International Journal of Law and Information Technology, 2019, 27, 292–305
doi: 10.1093/ijlit/eaz009
Article

OXFORD

Does regulation of illegal content need reconsideration in light of blockchains?

Maurice Schellekens*

ABSTRACT

Blockchains are increasingly being used for content distribution, sometimes as an unwanted side effect of blockchain applications that have other primary purposes, sometimes as intended content distribution. The typical characteristics of a blockchain such as its claimed immutability raise new questions as to what preventive measures can reasonably be demanded from blockchain intermediaries, and managers of nodes in particular. The article asks whether the exemptions introduced in the Directive on e-Commerce can be applied, what mitigating or preventive measures other than Notice-and-Takedown can be applied and how governmental regulators should react.

KEYWORDS: blockchain, content distribution, liability, preventive measures, EU, Directive on e-Commerce

INTRODUCTION

Amongst their many uses, blockchains can be used to distribute content. Some blockchain applications are set up to distribute content, such as SteemIt.[1] In other blockchain applications such as bitcoin, arbitrary content can be added to transactions even though the distribution of content is not their primary purpose.[2] Where content is distributed, illegal content distribution lures. Blockchain applications are already to some extent used to distribute illegal content.[3]

Combatting illegal content involves intermediaries, such as those that host illegal content on their servers. They are in a unique position to help enforcement initiatives. The European Union (EU) Directive on electronic commerce stimulates such

* Senior researcher at the Tilburg Institute of Law, Technology, and Society, Tilburg University. E-mail: m.h.m.schellekens@tilburguniversity.edu.

1 See Introduction in J Kishigami and others, 'The Blockchain-based Digital Content Distribution System' <https://www.researchgate.net/publication/308861913_The_Blockchain-Based_Digital_Content_Distribution_System> accessed 21 March 2019.

2 See Introduction in R Matzutt and others, 'A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin', in *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC)* (Springer 2018); T Claburn, 'Bitcoin's Blockchain: Potentially a Hazardous Waste Dump of Child Abuse, Malware, etc.' Boffins warn of legal risks from arbitrary data distribution (*The Register*, San Francisco, 19 March 2018) <https://www.theregister.co.uk/2018/03/19/ability_to_dump_illegal_content_in_bitcoins_blockchain_puts_participants_in_peril/> accessed 20 August 2019.

3 Matzutt, ibid, s 4.2.

help by giving a conditional exemption from liability to hosting intermediaries.[4] The exemption is premised on the idea that hosting providers take notified illegal content down and leave the door open for further potential preventive measures.

The benefit of blockchain is said to be its immutability. Once data are placed on a blockchain, they can never be removed or changed, not even by the node administrators that host the data. So it looks like tried and tested Notice-and-Take-Down (NTD) systems cannot be applied in a blockchain context.

Does this mean that those victimized by illegal content on a blockchain have to forego help from blockchain intermediaries? Does it mean that node administrators have to do without the exemption from liability? Are there other measures that can (and should?) be taken? This article will examine these questions.

In doing so, it focuses on illegal content such as copyright infringement, child pornography and terrorist content. A common denominator of these forms of illegal content is that the availability of such content cannot be remedied by adding a rectification: the information must be deleted or made inaccessible. This article does not address personal data, the continued storage of which may, for example, become illegal under the principle of data minimization or the right to be forgotten.

The next section explains relevant terms of blockchain technology. The section 'Responsibilities of Internet intermediaries' investigates whether nodes in a blockchain can benefit from the exemptions for Internet intermediaries established in the Directive on electronic commerce in 2000. The section 'How to move forward?' is forward-looking, it delves into possible alternative, preventive measures that can and perhaps should be taken and formulates ideas about how blockchain intermediaries should relate to illegal content.

WHAT IS A BLOCKCHAIN?

In 2008, Satoshi Nakamoto published his paper on bitcoin, a peer-to-peer electronic cash system.[5] The interesting part of this system is the underlying distributed database. A blockchain is in essence a database of which many copies exist (also called nodes), held by different administrators.[6] New data to be added to the blockchain are first collected in a so-called block and then en-bloc appended to the existing database.[7] A newly added block contains a hash of (ie a reference to) the last block in the existing chain.[8] This explains the term blockchain. The most salient property of a blockchain is its immutability. An individual administrator may remove old data from his copy of the blockchain, but this does not change what is considered the contents of the blockchain. Immutability thus must be understood as contents of the blockchain having an existence (to a certain extent) independent from the individual administrator(s) of copies of the blockchain. According to Nakamoto, the

4 art 14 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1, 17 July 2000.

5 S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' <https://bitcoin.org/bitcoin.pdf> accessed 21 March 2019.

6 Nakamoto, ibid 3, s 5.

7 ibid 3, s 5.

8 ibid 3, s 5, Step 6.

immutability eliminates the need to trust the administrator of a database[9] and further down the line, other actors need not be trusted anymore.[10] This section neither delves in the question whether a blockchain succeeds in eliminating trust, nor in the question whether the elimination of trust is desirable in the first place.[11] It concentrates on the more elementary issue of immutability.

How is immutability achieved?[12] A first element has already been mentioned above: redundancy. There are many copies of the database thus strongly reducing the dependence on individual administrators of copies.

A second element is a system of crypto-economic incentives. There are positive incentives—a node playing by the protocol can earn cryptocurrency (such as bitcoin). There are negative incentives—an administrator of a copy needs to invest first, eg computer equipment and electricity, in order to be able to earn cryptocurrency.

The replacement of a central database held by a central authority (such as a bank) with multiple copies of the database, creates however a new problem, namely that the various copies must stay in sync.[13] Creating synchronicity by designating one node as a master node that other nodes (the slaves) must follow at all times would not fit in Nakamoto's ideas about elimination of trust: it would reintroduce dependence on a central authority.[14]

By way of example, the following paragraphs will describe how the synchronization in the Bitcoin blockchain is achieved and in the process, it will become clear how immutability is achieved.

Synchronicity and immutability require that is defined, what is seen as the valid database/copy of the blockchain. The valid blockchain is the longest chain starting with the genesis block and only containing valid blocks.[15] What a valid block is, will become clear below.

How is a new block added to bitcoin blockchain?

If a participant in the bitcoin blockchain wants to perform a payment, his transaction data are sent to all the nodes in the network.[16] For a period of about 10 minutes, the nodes collect all incoming transactions and place them in so-called blocks. Since the transaction data are sent over the Internet, which is an unreliable network, the blocks that the various nodes prepare show similarity, but they are not identical. The order

9 ibid 1, Introduction.

10 Blockchains are claimed to have many applications beyond creating a crypto-currency. See eg D Tapscott and A Tapscott, *Blockchain Revolution: How the Technology behind Blockchain is Changing Money, Business, and the World* (Portfolio/Penguin 2016) and M Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly Media 2015).

11 Evidence that blockchains have many practical uses is thin, see M Higginson, M Nadeau and K Rajgopal, 'Blockchain's Occam Problem' <https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem> accessed 21 March 2019, introduction of the article.

12 A Antonopoulos, *Mastering Bitcoin. Programming the Open Blockchain* (O'Reilly Media 2017); J Bonneau and others, 'Research Perspectives and Challenges for Bitcoin and Cryptocurrencies', in *IEEE Security and Privacy* (IEEE 2015); P Franco, *Understanding Bitcoin: Cryptography, Engineering and Economics* (Wiley 2014).

13 Nakamoto (n 5) 2, s 2.

14 ibid 2, s 2.

15 ibid 3, s 5.

16 ibid 3, s 5.

of the transactions may be different. Also, some nodes receive a transaction in time to include it in the block while other nodes do not.[17]

At the end of that 10-minute period, the nodes start solving a cryptographic puzzle based on their respective blocks competing with each other to be the first to solve their puzzle. In doing so, the administrators of the nodes commit computer time and electricity to the competition. Who wins the competition is to a large extent determined by chance. The winner sends proof-of-work (proof that he solved the puzzle) to all other nodes, who can then verify that he indeed succeeded in solving the puzzle. The winner's block extends (if all is well) the existing longest chain with one block and becomes the new longest chain. Nodes express their acceptance of the new longest chain by appending their new candidate block to the block just added to the longest chain. The winner cashes in on a cheque that he wrote to himself in the block he prepared.[18] The cheque is paid for with newly created bitcoins. This procedure for determining which new block to add to the chain is usually referred to as the consensus mechanism.

How does this system relate to the claims made above?

First, since the outcome of the competition is to a large extent based on chance, it is likely that every 10 minutes another node elevates its candidate block to a canonical block. In this way, no node can gain a predominant influence on the contents of the blockchain. Secondly, there are negative and positive incentives: each administrator of a node invests electricity in mining, depends on winning bitcoins, owns bitcoins and bitcoins only have value as long as the bitcoin blockchain is alive.[19] Thirdly, since every node administrator builds on the longest chain, the administrators will (over time) converge to the same chain (synchronicity).[20] Fourthly, the blockchain is immutable. How is this achieved? Suppose that the administrator of a node would change data in an old block in his copy of the blockchain. This would have two immediate consequences: first, the proof-of-work of this block would no longer be correct and the block is invalid. Secondly, the reference in the subsequent block to the block in which the change took place would no longer be correct. The chain of our node would thus be broken. It is no longer the longest chain and will be ignored by the other nodes. The administrators of the other nodes can only earn cryptocurrency by building on the longest chain. So, an administrator of a node can physically change data in an old block, but if he does so he pays a high price: he disqualifies himself for meaningful participation in the blockchain. The community of miners at large will not see his chain as valid.

Distinction full node/miner

In general, the functions of nodes are divided in two parts: a so-called full node maintains a copy of the entire blockchain and performs checks on transactions (for

17 ibid 4, s 5.

18 In fact, the winner can only cash-in after another 100 rounds. The finality of the block is then deemed statistically certain.

19 Antonopoulos (n 12) ch 2, s 'Bitcoin Mining'.

20 Nakamoto (n 5) 3, s 5.

example, on double spending in the bitcoin blockchain) and the so-called miner participates in the consensus mechanism.[21]

Public/private

Blockchains may be public: The public character relates to the contents of the blockchain. The bitcoin blockchain is public, ie all bitcoin transactions can be inspected by anybody. Data added to a transaction, such as child pornography or a work protected by copyright is equally visible. The privacy of the transactions is only protected in that those involved in bitcoin transactions are only known by a pseudonym (a bitcoin address or public key). If a blockchain is permissionless, anybody can participate in the consensus mechanism. In a permissioned blockchain, a central party may decide who is accepted as a node participating in the consensus mechanism.[22] It is also possible that other procedures are used to decide on the admission of new nodes. For example, all participating nodes together could decide who will be admitted as new nodes.

Smart contract

The code underlying the bitcoin blockchain is written by a core development team. In some blockchains, such as Ethereum, users have possibilities to add code to a blockchain[23]; the users can create so-called smart contracts. This is a code that a user can place on the blockchain. Once it is placed on a permissionless blockchain, the uploader can no longer change the code or withdraw it from the blockchain (with the same proviso as made above for immutability of data on a blockchain). When (another) participant chooses to use the smart contract, ie run its code, the code is executed on the computer systems of the nodes. A smart contract can be used to automate a legal contract. An example could be that a smart contract upon reception of a payment sends a download link to the person making the payment. However, unlike its name suggests, it is not given that a smart contract code forms an agreement or contract in the legal sense of the word. Also the term 'smart' needs to be taken with a grain of salt: it is any code and need not show sophistication in the form of artificial intelligence (hereinafter AI). In essence, a smart contract is simply a code.

Drawbacks of blockchain

The opportunities blockchains offer do come at a price. Blockchains do demand much computer time and data storage space.[24] Especially, consensus mechanisms based on proof-of-work (as in the bitcoin blockchain) are very resource intensive. Alternative consensus mechanisms are being developed that are less resource

21 Antonopoulos (n 12) 140–41.

22 'BitFury Group in collaboration with Jeff Garzik. Public versus Private Blockchains. Part 1: Permissioned Blockchains' (20 October 2015) White Paper (Version 1.0), 10 <https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf> accessed 28 June 2019.

23 The bitcoin blockchain only has the possibility to repurpose bitcoins. For more information on these so-called colored coins, see Antonopoulos (n 12) 221.

24 B Carson and others, 'Blockchain Beyond the Hype: What is the Strategic Business Value?' <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value> accessed 21 March 2019, para 'Nuts and bolts of blockchain'.

intensive. An example is proof-of-stake where nodes commit cryptocurrency instead of computer resources and electricity. But with blockchains with alternative consensus mechanisms little experience exists and it is unclear how reliable they are.

Correctness

What is stored in a blockchain is not per se correct.[25] Data in a blockchain are only correct to the extent that they have been introduced in the blockchain correctly. At the entrance limited checks can be performed, such as the check on double spending in the bitcoin blockchain. Code on the blockchain may need to be inspected by those wishing to use it in order to convince themselves that the code is usable for the purpose for which they intend to use it. This may lead to a need for new intermediaries, such as gatekeepers that prevent the blockchain from becoming polluted. This in turn may lead to new dependence on intermediaries.

RESPONSIBILITIES OF INTERNET INTERMEDIARIES

Internet intermediaries bear some responsibility for content uploaded by users,[26] especially if the intermediaries host information. In a blockchain, the full nodes host content. The question arises whether they are subject to the same responsibilities as more traditional hosting providers, such as Internet Service Providers (hereinafter ISPs) offering webhosting. In the EU, the Directive on electronic commerce is the starting point for discussing responsibilities of Internet intermediaries. The Directive creates exemptions from liability. The conditions under which the exemptions are available give a first indication of the responsibilities.[27]

Directive on electronic commerce

The Directive on electronic commerce is applicable to information society services. These are:

> any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.[28]

25 ibid.

26 DA Zetzsche, RP Buckley and DW Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) U Ill L Rev 1361, 1403.

27 That is, assuming that in the absence of the exemption there is liability. That is not completely certain, because it depends on national liability law. C Angelopoulos and S Smet, 'Notice-and-Fair-Balance: How to Reach a Compromise Between Fundamental Rights in European Intermediary Liability' (2016) 8 J Media L 266, s IV A shows that a wide variety of responsibilities have developed.

28 For the purposes of this definition:

- 'at a distance' means that the service is provided without the parties being simultaneously present,
- 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

An indicative list of services not covered by this definition is set out in Annex V of Directive 98/48/EC.

Hosting providers in the WWW fall under this definition. The administrators of full nodes are probably also covered by this definition. The administrators often provide their services for a transaction or block fee, or at least a chance on a block fee. Full nodes host the data stored in the blockchain. The data is uploaded by a user, eg somebody initiating a bitcoin payment and in a public blockchain these data can be inspected by anybody. The users of a blockchain can be seen as the recipients of the service.

The exemption from liability only applies to an activity that 'is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored'.[29] In L'Oréal/eBay, the CJEU decided that Article 14 Directive on electronic commerce applies to 'the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored'.[30] Is a full node a passive operator as meant by the CJEU or does he play an active role? A full node receives data from a user. The data are automatically stored and automated checks are performed, for example, a check on double spending in the bitcoin blockchain. The role of the full node strongly tends to the passive side. The administrator of the node does not gain knowledge of the data stored in the normal course of processing.[31] Moreover, its control over the storage or the type of checks to be performed is limited. The checks that are performed are not defined by the full node. The core implementation or an application at a higher level, such as a smart contract or DAO,[32] defines the code that is used to perform the checks. The full node merely executes the checks in a fully automated manner.

The exemptions in the Directive on electronic commerce relate to a mere conduit, caching and hosting providers. A full node does not qualify for the first two functions, since its storage of data is neither transient (Article 12(2)) nor temporary

29 Recital 42 Directive on e-Commerce.

30 Case C–324/09, *L'Oréal SA et al v eBay International AG et al* (ECJ 12 July 2011) ECLI:EU:C:2011:474

31 Compare in this respect that the ECJ allowed the following operators to benefit from the exemptions of the Directive on e-Commerce as passive service providers: provider of an IP address rental and registration service allowing the anonymous use of internet domain names (Case C–521/17 *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* (ECJ, 7 August 2018) ECLI:EU:C:2018:639), the provider of free WiFi (Case C–484/14, *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* (ECJ, 15 September 2016) ECLI:EU:C:2016:689), the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored (*L'Oréal v eBay* (n 30)) and an Internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored (Joined Cases C–236/08 to C–238/08 *Google France SARL et al v Louis Vuitton Malletier SA et al* (ECJ, 23 March 2010) ECLI:EU:C:2010:159). The ECJ found the following operators not to be passive providers: a newspaper publishing company which operates a website on which the online version of a newspaper is posted, that company being, moreover, remunerated by income generated by commercial advertisements posted on that website, since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge (Case C–291/13 *Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, and Giorgos Sertis* (ECJ, 11 September 2014) ECLI:EU:C:2014:2209).

32 A DAO is a decentralized autonomous organization. It is a decentralized organization, the bylaws of which are completely laid down in smart contracts, ie code and where governance highly depends on tokens. See https://blockchainhub.net/dao-decentralized-autonomous-organization/

(Article 13(1)). A full node may qualify as a hosting provider because it does store data. An Internet provider with a webserver hosts the HTML-pages of its clients. It clearly is a hosting provider since hosting data is a substantial element of the service provided. Also eBay is seen as a hosting provider for auction data, even though it does support auctions and thus does more than merely offering storage space and making the stored content available to the Internet public.[33]

In the bitcoin blockchain, a user delivers an electronic document of the desired transaction which then is registered by the nodes of the network. The blockchain only registers the transaction but does not provide further services such as an indication of the amount in the account of the client. Other service providers such as wallet providers may provide such service. A blockchain offering a cryptocurrency is therefore likely to be qualified as a hosting provider.

Assuming an application in which a full node can be qualified as a hosting provider, the full node may make use of the exemption from liability provided in Article 14(1) Directive on electronic commerce. The exemption requires that:

a. the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
b. the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

The latter condition has in the practice of ISPs given rise to NTD systems. This requires that a hosting provider can remove content from his server or make it inaccessible.

Application of an NTD system to a blockchain

Can you implement an NTD regime in a blockchain that builds purely on crypto-economic incentives? A straightforward way to apply NTD in a blockchain is that those notifying content do so by addressing an individual administrator of a full node. Assuming that the administrator of the node deems the notified content illegal, can he remove the content from the blockchain? From a purely technical perspective, he can. It is simply data on his computer system. However, from a broader business perspective, he cannot. If he removes content from his copy or version of the blockchain, the chain in his version of the blockchain would be broken. Miners in the network will ignore our administrator's version of the blockchain since it no longer represents a valid version of the blockchain. Our administrator would therewith disqualify himself from further meaningful participation in the blockchain. Given the high cost of complying with a request to remove, an administrator is highly unlikely to comply.

That said, there are a few academic explorations into the creation of a permissionless blockchain from which data can be deleted. Florian et al. developed a system that allows some nodes to erase data as long as there are other nodes

33 *L'Oréal v eBay* (n 30).

that maintain the entire chain.[34] Deuber et al. propose a system in which administrators can vote about deletions.[35] These are theoretical solutions with which no practical experience exists outside a laboratory setting.

The above presumes that a notification is sent to a single node in the network. Even if the node would remove content from his copy/version of the blockchain, the content would still be available on many other nodes. Therefore, it is interesting to ask, what would happen, if a notification is sent to all or nearly all nodes?[36] Could they collectively comply with the request to remove? The incident of the so-called The DAO hack can give some insight into this. The DAO was an initial coin offering. Through a bug in the smart contract code one participant could appropriate a large amount of the invested cryptocurrencies and divert them to his own account. The Ethereum community was split over the question whether there was a wrongdoing here. One faction contended that the smart contract represented the entire relationship between the parties involved. The hacker simply used the code as it was and had been visible for everybody from the beginning. Hence, in this view, there was no wrongdoing. Another faction placed the hack in a wider context. The cryptocurrencies were brought together to help start-up companies. From this perspective, the diversion of cryptocurrencies to somebody's personal account was wrongful. The latter faction had more than half the processing power in the network. They rebuild the blockchain from the moment of the appropriation of the cryptocurrencies. It goes without saying that the transactions diverting cryptocurrencies to the hacker were left out of the newly rebuilt blockchain. So, what is the implication of The DAO hack? Is a blockchain built on crypto-economic incentives mutable after all? That depends on the context in which you ask the question. In an absolute sense, even a blockchain based on crypto-economic incentives is not completely immutable. However, if you ask the question whether the mutability as demonstrated in The DAO hack can be utilized to implement an NTD regime the answer is very different. The DAO mutation was very costly (rebuilding the last part of the blockchain) and required the cooperation of administrators, representing more than half the processing power in the network. Assuming that under an NTD system, notifications would be received regularly, then the processes followed in The DAO hack case are too laborious and too dependent on finding a majority to be a realistic option. At present, it seems that there are no possibilities to implement an NTD system in a blockchain that is based purely on crypto-economic incentives.

34 M Florian and others, 'Erasing Data from Blockchain Nodes' (Humboldt Universität zu Berlin/ Weizenbaum Institute, 2019) <https://arxiv.org/pdf/1904.08901.pdf> accessed 29 September 2019.

35 D Deuber, B Magri and SAK Thyagarajan, 'Redactable Blockchain in the Permissionless Setting' (4 December 2018) <https://bernardomagri.eu/wp-content/uploads/2018/12/redactable_premissionless.pdf> accessed 29 September 2019.

36 By the way, finding out who the administrators of nodes are and reaching out to them, would be a task for the notifier, since blockchains generally (or even never?) support distribution of notifications to administrators of nodes.

In practice, sending notices to administrators of full nodes in a blockchain purely based on crypto-economic incentives will not work and those sending notifications draw the short stick.

HOW TO MOVE FORWARD?

The Directive on e-Commerce finds in an NTD system a workable compromise between competing values. However, the old compromise (NTD) seems not to be workable in blockchain context. A hard conflict between the immutable blockchain and the law that under circumstances does require information to be taken down seems inevitable. Mattzutt et al. foresee that administrators in permissionless blockchains may find themselves between a rock and a hard place. Removal of information from old blocks is very detrimental to their business, but non-removal may lead to legal liability. Others contest that administrators will not so easily be found liable.[37] They point to the lack of knowledge of administrators of illegal content (which does not seem to be a strong argument since notifications may easily end a state of not-knowing) and their good intentions (which may under circumstances indeed be a relevant factor particularly where the blockchain application has not made publication its main purpose).

Matzutt et al. propose to be ahead of such problems by devising *ex ante* measures. These are measures that should prevent or lessen the chance of illegal content being introduced in the blockchain in the first place. Filtering and pricing of content are examples of such measures.

Filtering typically takes place 'at the entrance', ie when content is placed on the blockchain. In the bitcoin blockchain, we saw for example that new transactions are checked for double spends. These checks are performed automatically. In a similar fashion, checks on legality of input data may prevent unwanted data from entering the blockchain and thus prevent pollution of the contents of the blockchain. In the Bitcoin Satoshi Vision (BSV) blockchain, a filtering measure is actually applied.[38]

Another measure is pricing of content. Illegal content is mostly added to a bitcoin transaction by writing it in the space for the transaction output. The transaction output specifies the recipients for the payment and the amount they receive. Since the bitcoin blockchain allows a bitcoin payment to have many recipients, there are few space constraints and this can be abused by placing illegal content there, eg a child porn picture. Since by far the most transactions have no more than two recipients, longer transaction outputs can be correlated with illegal content. Pricing content according to its length (the space it takes) therefore can help discourage the inclusion of illegal content in the blockchain, without impeding the normal functioning of bitcoin as a system for performing payments.[39]

37 A Narayanan, K Werbach and J Grimmelmann, 'Why Porn on the Blockchain Won't Doom Bitcoin' (*Wired*, 29 March 2018) <https://www.wired.com/story/why-porn-on-the-blockchain-wont-doom-bitcoin/> accessed 24 June 2019.

38 BBC, 'Child Abuse Images Hidden in Crypto-currency Blockchain' 6 February 2019, <https://www.bbc.com/news/technology-47130268> accessed 24 June 2019.

39 R Matzutt and others, 'Thwarting Unwanted Blockchain Content Insertion' in *IEEE International Conference on Cloud Engineering (IC2E)* (IEEE 2018), 364–70.

Framework for *ex ante* measures

A framework for analysing (*ex ante*) measures can be derived from the ruling of the EU Court of Justice in Tiscali/SABAM. The framework developed in this ruling builds on fundamental rights.[40] In the case at hand, the protection of intellectual property (IP) needed to be balanced against other fundamental rights.[41] These include the freedom to conduct business,[42] the right to data protection[43] and the freedom to receive and impart information.[44] This framework can be generalized. Adapted to the challenges in the blockchain context, the framework would look as follows. On the one side, there are the fundamental rights of those harmed by illegal content on a blockchain. These rights may concern IP (eg copyright), privacy (eg reputation), health (eg child porn) or other fundamental rights. On the other side, there are the fundamental rights of the users of a blockchain, such as their freedom of expression, their freedom to receive information or non-discrimination. On this side of the discourse, we also find the rights of the full nodes themselves, such as their freedom to conduct business.

Analysis *ex ante* measures

Ex ante measures have important drawbacks when laid along the Tiscali-SABAM framework.

Ex ante measures lay pressure on the freedom of expression. Pricing makes exercising the right to freedom of expression more expensive. Filtering prevents information from becoming available at all. Moreover, filtering is applied by a private party (the administrator of a full node) without the intervention of a court. The European Court of Human Rights (hereinafter ECHR) has shown itself to be wary of *ex ante* filtering in the context of an online news portal. In the case *MTE v Hungary*, it ruled:

> The domestic courts held that, by allowing unfiltered comments, the applicants should have expected that some of those might be in breach of the law. For the Court, this amounts to requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet.[45]

The administrator of a blockchain node is likely to block too much content if his responsibility would be triggered by the mere possibility that something illegal be uploaded to his server. A blockchain as a means to realize freedom of speech is not just a theoretical issue. A blockchain has already been used as a means to circumvent

40 Case C -70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). (CJEU, 24 November 2011), ECR 2011 I-11959, ECLI:EU:C:2011:771.

41 ibid 45.

42 art 16 Charter of Fundamental Rights; ibid 46–49.

43 *Scarlet v SABAM*, ibid 50–51.

44 ibid 52–53.

45 Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary (ECtHR, 2 February 2016) ECLI:CE:ECHR:2016:0202JUD002294713, 82.

state censorship in China.[46] Moreover, blockchains may in future have explicit journalistic applications.[47]

Ex ante measures have important limitations where it comes to barring illegal information. Pricing does not guarantee that no illegal information enters the blockchain. Filtering is limited in its effectiveness because it is difficult to foresee what information will prove to be illegal. The assessment of legality of information often requires some contextual knowledge (eg that information uploaded is protected by copyright and that the uploader does not possess a licence). The administrator of a full node generally lacks such content knowledge, which complicates the assessment of its legality. From a perspective of those who are a victim of illegal information, *ex ante* measures will often not help.

Even though Mattzutt et al. introduce *ex ante* measures to help administrators, this does not mean that *ex ante* measures are easy and cheap to implement for administrators. This holds especially for filtering. A somewhat sophisticated filtering system is costly.

Maybe *ex ante* measures lessen the liability risk for administrators, but they do so at the cost of introducing many new issues. Therefore, it is questionable whether *ex ante* measures will bring the solution.

Hence there seems to be a dilemma. *Ex ante* measures raise many concerns, whereas an NTD system clashes with the immutability of a permissionless blockchain. At the same time, the pressure on Internet intermediaries to take in some form of responsibility for content uploaded by others (Internet users, blockchain users etc.) is mounting.[48] So, how to proceed from here?

The proper quest is to return to the basis. What is the reason to strive for immutability of the contents of a blockchain in the first place? Nakamoto claims that immutability takes away the need to trust intermediaries and even the need to trust an opposite party in a contract. It cannot indeed be ruled out that there are circumstances in which the elimination of the need to trust can be beneficial. However, it is unclear to what extent the need to trust is broadly felt as a problem. Two elements remain to be clarified. First, under what circumstances is an elimination of trust beneficial? Trust is in essence reliance that something will happen without being certain that it will. Phrased like this it is a form of risk-taking. This sounds as something you indeed would want to avoid. However, in reality it is a calculated risk. With simple measures, often a good impression of somebody's trustworthiness can be obtained. A limited investigation of the reputation of the envisaged business partner

46 See eg S Singh, 'Blockchain Is Helping to Circumvent Censorship in China. It's Not All Hype—At Least this Time' (*Slate*) 18 July 2018 <https://slate.com/technology/2018/07/blockchain-is-helping-to-circumvent-censorship-in-china.html> accessed 24 June 2019.

47 See eg 'Journalism and Blockchain: Freedom of Speech, No One Can Cancel' <https://medium.com/@endo_protocol/journalism-and-blockchain-freedom-of-speech-no-one-can-cancel-9138b00f56b5> accessed 24 June 2019.

48 See eg 'Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online' COM (2018) 640 final, 2018/0331 (COD), arts 3 and 6 <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf> and Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.) [2019] L130/92, art 17.

does already reduce the risk. For the rest risk, it is simply more cost-effective to simply take the risk. Further reducing the risk requires that expensive checks are performed. A blockchain in itself does nothing to reduce the cost of further checks. Moreover, the need to avoid trust is context-dependent. In western European societies, long since effective mechanisms have been developed to do business safely. In addition, the legal system is a fall-back option might it go wrong after all. In conclusion, trusting often is an efficient way to do business and elimination of trust requires that measures are taken that carry a cost. The question is how much need there is for a means to eliminate trust completely.

A second element that remains unclear is whether a blockchain actually succeeds in eliminating the need to trust. In essence, a participant in a blockchain must trust the blockchain core code and the code of smart contracts. The DAO hack case shows that blockchain code is not without bugs and that bugs can be exploited. Theoretically, the counterargument could be made that blockchain code need not be trusted since it is open source and can be inspected before use. However, inspection of code costs time. This confirms the point made above that the elimination of trust is costly. The DAO hack case shows that in practice, those relying on the blockchain do not check the code. The cost of code-checking is avoided by trusting the blockchain... If the inspection of code would be outsourced to an expert, the expert must be trusted. In that case, trust is not eliminated but merely displaced.

If even a blockchain building on crypto-economic incentives does not escape the economic reality that trust is to a certain extent efficient and that measures to eliminate trust completely are not worth their cost, this places into perspective the need to strive for absolute immutability.

An NTD system is incompatible with a permissionless blockchain modelled after the bitcoin blockchain as it currently functions. It is however premature and probably unnecessary to draw from that the conclusion that NTD systems have no future for blockchains. The question for the future is what the actual need is for 'hardcore' blockchains. Many blockchain projects already opt for the 'softer' permissioned variants of blockchains.

If there is a blockchain future, then this will probably be a future in which blockchains are adapted to the true needs of society. Such blockchain would have to confront many challenges in relation to illegal content. It would need to be receptive to an NTD. Perhaps, it would need to provide for a possibility to send notices to many nodes at once. It may also have to confront the global character of blockchains. The nodes of permissionless blockchain network can be found all over the world. The effectiveness of an EU-wide NTD would be diminished because of the many nodes outside the EU. However, the problems of not being able to remove content from a blockchain will likely be relevant in most jurisdictions: rightsholder will not be happy with continued presence of their works on blockchains, authorities will want to make child pornography inaccessible and terrorist content continues to be a thread as long as it is available. In that sense, the EU may play an important role as forerunner. Solutions that have proven to work are attractive to other jurisdictions.

CONCLUSION

Blockchain has many applications. They can be used for content distribution. This may serve praiseworthy purposes such as circumvention of censorship, but may also be used for the distribution of illegal content. In computer science literature, concern is raised whether content distribution will involve the responsibility of administrators of full nodes. The EU Directive on e-Commerce dealing with the responsibility of hosting service providers premises a preemption of liability on the timely removal of notified content. It is contended that this is problematic in view of the immutability of permissionless blockchains. The proposed solution in computer science literature is to devise *ex ante* measures that prevent or at least diminish the chance that the blockchain is polluted with illegal content in the first place. This article shows that such *ex ante* measures raise serious concerns with respect to freedom of expression and protection of victims of illegal content. This article invites to revisit the position that NTD is not workable for blockchains. Immutability is not absolute, but rather a question of degree. A critical appraisal of which degree of immutability is needed for which practical application of blockchain is generally lacking. Holding on to the current legal framework will invite a technical development that accommodates the current legal framework. This will not make blockchain impossible. Technology is more flexible than is sometimes thought and adaptation of technology to society's true needs is imperative.