and be enforceable by him on the other. This would

---

20 Eturas, ECJ C‑74/14, 46 ff. (ECLI:EU:C:2016:42, 2015).

21 David Saive, *Blockchain in der Transportwirtschaft*, RDTW 85, 88 (2018).

probably also be possible with simple reverse information. However, an enterprise could not comply with the obligation imposed on it to dissolve all blocks, including other blocks, with the information contained therein. Otherwise this would result in an obligation affecting all nodes. If a node is not involved in an anticompetitive vote, but only in the technical calculation processes, its antitrust responsibility is lacking and it cannot be obliged to eliminate or refrain from doing so for legal reasons. Despite the technical involvement and ownership of the data stored in the blockchain, their use would be inadmissible due to a lack of participation in the anticompetitive collusion. In the case of advanced technical involvement, it would also depend on those involved only technically. Therefore complete reverse information cannot be enforced on the sender, since it is not possible for him alone to re-execute the transaction. This action would be inadmissible as a violation of the principle of ultra posse nemo obligatur.

b) Reversal information by the information recipient

In addition, the recipient can carry out the reversion information if he wants to relieve himself of the accusation of unauthorized contact in accordance with the principles mentioned above. The sender would either have to send the same information back to the sender with opposite signs. This would be acceptable in a price-related agreement if the information contained the rejection of the vote. According to the principles of the Eturas jurisprudence, even contradiction information would therefore be sufficient. However, this would be problematic in the case of votes that allow an anticompetitive contact to be expressed, since this could already lead to a collusion that could not easily be contradicted. Moreover, the objection of permissible parallel behaviour within the framework of the application of blockchain technology would no longer be possible, since a coordination would always have to be assumed. If a company distances itself according to the principles of the Eturas decision "outside" the blockchain, for example in the context of a complaint to the competition authority or by a general notice of objection to the other voting participants, this must not contradict its conduct "in" the block chain.

c) Disclosure of information

All approaches at the same time, however, do not delete the information completely in any of the cases. It is still stored by the nodes. Through the reversion of the illegal information, it can only be withdrawn from the network-inherent disclosure. This would in any case comply with the requirements of antitrust law in order to avoid an anticompetitive vote. Both the injunction ordered by the authorities and the court would relate exclusively to the elimination of the anticompetitive agreement. In doing so, the principle of effectiveness and the principle of proportionality must be observed. On the one hand, a cancellation order could be issued by companies not participating in the competitive vote. On the other hand, a deletion order would affect the integrity of the blockchain as such, since in the meantime firmly entangled data would have to be dissolved. Since the only decisive factor is the elimination of anti-competitive coordination, it is therefore not the existence of information that counts, but the exchange of information as such, which must be prevented. Thus, a technical procedure would be sufficient, in which data is exchanged within the block chain, but which cannot be read by the individual nodes without objective justification. Objective justifications could exist if the information necessarily has to be exchanged in the course of concrete contract negotiations or implementation. Similarly, security-related aspects could play a role or competition-immanent qualitative aspects could be exchanged. This can also apply to system-relevant data of the blockchain itself, without which the entire network could no longer be operated.

d) Modification of the blockchain during operation

Alternatively, the anti-competitive exchange process as such could be dispensed with by changing the procedure. The basic concept of the blockchain requires that the underlying algorithm be defined in advance. This is the basis for all further information added and the authentication and validation process of new information. If the algorithm is to be changed, all nodes must again be convinced to use it. If only a part of the nodes can decide to change, the blockchain splits at this point. This process is often referred to as forking of the network.[22] There are now two independent blockchain networks, one based on the old algorithm and one on the new algorithm. This could be done by means of a concerted appeal in accordance with the principles of the Eturas decision. As a result, the companies involved could continue to use the technology without fundamentally abandoning it and without incurring liability. However, this will result in a loss of comfort due to the splitting of the network.

2. Prophylactic prevention

The above-mentioned reverse transaction situations relate to infringements already committed. In the context of compliance-conscious and thus also antitrust law-compliant conduct, companies are required to avoid antitrust violations in the first place, i.e. to prevent any situation that may have to be reversed. This is further strengthened by the fact that the blockchain technology can withstand documentation. On the other hand, it is important to prevent a contact of mutual trust between the companies involved, which would lead to an unjustified competitive trust due to the information provided by means of a blockchain technology. Further difficulties arise in the enforcement of antitrust law by the authorities, as there are no plans to seek approval under European antitrust law.

a) Conditions for exemption

In addition to the measures already mentioned above, which are inherent in competition and therefore permitted, measures restricting competition may be exempted under the conditions of Art. 101 (3) TFEU if there are efficiency advantages and consumers are adequately involved. First, this can be done by way of individual exemption, whereby the companies concerned are faced with a higher burden of proof and justification with the associated risks of misinterpretation. Second, according to the conditions for exemption, abstract-typed rules have been established for certain sectors in corresponding block exemption regulations (BERs), but these only apply below certain market share thresholds. Nevertheless, they do provide a certain degree of security for the companies involved. In particular, it is important to avoid the so-called hardcore restrictions, for which there is no exemption effect.

The different possible coordination measures for the use of blockchain technologies should not easily fall within the scope of a specific block exemption regulation. Unless the subject matter scope of special regulations such as the technology transfer BER or the specialisation BER is touched, the acceptance of a vertical agreement within the meaning of Art. 1 para. 1 lit. a Vertical BER, which could be exempted below the relevant market share and turnover thresholds, is usually obvious in conventional platform situations and the conditions of their offer. This constellation can basically be applied to private blockchain constellations, i.e. if a company uses a blockchain platform as a means of distribution and regulates the structure of this distribution relationship with its users. But this does not apply on Public Blockchains. It is true that many companies will have different levels of distribution in relation to each other, so that specific areas of application of vertical BERs will be touched in the respective proportions. For the purposes of these specific distribution agreements or similar measures, the companies are also at another level of the production and distribution chain within the meaning of Article 1(1) vertical BER. This is not the case with regard to the coordination on the use of the blockchain technology, as all users stand at the same level for these purposes. This should also apply

[22] ELFRIEDE SIXT, BITCOINS UND ANDERE TRANSAKTIONSSYSTEME, 10 (2017).

to the dual function of the users as node and client, especially if verifications are triggered via the blockchain-immanent consensus mechanism, since this only serves as a vehicle.

b) Remedies and commitments

From a technical perspective, it is important to avoid the discovery of information stored within the blockchain network that is not or no longer justified in terms of competition from the outset. It is therefore important that information is not disclosed in relation to anticompetitive voting among themselves, but only if there is a legitimate, non-competitive or immanent objective interest. This legitimate interest could be codified in the blockchain and verified in accordance with the existing requirements. Using the example of contract implementation, the specific companies involved should have access to the information, so that disclosure would be permitted. It would also be the disclosure of safety-sensitive or standard-setting information.[23] If such a justified interest cannot be proven, disclosure would be refused on technical grounds. The verification function of the blockchain technology would thus not be used to create trust that raises competition concerns, but would instead serve as a function of trust, precisely to prevent it.

The first person affected by these challenges under competition law can therefore be the developer of the underlying algorithm. Although the developer of the blockchain is now in the focus of the competition law consideration, he cannot be held liable for his pure programming behaviour if he does not decide on the later use in the sense of a coordination.

The main practical burden is therefore borne by the users of the respective technology. To avoid this, they must check for themselves that the algorithm complies with competition law. If necessary, they must refrain from participating in the blockchain, ask the developer to make improvements or resist the vote inside and outside the blockchain according to the principles of the Eturas decision. To avoid process disturbances and since a change of the algorithm during operation would be difficult to implement, influencing the blockchain developer would therefore be most promising. However, contradiction or concealment mechanisms could also be programmed in the respective blockchain technology as an internalized compliance mechanism. This would allow the participating companies to continue to use the distribution channel, which initially poses no competition concerns, without participating in anti-competitive measures.

c) Chameleon Hashes

A possible technical solution can be found by adding a second hash function to the blockchain-algorithm, which also relies on a public-private-key-architecture. These so-called *chameleon hashes* form a trapdoor to the information stored inside the blocks.[24] This makes the alteration of stored information possible and creates a *redactable blockchain*. The name *chameleon hash* derives from the fact, that the hash function looks always the same, regardless of the information stored. Even if an information has been modified or deleted, the hash of the whole block remains unchanged, because the initial hash function to create a new block, always calculates with the same amount of the chameleon hash. The holder of the private key is now able, to change the content stored inside a blockchain, without the recalculating of all block hashes. If there is only one holder of the private key, one of the main merits of a blockchain, its irreversibility and consensus-based algorithm is destroyed. The holder of the private key can change the information without the consent of all other nodes, like a conventional platform. Therefore, the private key to the chameleon hash shall be distributed among

---

23 Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, 300 ff.

24 See for the whole paragraph: GUISEPPE ATANIESE, REDACTABLE BLOCKCHAIN OR REWRITING HISTORY IN BITCOIN AD FRIENDS , 8 ff. (2017).

all or at least a few designated nodes inside the network. They, in turn, need to decide via consensus, if information shall be modified or deleted. To create trust and transparency, the alteration of an information should be flagged, that all other nodes can track the changes. In this case, the voting is simply transferred to another function. The real problem, the risk of anti-competitive coordination via a consensus algorithm, cannot be avoided by this. Admittedly, this function can secure a blockchain-internal legitimate interest in a transaction.

d) Regulatory leeway

Basically, the competition authorities have legal powers to prohibit anti-competitive measures. Since the enforcement of any prohibition orders could be partially inadmissible for the reasons mentioned above, the question of effective antitrust enforcement also arises here. After all, prophylactic prevention of blockchain-based anti-competitive coordination by the competition authorities amounts to ex ante regulation, which is basically unfamiliar to European antitrust law. Although the antitrust law merger control contains a perspective to take prior to the measure in question on the basis of its prognostic assessment of the merger. However, this also refers to the effects to be expected after the merger and is limited after the clearance decision to a repressive control of possible remedial measures. Instead, entrepreneurial actions are not subject to approval.

The above-mentioned block exemption regulations could provide legal certainty against the intervention of the competition authorities. Secondly, by means of public communications, the authorities could commit themselves in the exercise of their margin of judgement and discretion powers and show companies the possibilities under which conditions their behaviour in connection with blockchain technologies would be unobjectionable under antitrust law. Below the instrument of the exemption there is the possibility of a determination in accordance with Art. 5 para. 2 Regulation 1/2003 relating to individual cases that, subject to new findings, there is no reason for action by the authorities. Section 32c sentence 1 German law against restraints of competition (GWB) contains a corresponding declaratory provision for German antitrust law.

V. Summary and Outlook

The ban on concerted practices under antitrust law can be applied without further ado to blockchain situations. Traditional attribution concepts can be used for anticompetitive information exchange. As far as a current blockchain technology enables an extensive contact among the participating companies by means of its consensus mechanism, this is associated with a high risk, which can be countered by a compliance-sensitive design of the respective blockchain technology. This can also eliminate possible risks in the enforcement of official or judicial prohibition orders that could otherwise affect the entire operation of a blockchain. Just as the consensus mechanism can encourage a feeling, it could prevent it if it is properly designed.