Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Creating markets in no-trust environments: The law and economics of smart contracts

Helen Eenmaa-Dimitrieva[a,*], Maria José Schmidt-Kessen[b]

[a] JSD Yale Law School, Postdoctoral Researcher in Information Technology Law, Founder of the Research and Study Programme in Information Technology Law, School of Law, University of Tartu, Näituse 20, Tartu 50409 Estonia
[b] PhD European University Institute, Postdoctoral Researcher and Teaching Associate at Queen Mary University London, Centre for Commercial Law Studies, 67-69 Lincoln's Inn Fields, London WC2A 3JB, United Kingdom

ARTICLE INFO

Article history:

Keywords:
Primary: law and economics
Contract law
Smart contracts
Enforcement
Trust
Secondary: efficient breach
Relational contracts
Blockchain
Trustless trust
No-trust

ABSTRACT

Smart contracts, self-executing agreements based on blockchain technology, have the capacity to create trust in what we term no-trust contracting environments. We argue that using them in such environments is the path to unleash the full potential of smart contracts. Compared to the contract enforcement mechanisms characterized by traditional contract law or relational contracts, smart contracts can offer a superior solution for facilitating trade.

Several lawyers and economists have debated whether smart contracts might offer the prospect of cheaper, faster and better transactions. As we discuss below, contract law scholars caution that they neither replicate the relational context essential for the day-to-day practice of contracting nor offer a superior solution to problems addressed by traditional contract law, such as contract validity and legality. We clarify and systematize the current thinking on the legal nature and reliability of smart contracts, and address the concerns of contract law scholars. While doing that, we suggest a step forward in characterizing contracting environments, contract enforcement mechanisms and the trust relationship underlying contracts.

1. Introduction

Smart contracts, agreements written in code that are automatically executed in a blockchain environment, are a hotly debated topic.[1] They have been discussed by computer scientists extensively, and legal literature on the topic is quickly growing. The purpose of this paper is to situate smart contracts in the field of law and economics of contracts, something that has not yet been done so far.

Broadly speaking, existing literature on the law and economics of contracts can be split in two strands. One strand

[*] University of Tartu School of Law, Näituse 20, Tartu 50409 Estonia.
E-mail address: helen.eenmaa@ut.ee (H. Eenmaa-Dimitrieva).

[1] Smart contracts can be generally understood as self-executing digital transactions using decentralized cryptographic mechanisms for enforcement. (See Kevin Werbach and Nicolas Cornell, 'Contracts *Ex Machina*' (2017) 67 *Duke Law Journal* 313) Today, blockchain seems to have become the primary technological choice for the implementation of smart contracts. The term 'smart contract' was coined by Nick Szabo, a US computer scientist and legal scholar in 1996. According to his definition a smart contract is 'a set of promises, specified in digital form, including protocols within which the parties perform on these promises'. (Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996) 16 *Extropy* <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 11 July 2017.

https://doi.org/10.1016/j.clsr.2018.09.003
0267-3649

discusses the efficiency and costs of existing contract law regimes, and provides normative ideals for efficiency enhancing contract law design. A second strand has tackled the area of contractual practices outside the strict confinements of the legal system. These include game theoretical accounts of contracting and the discussion relating to so-called relational contracts that focus on the social context, more than on the legal context, of contracting. We suggest that smart contracts could open up a third field of inquiry within the law and economics of contracts, characterized by the study of new modes of contract enforcement as sources of market creation.

New technologies are changing how we understand law and operate in a legal system. Most of the disruption in law comes from other business sectors – computer engineers or business people who use legal services and want to change the industry. One track in these changes belongs to the opportunities created by distributed computing.[2] In this paper, we discuss how smart contracts - one of such applications of distributed computing - could provide a possible alternative mechanism for ensuring cooperation in transactions between two or more parties that cannot rely on any common legal or social background guaranteeing contract enforcement. Blockchain technology makes it possible for parties to preserve their anonymity while contracting with each other and smart contracts seem to be able to function in precisely such contracting environments where parties could meet in anonymity. We claim that this feature sets smart contracts apart as new modes of contracting governance.

In particular, we argue that smart contracts have the capacity to create trust in what we term no-trust contracting environments and using them in such environments is the path to unleash their full potential. Compared to the contract enforcement mechanisms characterized by traditional contract law or relational contracts, smart contracts could, at times, offer a superior solution for facilitating trade.[3] Several lawyers and economists have debated whether smart contracts might offer the prospect of cheaper, faster and better transactions. As we discuss below, contract law scholars caution that they neither replicate the relational context essential for the day-to-day practice of contracting nor offer a superior solution to problems addressed by traditional contract law, such as contract validity and legality. We clarify and systematize the current thinking on the legal nature and reliability of smart contracts, and address the concerns of contract law scholars. In the process, we suggest a step forward in characterizing contracting environments, contract enforcement mechanisms and the trust relationship underlying contracts.

The article thus relies on various distinctions. In addition to those already mentioned we explain why in terms of both regulatory and economic implications it might be helpful to draw a distinction between smart contracts based on public blockchains and those based on permissioned blockchains. The design of the underlying technology (at least in terms of the identifiability of persons transacting on blockchain, the selection of nodes and the size of network, the particularities of the consensus mechanism and the transparency of the content of the blocks) is a significant feature that needs to be factored into the discussion. This is a point often overlooked in legal academic literature.

The paper is not focused on discussing external mechanisms to regulate smart contracts. In fact, we do not claim that smart contracts cannot be regulated by contract law or social norms - they could. Our focus is on explaining how smart contracts can themselves provide such an alternative mechanism of contract governance. While the impact of smart contracts is potentially broader, in this paper, we confine our argument solely to their effects on contracting and relations with contract law.

In order to put forward the new way of thinking about smart contracts from a law and economics perspective we offer two interlinked narratives.

- The first narrative engages with the two strands of literature that have developed within the field of law and economics of contracts, namely the analysis of black-letter law on the one hand, and the sociological mechanisms that lead to contract enforcement outside black-letter contract law on the other hand.
- The second narrative is a cost-benefit analysis, in which we discuss the possible efficiencies of smart contracts.

The main steps of our argument are the following:

1. Parties to smart contracts on public blockchains can remain anonymous (to an extent and depending on the substantive content of the contract)
2. When you have anonymity and other legal or relational enforcement mechanisms are weak or not available, you have the paradigm set of circumstances for a no-trust environment for contracting (which is different from legal or relational contracting environments)
3. In order to contract in no-trust environments, there is a need for an enforcement mechanism which provides sufficient safeguards for contracting
4. When enforcement through law or social relations is unavailable or inconvenient, smart contracts allow us to rely on enforcement through technology.
5. Trade relies on trust and while other enforcement mechanisms support trade through other trust mechanisms (first-personal, peer-to-peer, or Leviathan trust mechanisms), smart contracts offer a new mechanism characterized by trustless trust.
6. Based on the potential efficiency gains and losses from contracting in no-trust environments, there would be

[2] Distributed computing enables not only the creation of decentralized currencies like Bitcoin, but also intelligent assets that can be controlled over the Internet (smart property), new governance systems with more democratic or participatory decision-making, decentralized or autonomous organizations that can operate over a network of computers without any human intervention as well as self-executing digital transactions (smart contracts). Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia'(2015) <http://papers.ssrn.com/abstract=2580664> accessed 11 July 2017, 1; Voshmgir Shermin, 'Disrupting Governance with Blockchains and Smart Contracts' (2017) 26 *Strategic Change* 499.

[3] As we will explain below, while this claim assumes that both parties have the infrastructure to participate in the blockchain, it does not necessarily presume the existence of a legal system which recognises and enforces such transactions.

reasons to prefer smart contracts to other methods of contract governance.

2. The nature of smart contracts

2.1. *What are smart contracts?*

Blockchain technology, the technology underlying smart contracts, is one of the distributed ledger technologies (also known as decentralized public ledger, trustless public ledger, shared ledger technologies). This technology is not a leap in technological progress. Distributed computing as in peer-to-peer networks, the use of cryptographic keys, distributed data storage and consensus mechanisms had all been invented and put to use by the late 1990s.[4] Nonetheless, blockchain technology helps to resolve the problem of how coordination of individuals' activity could be ensured without a central authority guaranteeing the validity of transactions, and as such it is currently causing a disruption in many business sectors.[5]

There are several debates about the nature of smart contracts. In order to participate in them, it is certainly helpful to understand the distinctions between various types of computerized programmes we operate with on a daily basis as well as to see how digital agreements have evolved.[6] Today, smart contracts are mostly understood as agreements that are encoded in computer code and placed on a decentralized virtual infrastructure. Computer protocols verify and execute the clauses and performance of a contract thus making some traditional contractual activities involved in the enforcement unnecessary. The technology allows the automatic implementation of the terms of an agreement.[7] It also makes it possible for parties to preserve their anonymity to some extent while contracting with each other. The literature includes a wide range of definitions for smart contracts that vary mostly due to the different points of emphasis.[8] The common defining characteristic of smart contracts is, however, that they are executed automatically without the need of human intervention.[9] We recognize that smart contracts do not necessarily need to be based on a blockchain but limit the current discussion to those that are.

There is a good reason for the definitions to vary. Smart contracts can have different functions; a smart contract in the technical sense is not necessarily the same as a contractual agreement in the legal sense. At times, a smart contract indeed represents the translation of a specific contractual agreement with legal force between two parties. In other cases, smart contracts codify relationships that are both defined and automatically executed by code, 'but which are not linked to any underlying contractual rights or obligations'.[10] In these cases, the term 'smart contract' loses any legal meaning and becomes a technical term in the world of computer engineering. There are, for example, smart contract models for one party only.[11] In the latter case, smart contracts might be used to coordinate tasks between different units of an organization. To function, these smart contracts will need immediate access to organizational information external to the blockchain, such as the organization's internal data and business processes.[12] One-party smart contracts, and their underlying blockchain system, are therefore also technologically different from bilateral or multi-sided smart contracts and their blockchain ecosystem.[13]

2.2. *Public and private blockchains*

In general, one could opt for a public blockchain ('fully decentralized'), a consortium blockchain ('partially decentralized'), or a private blockchain ('centralized') for building smart contracts on top.[14] Consortium and private blockchains are usually referred to jointly as permissioned blockchains. The three core technologies that make up blockchain technology, the distributed network of computers that keeps a chronological database of all transactions (the ledger), the use of cryptographic keys, and a network servicing protocol (the consensus

[4] Wright and De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 2) 4–5.

[5] ibid 5.

[6] Surden distinguished between various types of computerized programmes. Harry Surden, 'Computable Contracts' (2012) 46 *UC Davis Law Review* 629. Werbach and Cornell provide a summary of the evolution of digital agreements. Werbach and Cornell, 'Contracts *Ex Machina*' (n 1).

[7] We should not confuse or equate enforceability with guaranteed performance in the context of smart contracts. These concepts should not be collapsed. The technology automatically implements the terms of an agreement or performs the contractual clauses. This is different from the enforcement of a contract in a legal sense. Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9 *Law, Innovation and Technology* 269, 280.

[8] See a variety of different definitions e.g. in Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (n 1); Vitalik Buterin, 'DAOs, DACs, DAs and More: An Incomplete Terminology Guide' (2016) Ethereum Blog (6 May 2014) <https://blog.ethereum.org/2014/05/06/daos-dacsdas-and-more-an-incomplete-terminology-guide/> accessed 14 April 2017; Rob Marvin, 'Blockchain in 2017: The Year of Smart Contracts' (2016) *PC MAG* (12 December 2016) <http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts> accessed 12 June 2017; The Economist, 'Not-so-clever Contracts' (2016) <http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted> accessed 11 July 2017.

[9] This definition is similar to the definitions provided in Werbach and Cornell, 'Contracts *Ex Machina*' (n 1), Wright and De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 2) 10-11, and Max Raskin M, 'The Law and Legality of Smart Contracts' (2017) 1 *Georgetown Law and Technology Review* 305, 309 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166> accessed 11 July 2017.

[10] Wright and De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 2) 11.

[11] Henry Kim and Marek Laskowski, 'A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange' (2017) <http://blockchain.lab.yorku.ca/files/2017/05/UBC_blockchain_paper_HK_and-Marek.pdf> accessed 11 July 2017.

[12] ibid.

[13] ibid.

[14] Vitalik Buterin, 'On Public and Private Blockchains' (2015) Ethereum Blog <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> accessed 11 July 2017.

mechanism, for example mining in the case of bitcoin)[15] can be designed in different ways depending on the type of the blockchain needed for the particular purpose.

The choice between operating a public or permissioned blockchain has implications for:

1. The identifiability of persons transacting on blockchain,
2. The selection of nodes and size of network as well as the related expenses,
3. The particularities of the consensus mechanism and
4. The transaction transparency of the content of the blocks.

Let us describe the different types of blockchains based on these four characteristics.

2.2.1. *Public blockchains*

The most prominent example of a public blockchain is bitcoin. In the case of bitcoin, the underlying blockchain is a truly public space.

1. *Identifiability:* On a public blockchain, anyone can make use of it and join the network anonymously.[16] As a result, for example, the identity behind a bitcoin public key can be difficult to establish.
2. *Selection of nodes:* Any computer can become a node in the network. The reliability of nodes and the growth of the blockchain network is difficult to control. Not having restrictions on who can participate can pose challenges if changes in governance of the blockchain are necessary, as the consensus from a majority of servicing nodes will be required to implement any rule changes.[17]
3. *Consensus:* On a public blockchain, anyone can participate in the consensus mechanism. In the case of bitcoin, we use so-called proof-of-work as consensus mechanism. Proof-of-work requires participants in the consensus mechanism ('miners') to compete against each other in solving computationally-intensive mathematical problems in the process of validating a transaction and adding a block to the blockchain. In order to incentivize individuals to provide computational power for the validation of transactions,[18] miners are rewarded in bitcoin for servicing the bitcoin network. The proof-of-work mechanism makes the bitcoin network secure against fraud or corruption, and its security grows with the number of miners. As an alternative to proof-of work, many blockchain entrepreneurs (including those working on smart contracts) attempt to achieve validated transactions with the proof-of-stake consensus mechanism, which is less demanding in terms of resources, but provides a comparable level of security. In case of proof-of-stake, the creator of a new block is chosen in a deterministic way, depending on its wealth. Since there is no block reward for creating the new block, the creators take transaction fees (and for that reason are not called miners but validators or forgers). One should keep in mind that in case of proof-of-work, not having restrictions on who can participate in the consensus mechanism can offer a good defence against hacking (bad actors are cut out thanks to technological and economic disincentives). For similar defence, the proof-of-stake mechanism needs to implement a different algorithm which disincentivizes hacking (bad actors are cut out thanks to economic disincentives).[19]
4. *Transaction transparency:* Public blockchains have a high degree of transparency. Anyone can read the content of the blocks on the bitcoin blockchain. While this might not be problematic in case of bitcoin, the openness/transparency of public blockchain can pose a challenge if the content of blocks contains sensitive information.[20]

It has been considered an important advantage of blockchain technology - particularly when it comes to a public blockchain - that the transactions it facilitates are public and shared. This creates transparency which has been considered to support the trustworthiness and security of the technology for accounting for transactions. At the same time, privacy is protected to an extent since users' identity is hidden behind pseudonyms. By allowing a countless number of parties to maintain a correct record of their transactions it also allows them to get rid of some unfavorable middlemen with their own agendas and interests.[21] It would certainly be exaggerative to maintain that all middlemen, due to being centralized or powerful, are unfavorable. In many cases they offer a certain level of convenience and, much like miners implementing the consensus process, perform a valuable service for reward.[22] Yet, where middlemen do become unfavorable, the technology has the potential to replace them with algorithms.

[15] Joseph Bonneau and others, 'SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies' (2015) *2015 IEEE Symposium on Security and Privacy* (IEEE 2015), 104.

[16] For further explanations on the nature of anonymity on public blockchains see Section 2.1. below.

[17] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018) 36.

[18] The payment to miners in bitcoin acts as market-based mechanism to overcome an otherwise ensuing tragedy-of-the-commons problem. Since a public blockchain has public good characteristics, nobody would be willing to service the bitcoin network in the absence of payment.

[19] Bonneau and others, 'Research Perspectives and Challenges for Bitcoin and Cryptocurrencies' (n 15).

[20] This could be for example the case for information about individuals in healthcare applications based on blockchain.

[21] There are arguably still middlemen left, for example the miners that help implement the consensus process. Nonetheless, single miners lack the central power of intermediaries that blockchain could replace, such as banks, public administration, and large internet intermediaries.

[22] We reflect the excellent well-balanced point of view of middlemen expressed by our reviewer here. For a thoughtful analysis of whether or how blockchains and smart contracts could bypass traditional principal-agent dilemmas of organizations, which are among else characteristic of the problems faced with middlemen, see Shermin, 'Disrupting Governance with Blockchains and Smart Contracts' (n 2), and Arruñada B. Blockchain's struggle to deliver impersonal exchange. *Minn J Law Sci Technol* 2018;19:55 https://ssrn.com/abstract=2903857 or http://dx.doi.org/10.2139/ssrn.2903857 accessed 16 August 2018.

One of the well-known platforms of smart contracts on public blockchains is Ethereum.[23] Some of its possible applications include money management (the creation of cryptocurrencies), other financial apps (crowdfunding and crowd sales), voting systems and governance systems, including decentralized autonomous organizations. Ethereum was developed against the backdrop that all other blockchain projects after Bitcoin had been based on specific protocols aimed at providing financial services or tools for enhanced cryptocurrencies. While other projects had taken off using the Bitcoin infrastructure to provide different applications, such as Mastercoin and Counterparty, Ethereum's founder, Vitalik Buterin, aimed at providing a wholly new blockchain infrastructure that would allow for a much wider range of application than just cryptocurrencies.[24]

Consortium blockchains are blockchains that are used by a limited number of participants and designed to fit the needs of a particular industry.[25] Examples include the R3 Corda project[26] and Enterprise Ethereum Alliance.[27] In a consortium blockchain, a central entity determines who may act as a participant in the consensus mechanism which validates transactions, and writes them into the blockchain. Equally, that central authority can predetermine who can act as a user making transactions on the blockchain. As such, consortium blockchains are seen to deliver the advantages of trustworthiness and security while helping to meet some of the challenges that public blockchains pose for organizations.

The four characteristics of blockchain design of consortium blockchains differ from public blockchains.

1. *Identifiability:* Since blockchain participants must first be authorized to transact on the blockchain, their identities can be verified.
2. *Selection of nodes:* Only authorized machines can become nodes in the blockchain network. As validators are known and trusted by the consortium, and their number will be relatively small, reaching consensus is easier. This facilitates the changing of rules, the reversal of transactions or other modifications in the blockchain. Such increased flexibility can be a drawback, however, if the aim of a blockchain is absolute immutability to avoid any form of manipulation of the ledger.
3. *Consensus:* Since only selected participants can act as validators in the consensus mechanism and their number can be controlled, the consensus mechanism becomes cheaper and faster compared to a public blockchain. The consensus mechanism does not need to be as resource-consuming as proof-of-work, and since a smaller amount of nodes will be engaged in the consensus process, blocks will be added at higher speed to the blockchain.[28] Furthermore, it might be possible to do away with the necessity of an inbuilt market-based incentive mechanism in the consensus process (in case of bitcoin this incentive is the reward in bitcoins to miners), which is always needed in a public blockchain system.[29]
4. *Transaction transparency:* Consortium blockchain designers can choose to hide the content of blocks on the blockchain and make it available only to certain users affected by a specific transaction. Privacy issues posed by wholly public blockchains can thus be avoided.[30]

Private blockchains are blockchains which are entirely managed by a single organization, a group of people, or a single person. While they generally share the properties of consortium blockchains, when operating wholly private blockchains, the decentralized nature of system is lost. The operators continue to benefit from the other advantages of the use of blockchain technology, e.g. the ability to maintain data integrity and the correctness of transactions. As Buterin puts it, a private blockchain is however little more than 'a traditional centralized system with a degree of cryptographic auditability attached'.[31] An example of a wholly private blockchain is JP Morgan's experiment with Quorum (an Ethereum-based permissioned blockchain architecture) in its internal Global Network Payments initiative.[32]

[23] Ethereum was founded in 2014 and describes itself as 'a Next-Generation Smart Contract and Decentralized Application Platform'. See 'Ethereum White Paper. A next-generation smart contract and decentralized application platform, https://github.com/ethereum/wiki/wiki/White-Paper; 2017 accessed 11 July 2017.

[24] Vitalik Buterin, 'Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform' (2014) *Bitcoin Magazine* 23 January 2014 <https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/> accessed 11 July 2017.

[25] Buterin 'On Public and Private Blockchains' (n 14).

[26] Richard Gendal Brown, 'Introducing R3 Corda: A Distributed Ledger Designed for Financial Services' (2017) <http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services> accessed 11 July 2017.

[27] Enterprise Ethereum Alliance, https://entethalliance.org/about/; accessed 11 July 2017.

[28] Buterin, 'On Public and Private Blockchains' (n 14).

[29] De Filippi and Wright, *Blockchain and the Law: The Rule of Code* (n 17) 32.

[30] Buterin, 'On Public and Private Blockchains' (n 14).

[31] ibid.

[32] Morgan JP. Distributed ledger technology, https://www.jpmorgan.com/global/distributed-ledger-technology; 2017 accessed 11 July 2017. The Keyless Signature Infrastructure (KSI) blockchain technology that has been used by the Estonian government next to the traditional public key infrastructure (PKI) is another example of using the underlying time-stamping technology by an organization, in this case a state . The KSI is currently used to preserve the integrity of several vital registries (business registry, land registry, e-health records) in Estonia. There are several advantages of doing this in governance, even if the use of non-public blockchain does not provide all the acclaimed advantages of a public blockchain. It empowers citizens as each citizen gains an ability to verify the integrity of their records at government databases at will, independently of the government or any other third party. It creates government accountability as the KSI makes it impossible for privileged insiders to perform illegal acts inside the government networks, and erase the log evidence pointing to their actions without it being immediately evident. It also provides long-term data integrity thanks to the fact that KSI is based solely on hash-function cryptography, and as such it will not be vulnerable to attacks utilizing quantum computing, unlike RSA-based digital signature schemes. For details on the technology, see Buldas A, others. Keyless signatures

Table 1 – The use of smart contracts on permissioned blockchains across industries.

Industry	Problem	Solution	Examples
Banking	Clearing and settlements through intermediaries is slow and very costly.	Smart contract system helps to eliminate intermediaries, as e.g. central banks, correspondent banks, clearing houses	R3 Corda[a] Ripple[b]
Public Health	Sharing of health care data poses privacy threats for patients, inter alia due to current centralized structures of healthcare data collection	Smart contract system helps to protect privacy while allowing sharing of aggregated data to improve national health care delivery priorities	ModelChain[c]
Supply Chain	Loss of goods, insurance fraud, authenticity of high value goods, evaluation of provenance	Smart contract system would create immutable record of goods along supply chain[d]	Everledger[e]
Music Royalties	Up to 50% of music royalty payments are not received by right owners[f]	Blockchain system could help to create a world-wide database of music metadata,[g] which could then in turn be used to trigger automatic royalty payments to rightholders through the deployment of smart contracts	So far only preliminary proposals[h]

[a] It should be noted that R3's CTP claims that Corda is *not* a blockchain. See Brown (n 26). It could be argued, however, that it simply is a special type of permissioned blockchain.

[b] Similarly to the case in R3 Corda, Ripple does not claim to be a blockchain system - nonetheless the architecture of its network is a form of a permissioned blockchain. See Ripple, 'Technology' <https://ripple.com/technology/> accessed 11 July 2017.

[c] Tsung-Ting Kuo and others, 'ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modelling Framework on Private Blockchain Networks' (2016) ONC/NIST Blockchain in Healthcare and Research Workshop, Gaithersburg, MD, September 26-7, 2016 <https://www.healthit.gov/sites/default/files/10-30-ucsd-dbmi-onc-blockchain-challenge.pdf> accessed 11 July 2017.

[d] Kim H, Laskowski M. Towards an ontology-driven blockchain design for supply chain provenance. Proceedings of the Conference Paper for Workshop on Information Technology and Systems (WITS), 2016. https://arxiv.org/abs/1610.02922 accessed 11 July 2017.

[e] See for example London-based start up Everledger, https://www.everledger.io/; 2017 accessed 11 July 2017.

[f] Libby Botsford, 'BerkleeICE's Rethink Music Releases Report on Transparency and Fairness in the Music Industry' (2015) <https://www.berklee.edu/news/fair_music_report> accessed 11 July 2017.

[g] Music Business Worldwide, 'ASCAP, PRS and SACEM Join Forces for Blockchain Copyright System' (2017) <https://www.musicbusinessworldwide.com/ascap-prs-sacem-join-forces-blockchain-copyright-system/> accessed 11 July 2017.

[h] Wallach DA. Bitcoin for rockstars. *Wired* 2014. 12 October 2014 https://www.wired.com/2014/12/bitcoin-for-rockstars/. accessed 11 July 2017, Music Business Worldwide (n 39).

In different industries, smart contracts on permissioned blockchains have been used to propose specific solutions to particular problems: see Table 1.

After this outline of the different options of smart-contract and blockchain design, we will focus for the rest of our analysis on bilateral or multilateral smart contracts that represent a translation of a specific contractual agreement with legal force into code. Furthermore, we will mainly focus on smart contracts on public blockchains as they present a unique trust relationship between the participants as well as more challenges from a regulatory perspective, in particular due to the possible anonymity or pseudonymity of public blockchain users. In order to still provide a comprehensive picture of the blockchain landscape, discussions on permissioned blockchains will be included in the analysis to illustrate some of their advantages over public blockchains from a regulatory perspective.

2.3. *The assessment of smart contracts in legal literature*

While industry appears enthusiastic about adopting smart contracts, legal scholars have adopted a more cautious position. This section provides a review of recent literature on smart contracts published in law journals. Significant parts of it try to evaluate smart contracts from a contract law perspective.[33] This literature highlights shortcomings of smart contracts compared to traditional, court-enforced contracts.

Most legal scholars recognize that smart contracts could, in theory, reduce transaction costs and increase efficiency in contracting.[34] Some legal scholars have even placed a strong

infrastructure: how to build global distributed hash-trees. In: Nielson HR, Gollmann D, editors. Secure IT systems. Springer; 2013 https://eprint.iacr.org/2013/834.pdf accessed 11 July 2017.

[33] Alexander Savelyev, 'Contract Law 2.0: 'Smart' Contracts As the Beginning of the End of Classic Contract'(2017) 26 Law. *Information & Communications Technology Law* 116; Werbach and Cornell, 'Contracts Ex Machina' (n 1); Raskin, 'The Law and Legality of Smart Contracts' (n 9), Cuccuru P. Beyond Bitcoin: an early overview on smart contracts. *Int J Law Inf Technol* 2017;25:179; Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (n 7); Mark Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective' (2017) 33 *Computer Law and Security Review* 825.

[34] Cuccuru, for example, mentions a reduction in risk of non-compliance and a reduction of the likelihood of costly litigation. See Cuccuru, 'Beyond Bitcoin' (n 33) 187. Others mention

emphasis on the benefits deriving smart contracts,[35] in particular from a data and consumer protection perspective.[36] Many, however, consider smart contracts problematic for various reasons. The problems identified mainly derive from the fact (a) that smart contracts need to be translated in computer code, (b) no ex-post modification or deliberate breach is possible once a smart contract is placed on the blockchain, and (c) that smart contracts may not comply with mandatory rules in contract law. Let us elaborate on each of these critiques.

2.3.1. *Translation into code*

Smart contracts need to be written in code. The agreement between two parties thus needs to be translated from human to computer language, which requires the involvement of computer scientists for the creation of smart contracts. This leads to a critique of the claim that smart contracts reduce costs because compulsory involvement of computer scientists would reintroduce an instance of intermediation that could possibly neutralize efficiency gains from automation.[37]

Further concerns are raised regarding the reduction of possible contractual expressions to computer-readable instructions. Computer language eliminates the possibility of introducing vague contractual terms that are often employed in traditional contracts and allow for a flexible interpretation of contract performance, such as duties of good faith[38] or standards of best efforts.[39] As put by Mik, '[*p*]rogrammers fail to recognise that in contract law, ambiguity is a feature not a bug'.[40] Coding of contracts precludes contractual parties to adopt clauses that allow for desirable and necessary flexibility that allows for adaptations of contracts to unforeseeable future scenarios.[41] Others, however, point to the advantages of reduced ambiguity provided by terms drafted in computer language, that could lead to a reduction in misunderstandings and disputes.[42]

Another problem that comes with the encoding of smart contracts is the high likelihood that their code might not run as envisaged.[43] The code of any minimally sophisticated smart contract is likely to contain bugs, like any other computer programme, that will result in malfunctions.[44] In light of this problem, it is argued that the perfect execution of a smart contract would be a myth in practice.[45]

In case any problems in relation to a smart contract arose, possibly leading to a court case, it is mentioned as a further problem that judges would be incapable of understanding the content of a smart contract.[46] As a result, the costs and length of legal proceedings relating to smart contracts would increase due to the need of experts to decipher the terms of smart contracts.[47]

2.3.2. *Automated performance of smart contracts*

A further problem regularly discussed in relation to smart contracts from a contract law perspective is the immutable nature of smart contracts once placed on the blockchain. Since smart contracts are understood as 'unstoppable' due to their self-executing nature, neither the parties nor courts can intervene ex-post.[48] This means that remedies of traditional contract law are unavailable in case a smart contract executed wrongly, including injunctive relief[49] and self-help.[50]

Furthermore, even if a smart contract executes as foreseen, parties are incapable of breaching the contract even if it were efficient. Several authors point to the fact that smart contracts eliminate the possibility of efficient breach.[51] Deliberate and socially desirable non-performance of smart contracts is thus impossible, potentially causing welfare losses.

Lastly, there appear to be no feasible technical solutions to remedy automated performance gone wrong. Werbach and Cornell point out that the implementation of a hard fork[52] splitting the blockchain is no good remedy to a smart contract that malfunctions. In their words, 'a hard fork stands or falls on whether a majority of the mining power in the blockchain network adopts it. This is not how contracts work. We do not adjudicate disputes through opinion polls or the ballot box'.[53] At the same time, however, it should be noted that many smart contracts placed on the Ethereum and other public blockchain contain a 'kill switch' in their code that can stop the smart contract.[54] There are thus other types of remedies that could

disintermediation by smart contracts as a main factor of cost reduction in contracting. See, for example, Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41)..

[35] Trevor I. Kiviat, 'Beyond Bitcoin: Issues in Regulating Blockchain Transactions' (2015) 65 *Duke Law Journal* 569, 574.

[36] Joshua Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection' (2014) 71 *Washington and Lee Law Review Online* 35.

[37] Cuccuru, 'Beyond Bitcoin' (n 33) 188.

[38] Giancaspro, ' Is a 'Smart Contract' Really a Smart Idea?' (n 41) 832.

[39] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 365.

[40] Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (n 7) 292.

[41] ibid

[42] Raskin, 'The Law and Legality of Smart Contracts' (n 9) 324; Cuccuru, 'Beyond Bitcoin' (n 33) 187.

[43] Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 830.

[44] Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (n 7) 281, 293.

[45] ibid, 281.

[46] Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 832; Cuccuru, 'Beyond Bitcoin' (n 41) 11.

[47] Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 834.

[48] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 318, 361.

[49] Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 833.

[50] ibid

[51] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 366; Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (n 7) 283.

[52] A hard fork is a radical change to the blockchain protocol, which results in previous valid blocks being turned invalid. In this sense the effects of a wrongly executed smart contract could be rolled back. For a useful definition and visualization of the concept of hard fork on Investodpedia see <https://www.investopedia.com/terms/h/hard-fork.asp> accessed 2 February 2018.

[53] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 374. The radical remedy that was implemented to deal with the malfunction of the DAO could thus not be a general remedy against wrongly performed smart contracts.

[54] Massimo Bartoletti and Livio Pompianu, 'An Empirical Analysis of Smart Contracts: Platforms, Applications and Design Patterns'

be built into the code of the smart contract to mitigate the apparently non-mutable nature of smart contracts.

2.3.3. *Invalid and illegal smart contracts*

A last risk posed by smart contracts mentioned by several scholars is the fact that none of the safeguards provided by traditional contract law are in place for smart contracts. Since parties can contract anonymously on the blockchain, any problems with lack of capacity could not be cured.[55] A contract that would be deemed invalid under traditional contract law would thus execute if implemented as smart contract. This would equally apply in case of violations of other mandatory rules found in traditional contract law regarding, for example, duress, mistake or fraud.[56]

Furthermore, no safeguards against illegal smart contracts are in place.[57] Some authors draw parallels to bitcoin and the Silkroad incident to make a general point about how blockchain applications are prone for being used for illegal purposes.[58]

2.3.4. *Other critiques*

There are further critiques that can be found in legal literature about smart contracts. One regards the problems that can arise due to smart contracts having to rely on third-party sources, so-called oracles, to verify whether a relevant event for the smart contract has occurred in the real world.[59] Many authors point out that the reliance on sources external to the blockchain that could be manipulated introduces an element of uncertainty in the execution of smart contracts, damaging their apparently perfect reliability.[60]

Yet another critique regards the scalability of using smart contracts, since the energy resources needed to sustain a growing blockchain system might not be available or disproportionately wasteful.[61] This critique has already been made in relation to bitcoin,[62] and it would apply equally to public blockchains for smart contracts.

Lastly, when it comes to assessing smart contracts from a relational perspective, Levy criticizes that they cannot replicate the relational context in which contracts are usually concluded.[63] She argues, in line with relational contract theory, that contracts are social tools and are not always meant to be performed according to their letter. At times parties include deliberately unenforceable and vague terms in their contracts which are only meant as rough guidelines for behaviour. Furthermore, parties sometimes decide wilfully not to enforce a contract that has been breached by the other party in order to ensure a continued relationship. Automated implementation of the terms of smart contracts might foreclose such relational uses of contract.

3. The law and economics of smart contracts

In contrast to existing discussions about smart contracts by legal scholars, we aim at framing the debate around smart contracts from a law and economics of contracts perspective. The discipline of law and economics takes legal reality and analyses it from an economic efficiency perspective.[64] The area of contract law has been of particular interest to law and economic scholars, because it is the legal regime that applies to agreements between parties which underpin trade. Trade, in turn, is a socially desirable activity because it increases economic welfare.[65] The economic function of contract law is considered to be the prevention of inefficient opportunistic behaviour between parties engaged in economic exchange. The coercive nature of law, obliging parties to fulfill their contractual obligations, has been seen to ensure sustained cooperation in exchange.[66]

(2017) 11 <https://arxiv.org/pdf/1703.06322.pdf> accessed 2 February 2018.

[55] Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 829; Werbach and Cornell, 'Contracts Ex Machina' (n 1) 371.

[56] Cuccuru, 'Beyond Bitcoin:' (n 33) 191. Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 829; Werbach and Cornell, 'Contracts Ex Machina' (n 1) 368, 369.

[57] Werbach and Cornell refer as an example of an illegal smart contract to a price-fixing smart contract in breach of antitrust laws. See Werbach and Cornell, 'Contracts Ex Machina' (n 1) 373.

[58] See, for example, Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 835.

[59] For a definition of oracles see Section 1.1 above, in particular footnote 11.

[60] Cuccuru, 'Beyond Bitcoin' (n 33) 186; Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (n 7) 297.

[61] Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41) 835.

[62] See, for example, Kaminska I. The environmental costs of Bitcoin are not worth the candle. *Financ Times* 2017. 7 November 2017 https://www.ft.com/content/c166aa1e-c303-11e7-a1d2-6786f39ef675/. accessed 22 November 2018; Tirole J. There are many reasons to be cautious about Bitcoin. *Financ Times* 2017. 30 November 2017 https://www.ft.com/content/1c034898-d50f-11e7-a303-9060cb1e5f44/. accessed 22 November 2018; Badkar M. Bitcoin energy demand in 2018 could match Argentina – Morgan Stanley. *Financ Times* 2018. https://www.ft.com/content/93b22cb1-0346-38be-bebf-d2e676e19621/. accessed 22 November; Kobie N. How much energy does Bitcoin mining really use? It's complicated. *Wired* 2017. 2 December 2017 https://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use/. accessed 22 November 2018.

[63] Karen E. C. Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law' 3 *Engaging Science, Technology and Society*(2017) 1 <https://doi.org/10.17351/ests2017.107> accessed 11 July 2017.

[64] Richard Posner, *Economic Analysis of Law* (8th edition, Aspen Publishers 2011) 29.

[65] Benjamin Hermalin, Avery Katz, Richard Craswell, 'Contract Law' in A. Mitchell Polinsky and Steven Shavell (eds), *Handbook of Law and Economics* (Elsevier 2007) 7 <http://www.sciencedirect.com/science/handbooks/15740730> accessed 11 July 2017.

[66] In the absence of enforceable contracts, game theory predicts that in cases other than immediate exchanges, i.e. when there is a time gap between the agreement and its performance, each party will be reluctant to perform its part out of fear that the other party will appropriate it without counter performing (this applies in the case of one-shot games or repeated games played for a fixed number of rounds). As both parties expect the other not to perform in the absence of enforceable contracts, no economic exchange occurs. Contract law provides a solution to this prisoner's dilemma. See Robert Cooter R and Thomas Ulen, *Law and Economics* (6th edition, Pearson 2012) 285.

3.1. *Three contracting environments*

Law and economics literature on contracts is concerned with mechanisms that bring about the optimal amount of cooperation in economic exchange between individuals.[67] Within the field of law and economics of contracts, two broad discussions of these mechanisms can be distinguished: one relating to black-letter contract law and another relating to other social mechanisms that induce cooperation among individuals.[68] For the purposes of this article we will refer to these two strands of academic discussion as 'black-letter/legal' and 'relational'.

These two different strands of discussion within the field of law and economics of contracts can make us think of two different environments in which contracting can take place: black-letter law and relational contracting environments. These two contracting environments are not strictly separate, but it is recognized that each has its particularities for how contracting between parties works.

A commonality between legal and relational accounts of contracting is that 'trust' is considered as a necessary facilitator for parties to cooperate and to enter into commercial relations.[69] Whether trust is defined as a form of calculation about how others will act before one can monitor their actions,[70] as complexity-reducing lubricant that lowers transaction costs,[71] whether it is linked with a building of reputation through repeated interactions,[72] or with as a contextual factor provided by a certain environment for trading,[73] the presence or absence of trust determines whether contracting occurs, or not.

In a legal contracting environment, parties can *ex ante* draft contracts to include all necessary terms regarding performance and other obligations that will dictate remedies imposed by courts in case of performance failure. In a relational context, it is the social norms of a community, such as business custom or religious rules, that determine contract formation and enforceability. Additionally, in both environments a variety of enforcement tools are available *ex post* for ensuring that agreements are fulfilled. More generally, the environments differ in terms of the proactive and reactive mechanisms used for enforcing contracts, as well as in terms of the trust underpinning relationships between the contracting parties. We will discuss both grounds for distinction in detail below.

Before we go into detail, however, it is worth noticing that with the fast development of technologies we have a reason to start talking about a third contracting environment from the perspective of law and economics. We call it blockchain's no-trust contracting environment and relate this particularly to public blockchains. It is an environment with no particular pre-existing social or legal context to embed contracts. In an environment where there are no pre-existing business or family ties and no common cultural references, there is likely to be no trust coupled with no fear of losing reputation that would induce cooperation. Based on the standard operating principles of markets and legal environments, the nearly complete anonymity between parties which is part of the general mechanisms of public blockchain,[74] provides precisely such an environment and should be a red flag for anyone wishing to draw up and execute a contract (e.g. a contract operating on a blockchain).[75] In other words, when you have anonymity and other legal or relational enforcement mechanisms are weak or not available, you have the paradigm set of circumstances for a no-trust environment for contracting which is different from legal or relational contracting environments. In order to contract in no-trust environments, there is a need for an enforcement mechanism which provides sufficient safeguards for contracting. In such a setting, the weak or unavailable contract law would initially appear to be the only available option to ensure cooperation in economic exchange. Let us consider all the options.

What is the best way to understand the extent of anonymity on public blockchains? We will explain this with an example of bitcoin because it operates on a public blockchain, just like smart contracts, and the matters of anonymity are the same.[76] The transfer of bitcoins is anonymous to some degree. On a higher level, a bitcoin transaction has the following properties. Anyone who knows the private key of the sending address can perform a transaction to another address. All transactions are public, that is, the complete transaction ledger can be accessed by any person on the Internet. In the ledger, bitcoin addresses are represented by numbers (that is, public keys). No connection

[67] Ganuza J, Gomez Pomar F. The strategic structure of contract law. Book Draft on file with the authors 2017.

[68] For a similar distinction, that however sub-divides non-legal cooperation mechanisms into kinship, selfish cooperation, altruism and reciprocity in long-term relationships, see Ganuza and Gomez Pomar, 'The Strategic Structure of Contract Law' (n 75) Chapter 1. Similarly also Posner, who distinguishes between contract law as a mechanism to fuel voluntary exchange, and other mechanisms to enforce contracts such as reputation, altruism, reciprocity. See Posner,. *Economic Analysis of Law* (n 72) 96.

[69] As remarked in general terms by Arrow: 'Virtually every commercial transaction has within itself an element of trust, certainly any transaction conducted over a period of time. It can be plausibly argued that much of the economic backwardness in the world can be explained by the lack of mutual confidence'. See Kennet Arrow, 'Gifts and Exchanges' (1972) 1 *Philosophy & Public Affairs* 343, 357.We further elaborate on the notion of trust in various contracting environments in Section 2.3.

[70] Partha Dasgupta, 'Trust as a Commodity' in Diego Gambetta (ed), *Trust: Making and Breaking Cooperative Relations* (Blackwell, 1988) 49, 51.

[71] Edward H. Lorenz, 'Neither Friends Nor Strangers: Informal Networks of Subcontracting in French Industry' in Diego Gambetta (ed.). *Trust: Making and Breaking Cooperative Relations* (Blackwell 1988) 194, 198.

[72] Dasgupta,'Trust as a Commodity' (n 78) 53.

[73] Oliver E. Williamson, 'Calculativeness, Trust, and Economic Organization' (1993) 36 *Journal of Law and Economics* 453, 476.

[74] On public blockchains, see Section 1.2. above.

[75] As stated above (see Section 1.1.), while smart contracts do not necessarily operate on a blockchain, in this paper we limit our discussion to those smart contracts that do operate on blockchains, with particular focus on those that operate on public blockchains.

[76] This explanation of anonymity in this section derives from an earlier unpublished analysis that one of the authors carried out for the Supreme Court of Estonia together with Dominique Unruh, see Helen Eenmaa-Dimitrieva and Dominique Unruh, 'Report on the Architecture and Anonymity of Bitcoin Transactions for the Supreme Court of Estonia' (2016).

between physical or legal persons and the bitcoin addresses is maintained. While the bitcoin system does keep track of bitcoin addresses, it does not keep track of address ownership (whoever has the private key controls the address). Since it does not keep track of ownership, the address to which the bitcoins are transferred or from which they come do not have to belong to the given client. In particular, the facilitator cannot record the identity of the owner of the address.

However, anonymity is not absolute. Since all money flows are publicly visible in the public bitcoin ledger, it can be possible to use statistical tools to guess at the identity of the owner of a given bitcoin address. A user that wishes to maintain his anonymity can hide the money flows by transferring the money to a so-called 'mixing service' which collects money from many users and redistributes the money to other, otherwise unrelated addresses of the same users.[77] This allows obfuscating the money flow from one address to another, making the bitcoin address anonymous. The key idea is that Bitcoin addresses are not bound to user identities, but the anonymity of bitcoin addresses can nevertheless be broken in some cases. This can be avoided by the use of mixing services.

When it comes to the exchange of bitcoins, we should keep in mind that the facilitator of an exchange does not have the possibility to record whose bitcoin address he is transferring money to or from, but he can record which bitcoin address the money is transferred to. The facilitator of an exchange can also record information about the identity of the person getting or paying the normal currency if the normal currency is transferred in a way that is not anonymous. The anonymity depends on the mechanism used. For example, in a cash payment, anonymity is achievable, while a bank transaction will usually reveal the name of the client.

Is it possible for the facilitator of the exchange of bitcoins to save data about its clients and verify the identity of the clients? Many organizations and services such as online stores that accept bitcoins and facilitator of the exchange have access to identifying information regarding their users, e.g. e-mail addresses, shipping addresses, credit card and bank account details, IP addresses, etc.[78] In an exchange of bitcoins for normal currency or vice versa, the facilitator can save data about the identity of the person with which the transfer occurs. In this case, the data is collected and stored not under the bitcoin protocol and rules. Such information is not recorded in the blockchain. Online merchants and facilitators of the exchange are expected to collect and store the data according to the applicable laws and their policies. The regulations and policies extend only to situations where the bitcoins are exchanged for traditional currencies or goods.

There are facilitators of exchange of bitcoins that require no identifying information from their users and these facilitators are popular among users not wishing to share their personal information. It is the choice of user which facilitator of the exchange to choose. At the same time, even if the facilitator has chosen and declared not to collect any identifying information, it still has huge amounts of information recorded in the blockchain. This includes a traceable trail of each transaction. The facilitator is able to record to which and from which bitcoin address the bitcoins flow, but the facilitator cannot ensure that the address belongs to the same person as the one transferring the normal currency. Of course, despite the fact that the information is not linked to a particular user it could still be used to identify parties to the transaction. In sum, operating on a public blockchain can be to a great extent anonymous, even if the anonymity is not absolute.[79]

To some extent, similar forms ofanonymous transactions can be found in other online environments too, e.g. when agreeing to the terms of a software package before downloading it. If it is paid software, however, a credit card transaction would still record a great deal of information both about the card holder and the merchant. In the case of freeware, the software provider could still find out a considerable amount of information such as the location, repeat visits, how a user got to its page, etc. Furthermore, the provider can subsequently track a user. Much less of such information would be available in a public blockchain environment, providing thus for a higher degree of anonymity.

Until recently, such anonymity would provide for the paradigm set of circumstances where, for concluding agreements and sustaining trade, we would imagine needing a reliable system of contract law (or other legal mechanisms) in order to compensate for the challenges posed by greater risk for negative outcomes, bad faith, inability to track down the other party and general distrust.[80] This is because, due to anonymity, the contracts concluded in such circumstances would not be embedded in any social context that could work as an alternative enforcement mechanism to ensure that all parties cooperate.[81]

There is a need for a tool which facilitates contracting in such environments where, due to the anonymity between parties, one would need contract law or other enforcement mechanisms as tools for contract governance, but those are not available or reliable for various reasons. Speaking of reliability, for example, in case of anonymity, even if there is contract law, we do not know the identities of the parties to the contract. A potential plaintiff might thus not be able to find the

[77] De Filippi and Wright, *Blockchain and the Law* (n 17) 66. Newer forms of cryptocurrency that have evolved from bitcoin such as Zcash can also provide for anonymous transactions, due to improved cryptographic techniques.

[78] Fergal Reid and Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System' in Yaniv Altshuler and others (eds), *Security and Privacy in Social Networks* (Springer 2013) 197-223 <https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf> accessed 11 July 2017.

[79] Eenmaa-Dimitrieva and Unruh (n 84).

[80] In the terminology of Dixit, we would need state-provided contract law if a community grows too large (or information travels too slowly) to sustain honesty. In other words, with growing anonymity we would expect a shift from relation-based to rule-based governance. See Avinash Dixit, *Lawlessness and Economics: Alternative Modes of Governance* (Princeton University Press 2007), Chapter 3. For the distinction between relation-based to rule-based governance, see John Shuhe Li, 'Rule-based Versus Relation-based Governance: An Explanation of the East Asian Miracle and Crisis' (2003) 11 *Review of International Economics* 651.

[81] Eenmaa-Dimitrieva H, Schmidt-Kessen MJ. Session 10: Smart Contracts, Course on the Law and Economics of Contracts at Fundação Getúlio Vargas in Rio de Janeiro. 2017.

defendant. This deters from contracting unless a suitable and reliable contract enforcement mechanism is provided.

While a no-trust contracting environment - paradigmatically arising when anonymity is coupled with weak or unavailable law or community based enforcement mechanisms - differs from legal or relational contracting environments, these environments may overlap with each other. We view anonymity as one of the defining features of a no-trust contracting environment, but the same kind of anonymity exists also in legal and relational contracting environments, weakening, however, the enforcement mechanisms that are characteristic for these environments. While the three contracting environments overlap with each other to some extent, contracting between parties works differently in each of them. We distinguish between the environments by reference to their enabling contract enforcement mechanisms and the relationships of trust that help them flourish.

3.2. *Enforcement mechanisms*

Voluntary exchange is based on a functioning system of contract enforcement. As put by Posner, 'a system of unenforceable contracts would not be efficient'.[82] There are a variety of mechanisms for contract enforcement available. We discuss three of them in turn.

3.2.1. *Contract law*

In what we term black-letter law or legal contracting environment, agreements that fulfil the criteria of contract law to bring into existence a legally binding agreement between parties that can be enforced in front of courts. From a law and economics perspective, the guiding principle for the legal rules on contract enforcement and available remedies is that parties should be bound by their agreements in as far as they 'maximize the joint surplus from their contractual relationship'.[83] The involvement of centralized state institutions, courts, is a key feature that sets contractual enforcement through contract law apart from other contracting environments.

3.2.2. *Community enforcement*

Studies in law and economics and other fields of social science have explained how social mechanisms other than contract law ensure cooperation between parties in economic exchange in the long term. We will take a look at a subset in the studies of social cooperation mechanisms which is generally referred to as relational contract theory.[84]

Cooperation in contracting can be achieved without relying on formal contract law. In his work *Lawlessness and Economics*, economist Avinash Dixit discusses, for example, how cooperation in a community of traders can be sustained in an environment of 'lawlessness', where there is no state-provided contract law or state-provided enforcement mechanism to enable cooperation (and avoid opportunism) in exchange transactions.[85] He provides a game theoretical model showing to what extent cooperation can take place in a community of traders without relying on formal contract law, and which parameters determine whether cooperation will be sustainable or break down. In Dixit's model, community enforcement of agreements within a group of traders that do not repeatedly interact with one and the same other trader (i.e. there is little direct reciprocity) depends on two factors.[86] Firstly, it depends on the transmission of information about a trader's behaviour to the rest of the group, which is determined by the size of the group, and by the technology of communication. If a group is small, information is likely to travel faster, but information in a large group can also travel fast if communication technologies allow for it (think of a twitter post that can instantly reach a large group of followers).[87] Secondly, enforcement depends on the willingness of others in the group to counteract misbehaviour.[88] In small groups, where information travels quickly, and due to education or socialization other group members are willing to sanction cheaters that do not fulfill their agreements, trade will be sustained without the need of contract law. Conversely, trade will likely break down in very large communities, where information about misbehaving members of the group is slow to spread, and in which there is no willingness in the group to punish deflecting members. In this case, another mechanism, such as formal contract law and public institutions enforcing contracts (or, as we argue, technology) would be necessary for economic exchange to flourish.

While Dixit shows how cooperation can be obtained in the complete absence of formal, state-provided contract law, the entire body of work on relational theory of contract shows that contracting parties often do not rely on formal contract law even if available to them.[89] Family ties, reciprocity in established long-term relationships, uncodified business customs or even altruism can act as incentives for actors to keep their promises. When creating exchange relationships, modifying agreements, or when settling disputes, contracting parties often prefer to rely on social mechanisms outside formal contract law to ensure continued cooperation.[90]

In contracting environments that rely on social ties, there exist social mechanisms that function as alternatives to formal contract law, which rely mainly on trust, honesty or reputation among the parties of a business community to enforce

[82] Posner, *Economic Analysis of Law* (n 72) 97.

[83] Ganuza and Gomez Pomar, 'The Strategic Structure of Contract Law' (n 75) 10.

[84] Important foundational works for the relational contract theory are Stewart Macaulay, 'Non-Contractual Relations in Business: A Preliminary Study.' (1963) 28 *American Sociological Review* 55 Ian Macneil, 'Relational Contract: What We Do and Do Not Know' (1985) 4 *Wisconsin Law Review* 483.

[85] Dixit, *Lawlessness and Economics* (n 88) Chapter 3.

[86] ibid 63.

[87] Ibid 65.

[88] Ibid 63.

[89] Ibid;. Ian Macneil, 'Contracts: Adjustment of Long-Term Economic Relations under Classical, Neoclassical, and Relational Contract Law' (1978) 72 *Northwestern University Law Review* 854; Jay M.Feinman, 'Relational Contract Theory in Context' (2000) 94 *Northwestern University Law Review* 737.

[90] The shorthand used by economists for such relational contracts is to define them as 'informal agreements sustained by the value of future relationships'. See George Baker, Robert Gibbons, and Kevin J. Murphy, 'Relational Contracts and the Theory of the Firm' (2002) 117 *Quarterly Journal of Economics* 39, 39.

agreements. Under certain conditions, these can prove to be more efficient than relying on formal contract law.[91]

3.2.3. *Enforcement through technology*

Blockchain's no-trust contracting environment for smart contracts offers a different alternative for contract enforcement: enforcement through technology. The code of a smart contract automates the performance of a contract between parties without any external human involvement.[92] Just as much as enforcement of relational contracts, enforcement of contracts through technology can take place in the absence of law but also in a legal environment. It is not the absence of law that makes these types of enforcement special but the different system of sanctions.

Does enforcement through technology really constitute a separate category of enforcement mechanism? Does it reduce opportunism in contracting in a fundamentally different way? For example, an objector could suggest that this type of enforcement reduces to the contract enforcement typical of relational contracting behaviour because the parties are guided by a relationship which they have formed in the blockchain environment by the means of the particular technology and the terms of their contract are enforced by the community of miners.

One of the reason why we nevertheless distinguish the technology-based contract enforcement mechanisms from the relational mechanisms is that they are tied to different underlying motivations for fulfilling one's contractual obligations. In case of relational contracts, one fulfils contractual obligations in the interest of one's reputation and sustained relationships in the particular community. In case of contracting in the environment of a public blockchain, nearly anonymously, one does not necessarily need to rely on such relationships or reputation and has accordingly no need to develop them in that context. Contracting could occur in the absence of a community willing to sanction cheaters, and no information channels would be necessary to pass on the news about a cheater. The blockchain provides an environment for coordinating the activities of 'distributed trustless individuals' and on the level of concluding contracts this is possible without the reputational incentive mechanisms.[93] The miners enforce the terms of the contracts only in the sense that they validate transactions and add blocks to the blockchain by solving mathematical problems.[94]

Another reason for distinguishing the enforcement mechanisms is that in case of enforcement mediated by technology the relationship between these individuals is based on a different kind of trust relationship than the one characteristic of relationships between parties of relational or legal contracts. We explain the differences between these trust relationships in detail in the following sections.

3.3. *Trust*

3.3.1. *First, second and third party trust*

Trade relies on trust. Two parties are likely to only engage in an economic exchange or in another form of market-based cooperation if they trust that each party will fulfil their obligations. When people are afraid of being cheated, they are less likely to engage in economic transactions.[95]

Prior to blockchain, two main mechanisms that helped to bring about the necessary trust for economic exchange existed: Peer-to-peer and Leviathan trust mechanisms.[96] Following Dixit, we could actually classify methods of contracts governance into first-party, second-party, and third-party systems to avoid opportunistic behaviour in contracting.[97] We suggest that this list is not complete and that there exists a fourth system with a different kind of trust underlying the governance of contracts.

As Dixit suggests, 'First-party systems operate on the potential cheater's own internal value system: either internal satisfaction or pleasure of behaving honorably, or an internalized sense of shame or guilt in cheating others. If individuals have such preferences, opportunistic behavior can be reduced or eliminated at the source and governance simplified. It is important to recognize prosocial preferences, not merely because they exist, but also because the intrinsic incentives they generate can interact with the standard monetary or other extrinsic incentives.' [98]

In the second-party or peer-to-peer trust environments, parties entering into an economic transaction trust that the other party will not behave opportunistically because there are social norms in place that will incentivize both parties to fulfil their obligations. Peer-to-peer trust environments are usually limited to close-knit communities that share a common background as e.g. a specific profession or trade, culture,

[91] Stewart Macaulay, 'Relational Contracts Floating on a Sea of Custom? Thoughts About the Ideas of Ian Macneil and Lisa Bernstein' (2000) 94 *Northwestern University Law Journal* 775.

[92] This presupposes that the smart contract's code contains no bugs and actually reflects the intentions of the parties. For a critique of this assumption see Sections 1.3.1. And 1.3.2. above.

[93] Shermin uses the phrase 'distributed trustless individuals' in Shermin, 'Disrupting Governance with Blockchains and Smart Contracts' (n 2) 502. She points out that blockchain and smart contracts can be used beyond their simpler applications for the decentralized governance of anonymous and distributed group of people. In case of such more complex applications, reputational incentive mechanisms could, of course, become important as well. Our focus in this paper is on the enforcement of contractual obligations and not on decentralized organizations. Accordingly, we continue to maintain that in these circumstances the reputational incentives are not necessary for contracting.

[94] ibid 506-7 ('A smart contract simply checks whether participants in a transaction comply with the rules pre-defined in the smart contract. If they do, the transaction is validated, if not, the transaction is rejected. They are auto-enforceable, but are also only as smart as the people who developed and audited them, based on the information available to these people at the time of coding.')

[95] Dasgupta, 'Trust as a Commodity' (n 78) 50; Avinash Dixit, 'Governance Institutions and Economic Activity' (2009) 99 *American Economic Review* 5 <https://www.princeton.edu/~dixitak/home/PresAd_F1.pdf> accessed 18 December 2017, 2.

[96] This terminology stems from Werbach K. Trustless trust, https://ssrn.com/abstract=2844409; 2017 accessed 14 August 2017.

[97] Dixit, 'Governance Institutions and Economic Activity' (n 88).

[98] ibid. Dixit refers here also to Roland Beńabou and Jean Tirole 2003.

language, family ties or religious beliefs. Fear of losing reputation will cause members of such a community not to behave opportunistically towards other members. This would be the type of trust at play within a relational contracting environment.

The third-party or Leviathan trust environments refer to trust that relies on centralized coercive power, an example being formal, government-enforced law. Even though two parties in a Leviathan trust environment might have no common community norms, they will engage in economic exchange if they trust the central coercive power to force parties to fulfil their obligations. This is the case, for example, when courts enforce contracts with the help of contract law. Leviathan trust (law) has come to fill in the trust gaps that have been left by decreasing peer-to-peer trust in today's societies.[99] This is the form of trust that we would expect in a black-letter law contracting environment, coupled with a well-functioning court system.

A form of Leviathan trust can also be generated by non-governmental intermediaries that have the power to enforce contracts between people that have subscribed to them. At times, these intermediaries will even provide guarantees for performance themselves. In the digital world of sale transactions, these include, for example, payment processors such as credit card companies or PayPal that ensure payment and assume credit risk in return of a (at times considerable) fee.[100]

3.3.2. *Trustless trust*

Arguably, on blockchain, trust between parties (peer-to-peer) or trust in a central authority/intermediary (Leviathan) is not necessary for economic exchange to occur. We suggest that public blockchains indeed offer a new trust mechanism for trade and explain how smart contracts function in no-trust contracting environments which are characterized by parties meeting in anonymity and there being weak or no formal contract law or institutionalized intermediaries for ensuring the enforcement of contracts.

Of course, trust underlying smart contracts built within consortium or private blockchains might also take the form of second-party (peer-to-peer) trust or even third-party (Leviathan) trust.

In the first case, blockchain technology might be taken to merely codify what would otherwise be a set of social expectations or norms operating within a conventional socio-legal environment, coupled with enforcement by the particular community. As we also mention in the analysis of their efficiency below, such contracts bear the potential of establishing a parallel system to the state-provided legal system that is governed by its own rules. In such a manner, utilising a blockchain might facilitate indirect trust relationships between known participants and operate as a second-party trust environment.[101]

In the second case, particularly in smaller-scale consortium or private blockchains, the trust relationship inherent in smart contracts might reduce to trust in a central authority (Leviathan) typical of legal contracting behaviour.[102] This may be because either the blockchain itself (though admittedly comprised of its users), or the intermediaries managing the contract (writing the code, running the system or storing the data) might be viewed as the central authorities typical in legal contracting environments.[103] Owners of private or consortium blockchains might also offer a 'choke point' for regulatory intervention by state authorities, allowing the Leviathan to intervene indirectly with contracting activities occuring on these blockchains. The same kind of trust relationship might even develop when smart contracts operate on public blockchains where, paradoxically for systems built for decentralization, trust in a governing third party is required for the continued operation of blockchain applications as 'rules need to changed and governance decisions are recurrently needed' .[104]

At the same time, let us think whether such trust relationships are necessary when, thanks to the technological nature of smart contracts, there is also a new trust mechanism for trade that stems from public blockchain.[105] The trust relationships encouraged by private blockchains may indeed be similar to those in legal or relational contracting environments. In comparison, public blockchains with the combination of decentralization, cryptographic open source protocols, and crypto-proof consensus signal a high degree of reliability of blockchain technology - the 'trustless trust' - which does not necessitate additional trust between parties (peer-to-peer) or trust in a central authority/intermediary (Leviathan) for economic exchange to occur. This is how smart contracts could create markets where previously, due to the absence of trust, no contracting, and thus no exchange would take place.[106]

Smart contracts present an improvement for contracts which would be concluded in an environment with no particular pre-existing social context to embed them. We refer to the no-trust contracting environment which we have described above as typically the one where parties meet in anonymity and the legal or relational contract enforcement mechanisms

[99] Werbach, 'Trustless Trust' (n 104) 17; Robert Putnam, *Bowling Alone: The Collapse and Revival of American Community* (Simon & Schuster 2000) 135.

[100] We thank Giorgio Monti for a similar example from the 'analogue world': In the international sale of goods, contracts with a time-deferred delivery allow for deferred payment via so-called bills of lading that can be circulated through the seller's and buyer's bank, so that final payment is only released once the goods have been delivered in conformity with the contract.

[101] An excellent point made by our reviewer.

[102] For a comparison of blockchain governance with Hobbes's concept of the Leviathan see Wessel Reijers, Fiachra O'Brolcháin, and Paul Haynes, 'Governance in Blockchain Technologies & Social Contract Theories' (2017) 1 *Ledger* 134, 143-144 <https://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62/51> accessed 11 July 2017, date last accessed).

[103] An excellent point made by our reviewer as well as Arruñada 'Blockchain's Struggle to Deliver Impersonal Exchange' (n 22) 65-66.

[104] Ibid 65. Lehdonvirta V. The blockchain paradox: why distributed ledger technologies may do little to transform the economy. Policy Internet Blog 2016. 21 November 2016 http://blogs.oii.ox.ac.uk/policy/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy. accessed 21 August 2018.

[105] Werbach, 'Trustless Trust' (n 104) 538.

[106] For a similar argument see Werbach and Cornell, 'Contracts Ex Machina' (n 1) 333.

are weak or absent.[107] In such a setting, contract law (albeit weak in terms of enforcement) would initially appear to be the only available option to ensure cooperation in economic exchange. However, smart contracts could actually provide a new improved alternative to formal contract law and be superior to all other forms of contracting in such a setting. When parties avoid relying on traditional contract law or contract enforcement as a tool for sustaining efficient exchange (or mandatory for other reasons), they could therefore avoid uncertainties such as potentially costly litigation to establish applicable law and place of jurisdiction, as well as inefficient civil court systems. This does not mean that the contracts would not be subject to the laws of its jurisdiction. They are, just like all online transactions. Smart contracts would just offer a better option because of the combination of unique features of these contracts which help to avoid efficiency losses and increase reliability. These features include automated performance, decentralization and crypto-proof character.

Thanks to being uniform in nature (independent of the particularities of different jurisdictions), smart contracts can facilitate trade across the world, and across different societal embeddings, which would not take place but for the 'trustless trust' mechanism provided by blockchain technology.[108] Even more, in such a global setting, not even contract law could ensure the enforcement of agreements, due to limited jurisdictional reach in many cases.[109] While transacting parties can theoretically always ask assistance from legal institutions when something goes wrong, in practice there are multiple limitations to protecting one's rights in such a manner. In these cases smart contracts could prove to be the only instrument available to ensure cooperation thanks to automated performance.

When discussing no-trust environments, we mentioned briefly that arguably on blockchain, trust between parties (peer-to-peer) or trust in a central authority (Leviathan) is not necessary for economic exchange to occur. Let us think deeper, how blockchain's 'trustless trust' could offer a new trust environment for trade and think of public blockchain as the example of blockchain in particular. On public blockchains, parties can engage in contracting and economic exchange while being completely anonymous to each other. When parties trust the technology, they can act on their normal incentives to engage in economic exchange.

In a recent report, the UK Government Scientific Adviser has suggested that '[i]n cyberspace, trust is based on two key requirements: prove to me that you are who you say you are (authentication); and prove to me that you have the permissions necessary to do what you ask (authorisation). In return, I will prove to you that I am trustworthy by delivering services or products to you in a secure, efficient and reliable fashion.'[110] 'Authentication does not require that I know your identity but it does require that you provide me a token that is inextricably linked to your identity, for example the pin number associated with a credit or debit card, or a fingerprint allied to a biometric passport or other document.'[111] As Veerpalu has noted in reference to this, privacy is protected in distributed ledger technology far beyond current regulation of transactions as 'Satoshi eliminated the need to know the true identities of those others in order to interact with them'[112] and 'everything is based on crypto proof instead of trust'[113] as we have known it so far.[114]

Smart contracts on public blockchains could be reliable contracting devices for no-trust environments, because parties can rely on the underlying technology without having to trust the other party, a central authority or the agents in blockchain's consensus mechanism.

Automated performance: Trusting the other contracting party is not necessary, because the technology will take care that the other party performs her obligation.

Decentralization: Trusting a central authority is not necessary, because public blockchains escape any central control due to their decentralized nature.

Crypto-proof character: Trusting the nodes involved in the proofing mechanism is not necessary, because servicing nodes will only benefit from approving transactions on the blockchain if they comply with the rules of the system.

Transparency and ability to sustain integrity: Additionally, we should take account of two other general features of public blockchains that enhance trust in the technology - the transparency of transactions and the ability to sustain the integrity of data. Since the first has been explained above,[115] let us focus on the second. Integrity of data in this context is the maintenance of the consistency, accuracy, and trustworthiness of data over its entire life cycle. Blockchain-based applications direct us to thinking of the integrity of data and the ability to monitor and control the use of our data as further guarantees for reliability of the technology. The integrity of data together with the ability to monitor and control the use of our data, provides a strong guarantee for the security of our data, our trust towards the other parties to contracts, as well as to the certainty about performance. The traces that any operation on

[107] See Section 2.1 above.

[108] On blockchain's trustless architecture see the widely circulated draft paper Werbach, 'Trustless Trust' (n 104) as well as Werbach K. Trust, but verify: why the blockchain needs the law. *Berkeley Technol Law J* 2018;33:489 https://ssrn.com/abstract=2844409. accessed 1 February, and Jean Bacon and others, 'Blockchain Demystified' (2017) Queen Mary School of Law Legal Studies Research Paper No. 268/2017 <https://ssrn.com/abstract=3091218> accessed 1 February 2018.

[109] For a similar argument see Savelyev, 'Contract Law 2.0' (n 41) 127.

[110] Mark Walport (ed), 'Distributed Ledger Technology: Beyond Block Chain' (2016) London: UK Government Office for Science 13 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> accessed 21 August 2018.

[111] ibid. See also: Stephen Mason S and Timothy S. Reiniger, 'Trust' Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?' (2015) 21 *Computer and Telecommunications Law Review* 135.

[112] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How The Technology Behind Bitcoin is Changing Money, Business and The World* (Penguin Random House 2016) 41.

[113] Wright and De Filippi (n 2) 9.

[114] Anne Veerpalu 'Regulation of the Use of Blockchain Technology in Creating Decentralized Organizations and Digital Identities: Comparative Study. PhD Research Proposal' (2016).

[115] See Section 1.2.

blockchain leaves (the 'logs' created on the blockchain) make it possible to monitor activities related to us or hold other account holders accountable if necessary. Some have considered it one of the main advantages of blockchain technology that it provides foundations for consistent, public and shared transactions thereby using data integrity for guaranteeing higher data security than previous technologies.[116]

In such a manner, trust between parties would not be replaced by but supported by the trust in the technology powering smart contracts.[117] The trust in or reliability of the technology is built on the automated performance, decentralization, proofing mechanism underlying smart contracts, which provide the transparency and integrity of data. These important properties help us to put smart contracts forward as a response to the situations where the lack of social context, including lack of trust between parties or low level of certainty in terms of performance, might inhibit contracting.

Offering a new form of enforcement mechanism, and an alternative trust relationship between parties, smart contracts on public blockchains could open a new strand of research within the area of law and economics of contracts characterized broadly as the study of new modes of contract enforcement through technology as sources of market creation. While the precise parameters of inquiry would yet have to be determined, the research on smart contracts on public blockchains shows that next to the study of relational contracts and the research on the economics of black-letter contract law, we could benefit from a deeper legal-economic understanding of code-based systems of rules.

3.4. *Efficiency gains and losses*

Smart contracts seem to hold the promise of providing huge efficiencies over traditional contracts, but as Werbach and Cornell point out, we still need to explain how smart contracts can 'offer a superior solution to the problems that contract law addresses'.[118] Twenty years ago, American computer scientist and lawyer Nick Szabo expected smart contracts to improve four basic contract objectives: observability (both parties can observe each other's performance), verifiability (easy verification if and when transactions have been performed), privity (only the necessary details for completion of the contract are revealed) and enforceability (automated performance).[119] Werbach and Cornell conclude their recent study on the potential and the limitations of smart contracts with a somewhat more careful statement. According to them, smart contracts may significantly alter the commercial world, and will demand new legal responses, but will not displace contract law.

The purpose of this section is to delineate some of the mechanisms that make contract law efficient according to mainstream law and economics, and that potential critics could claim to be difficult to replicate in the code of smart contracts. Subsequently, we will discuss how to overcome some of these criticisms through the design of smart contracts. We will first discuss the potentially inefficient features of smart contracts when compared to traditional contracts and then explain why the smart contracts still have the potential to dramatically reduce costs compared to traditional contracts.

Some of the claimed advantages of traditional contracts over smart contracts are also advantages from an efficiency perspective. We will therefore pick up the criticisms of smart contracts and translate them into an efficiency narrative. Most of these criticisms implicitly assume that we are considering smart contracts on public blockchains. We will therefore, these criticisms are less justified when using smart contracts on permissioned blockchains, where private or consortium chain owners would still be able to exercise central control.[120] Lastly, we will provide arguments showing the advantages of smart contracts on public blockchains over traditional contracts that existing literature does not take sufficiently into account.

Contract law provides several ex-post correction mechanisms referred to as mandatory rules, to prevent that parties are bound by agreements that are detrimental to themselves and to society. They curtail the basic principle of freedom of contract to promote other overriding values.

3.4.1. *Defective consent*

Courts, for example, will not enforce contracts for which there was no genuine meeting of the minds, as in the case of mistake, fraud, duress or necessity. These contract law doctrines[121] provide excuses for non-performance and defences against formation. From an economic perspective, they cure market failures resulting from actions by market players that deviate from individual rationality (e.g. duress, necessity) or from asymmetric information (e.g. fraud, mistake).[122] As smart contracts are automatically executed, performance of the contract will occur, even though from a legal perspective the contract is invalid.[123] Smart contracts thus lack the function provided by courts in the case of traditional contracts to adjust results *ex post* that were due to *ex ante* defects in the consent of the parties.[124]

3.4.2. *Capacity*

Similarly, courts will not enforce a contract against a party that lacked capacity at the moment of contract formation, as for example against a minor or against an intoxicated person. The economic function of capacity is again to cure market failures resulting from deviations from individual rationality.[125] As in the case of other formation defences and excuses, smart contracts cannot account for whether a party had the capacity to enter into a contract, unless an identity

[116] Guardtime. An industrial blockchain for IoT, https://guardtime.com/solutions/internet-of-things; 2017 accessed 11 July 2017.

[117] Raskin, 'The Law and Legality of Smart Contracts' (n 9) 317-319.

[118] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 313.

[119] Szabo 'Smart Contracts: Building Blocks for Digital Markets' (n 1).

[120] For a similar argument see Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (n 7) 275.

[121] We refer to legal doctrine as encompassing not only the law but also the scholarship on the law.

[122] Cooter and Ulen, *Law and Economics* (n 74) 294-299.

[123] Savelyev, 'Contract Law 2.0' (n 41) 19. Werbach and Cornell, 'Contracts Ex Machina' (n 1).

[124] Werbach and Cornell, 'Contracts Ex Machina' (n 1).

[125] Cooter and Ulen, *Law and Economics* (n 74) 342.

verification system is in place in case of a permissioned blockchain. Still, it would be difficult to imagine how a smart contract could identify temporary incapacity as, for example, in the case of intoxication.

Capacity reveals a further problem with smart contracts: the identity of the party entering into a contract can be of fundamental legal importance.[126] On a blockchain on which keys cannot be linked to a particular natural person (because of pseudonymity or anonymity), as in the case of a public blockchain, it is difficult to establish the identity of the person using the key in a particular smart contract transaction.[127] Consequently, it is also difficult or impossible to establish whether the party had legal capacity to enter into the contract.

3.4.3. *Consumer protection*

Certain protections awarded under contract law to consumers have also been mentioned as a challenge for smart contracts.[128] Consumer protection measures in contract law remedy market failures of a monopoly type and of asymmetric information between consumers and businesses.[129] It is claimed that these protection measures could only be implemented with great difficulty by smart contracts.[130]

3.4.4. *Illegality*

Lastly, courts will not enforce contracts that have an illegal purpose. A smart contract programmed to implement a price-fixing cartel,[131] or to transfer illegal drugs or arms, or a Ponzi scheme,[132] impose externalities on society. While enforcement agencies would take action in such cases, they would be nearly powerless in trying to stop the execution of the smart contract, due to its automatic nature.[133]

Smart Contracts that would have any of the flaws outlined above would thus cease to be contracts in a legal sense, and they would be undesirable from an economic efficiency perspective. Nonetheless, as they would be enshrined in autonomous code on the blockchain, they would be enforced automatically. Smart contracts thus bear the potential of establishing a parallel system to the state-provided legal system that is governed by its own rules,[134] potentially creating an inefficient amount of (over) performance.

As technology stands at the moment it seems indeed difficult to implement any functions in a smart contract that would emulate contractual doctrines such as mistake, fraud, duress, necessity or capacity.[135] Filippi and Wright argue the same in relation to consumer protection provisions.[136]

Nonetheless, the effects on, for example, consumer protection, would not be exclusively negative. There are other capacities of smart contracts that could actually enhance consumer protection. Fairfield emphasises that the gains in consumer protection through use of smart contracts would be superior to consumer protection provided by courts.[137] According to him, automated agents programmed through smart contracts could search the internet for a given product sold in combination with the most beneficial standard-form clauses for the consumer and purchase it by being able to release funds from a connected bitcoin wallet.[138] This would enhance two goals of consumer protection: Firstly, the consumer could shop for the best possible contract terms at low cost. Secondly, the payment in bitcoin would limit the amount of payment data that the consumer has to reveal in the transaction. It would thus further consumers' control over the use of their personal data. At the same time, this would still not remedy the lack of ex-post regulation to protect consumers. Other means would need to be found to remedy this problem. reach a consensus on reversing smart contract transactions on a permissioned blockchain that have

In relation to traditional ex-post mechanisms of contract regulation, there are already some technologies in place that can be used to have a safeguard protecting against unwanted self-execution of a smart contract. Multi-signature ('multisig') verification technology allows for halting the execution of a smart contract until several parties have signed the transaction with their private keys. These can include not only the parties to the smart contract, but also an external third party (a so-called arbiter).[139] In a goods sale, for example, a multisig smart contract could e.g. require the signature of two out

[126] In addition, the legal concept of capacity varies across jurisdictions. See Giancaspro, 'Is a 'Smart Contract' Really a Smart Idea?' (n 41).

[127] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 371.

[128] Wright and De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 2) 26.

[129] Cooter and Ulen, *Law and Economics* (n 74) 297-298. While consumer protection laws also address other illegitimate business behaviors that do not strictly fall under the understanding of problems arising from monopoly (or abuses of dominance as understood in EU competition law), Cooter and Ulen adopt a broad understanding of market failures ensuing from monopoly, including contracts of adhesion and unconscionability (but then go on to refute these two doctrines as a basis to excuse performance from an economics perspective). For the sake of simplicity, we follow Cooter and Ulen here.

[130] Wright and De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia'(n 2) 26.

[131] On algorithmic collusion see Ariel Ezrachi A and Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016).

[132] Massimo Bartoletti and others, 'Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact' (2017) <https://arxiv.org/pdf/1703.03779.pdf> accessed 9 September 2018.

[133] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 373. The DAO is a vivid example of what happens when the blockchain and a smart contract system do not provide safeguards against illegality due to a weakness in the smart contracts' code, see ibid.

[134] The Lex Cryptographica (Wright and De Filippi) or a system of 'code-as-law' (Lessig).

[135] Savelyev, 'Contract Law 2.0' (n 41) 131. Werbach and Cornell, 'Contracts Ex Machina' (n 1) 369.

[136] 'Although implementing basic contractual safeguards and consumer protection provisions into smartcontracts is theoretically possible, in practice, it may prove difficult given the formalized and deterministic character of code.' Wright and De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (n 2) 26

[137] Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection' (n 44).

[138] Ibid 46.

[139] Werbach and Cornell 'Contracts Ex Machina' (n 1) 345. Vitalik Buterin, 'Bitcoin Multisig Wallet: The Future of Bitcoin' (2015 *Bitcoin Magazine* (13 March 2014) <https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504/> accessed 11 July 2017

of three parties. If the buyer is satisfied with the good, both buyer and seller would sign and the smart contract would execute. If the buyer and/or seller were mistaken as to the good to be sold, the buyer could refuse to sign after having received the wrong good. If the seller nonetheless signs, the signature of the arbiter would then determine whether the execution of the smart contract goes through or not.

Furthermore, the code of most smart contracts contains a 'kill switch'. Solidity, the language used to write smart contracts for the Ethereum blockchain allows for an operation called 'self-destruct' that removes the code of the smart contract from the blockchain.[140]

In relation to possible illegal transactions through smart contracts, the transaction transparency of public blockchains could be an advantage. As all transactions would be visible to everyone, and so would be the content of blocks that contain an illegal transaction. The fact that an illegal transaction would be visible to everyone could already provide a deterrent for entering into illegal smart contracts. While anonymity or pseudonymity of users could pose a challenge for law enforcement, experience with Bitcoin shows that there are mechanisms to identify a person behind a public key.

A defining feature of smart contracts is that they are automatically implemented, which gives a different meaning to breach of contract. While the automatic nature guarantees the performance of the contract and eliminates risks from non-performance in a great number of cases, it also makes it more difficult to breach a contract when it would be efficient. In common law countries, contractual breaches in cases where the costs of performing the contract turn out to outweigh its value are viewed as a common practice and are deemed acceptable (even if wrongful nevertheless)[141] as long as the breaching party pays damages to the victim.[142]

Common law does not explicitly provide an avenue for parties to walk away from their contractual promises. It asserts that the primary obligation of contracting parties is to perform their contractual promises, and incur liability to pay damages if that obligation is violated. In such a manner, law does not offer a choice between performing and not performing to the parties, as economists would suggest, adopting the Holmesian 'option view' of contracting.[143] However, a contracting party may nevertheless prefer to take advantage of more beneficial alternatives to promise-keeping, and decide to (wrongfully) not perform the promises but incur the liability to compensate the victim of the breach for the costs of non-performance through the payment of damages. The result is Pareto efficient: while the party in breach is better off by taking advantage of a better deal than the contract, the victim of the breach is not worse off. The theory of efficient breach has been built around this claim.[144]

The fact that due to automated performance smart contracts seem to lock parties into performance, together with the impossibility of being able to renegotiate a smart contract, have been pointed out as a problematic feature of smart contracts.[145] From the point of view of efficiency, the result of automated performance of smart contracts could lead to excessive performance of contractual obligations, which could in turn lead to overall efficiency losses.This claim is similar to the ones raised against the remedy of specific performance for breach of contract.[146] While the arguments for inefficiency of specific performance have been countered by the argument that specific performance as a remedy could incentivize efficient renegotiation of contracts,[147] this argument does not work in the case of smart contracts. Since the obligations taken with smart contracts are automatically performed once placed on the blockchain, automated performance would not allow for renegotiation to achieve more efficient outcomes.[148]

The issue of how to facilitate efficient breaches could possibly be addressed by features already present in smart contracts. It could be imagined that parties could include an option in their contract, which allows for breach upon the condition that damages are paid. This would be akin to a liquidated damages clause. For there to be a situation of efficient breach, the value of performing a contract plus expectation damages to the victim must be lower than the opportunity costs to enter into another, superior contract. Whether such a situation exists could be verified by including a reference to oracles in the smart contract. Oracles build a bridge from the blockchain system to the external world and can provide information as to whether certain conditions have been met.[149] They support the execution (or non-execution) of a smart contract by providing the signature that a certain state in the outside world required for the execution has been met. Oracles could for example provide information on stock prices or any other data about the world that is relevant for the execution or efficient breach of a smart contract.

A drawback of oracles is that they could make smart contracts more vulnerable to tampering due to the possibility of manipulating outside sources providing relevant information. This risk could be mitigated, however, by requiring the signature of several independent oracles that provide information

[140] See <http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html#self-destruct> accessed 12 December 2017.

[141] See Jules Coleman and Jody Kraus, 'Rethinking the Theory of Legal Rights' (1986) 95 *Yale Law Journal* 1335.

[142] Posner, *Economic Analysis of Law* (n 72) 149. See also Oliver Wendell Holmes, 'The Path of the Law' (1897) 10 *Harvard Law Review* 457, 462.

[143] Harrison J. A nihilistic view of the efficient breach. *Michigan State Law Rev* 2013;1:167; Jules Coleman, 'Some Reflections on Richard Brooks's 'Efficient Performance Hypothesis' (2007) 116 *Yale Law Journal Pocket Part* 416 <http://yalelawjournal.org/forum/some-reflections-on-richard-brookss-efficient-performance-hypothesis> accessed 23 August 2018.

[144] Posner, *Economic Analysis of Law* (n 72) 151.

[145] Werbach and Cornell, 'Contracts Ex Machina' (n 1) 366.

[146] Cooter and Ulen, *Law and Economics* (n 74) 328. Posner,. *Economic Analysis of Law* (n 72) 164.

[147] Steven Shavell, 'Specific Performance Versus Damages for Breach of Contract: An Economic Analysis' (2006) 84 *Texas Law Review* 831.

[148] Werbach and Cornell 'Contracts Ex Machina' (n 1).

[149] Thomas S, Schwartz E. Smart oracles: a simple, powerful approach to smart contracts, https://github.com/codius/codius-wiki/wiki/White-Paper#overview; 2018 accessed 9 September 2018.

about the same state of the outside world.[150] The gains of not being bound by a very disadvantageous smart contract in light of new, more beneficial alternatives would likely outweigh the possible costs of facing a corrupted oracle.

3.5. *Possible regulatory responses*

Smart contracts could provide sufficient safeguards in no-trust environments, if programmers managed to replicate efficiency-enhancing features of contract law in smart contract code and a blockchain's consensus mechanism. This would be particularly feasible with permissioned blockchains that would do away with the anonymity of users. Indeed, there are not any particularly vexing regulatory challenges when we consider the implementation of smart contracts on permissioned blockchains. Regulation would simply have to be addressed to the controlling entity (or entities) of the permissioned blockchain:

- Identifiability: Parties' identity is verified before allowing use of permissioned blockchain;
- Selection of nodes: A central entity is at least responsible for giving access to blockchain;
- Consensus: The verification mechanism could be controlled by a central entity; and
- Transaction transparency: Content of blocks can be hidden, thus avoiding confidentiality issues.

What are the regulatory challenges posed by smart contracts on public blockchains? In the absence of a central controlling entity (or group of entities) challenges seem to abound:

- Identifiability: The transactions are pseudonymous and accordingly we are faced with disguised identities, which possibly provide a tool for illegal activity;
- Selection of nodes: Blockchain operates in multiple locations raising jurisdictional matters and issues pertaining to the rules of conflict of laws;
- Consensus: Being immutable, blockchain transactions, by definition, cannot be changed *ex post*. Accordingly, new processes need to be introduced for making alterations in parties' relations with each other, if needed;
- Transaction transparency: Since the transactions are also transparent, they pose a potential privacy threat (mitigated, however, by the pseudonymity of actors).

At first sight, it appears that permissioned blockchains for smart contracts are to be preferred over public blockchains as they pose fewer regulatory challenges. The use of permissioned blockchains has drawbacks however. As permissioned blockchains are more centralized and contain fewer nodes, they are also more vulnerable to outside attacks, or to tampering or collusion by insiders. Participants on permissioned blockchains will still have to trust the other members of the consortium. Furthermore, permissioned blockchains allow for (potentially unjustified) discrimination, as a central entity can decide who is to be allowed into the system and who is excluded.

What would then be the advantages of having smart contracts on public blockchains? The fact that public blockchains are open to anyone makes them more egalitarian than permissioned blockchains. Furthermore, the fact that there is absolutely no form of central authority controlling the blockchain makes public blockchains more corruption or tampering-proof. It might be worth remembering that the ideological fuel for the creation of bitcoin was an aversion against centralized power being held by governments, central banks and commercial banks.[151] The complete absence of any centralized control is a worthwhile goal in itself that can only be offered by public blockchains.

Turning to smart contracts on public blockchains only, the number and gravity of challenges also depends on what purpose the blockchain-powered smart contracts are used for. When we look beyond using blockchain for transactions into using it for substituting traditional organizations and governance systems, we also need to take into account the challenges that arise for society as a whole. Until now they have been met with the help of national or international legal tools, but if we move towards operating via decentralized organizations and platforms, we also need new ways to mitigate the risks that this creates. We need to think how to implement safety-measures or procedures when necessary, considering that the technologies could operate without central authorities like central registries,[152] central adjudication,[153] or intermediaries such as banks, brokers, custodians.[154] There may be continued interest in a number of safety-measures, which markets together with governmental institutions are currently providing. Accordingly, the regulatory and institutional challenge is to ensure the continued existence of safety measures like for example:

- Mandatory rules in contract law that remedy market failures;
- Protection mechanisms like consumer protection, investor protection, protection of market competition;
- Measures for keeping certain activities within the socially permitted boundaries (boundaries to terrorist financing or money laundering);

[150] Ibid for how Thomas and Schwartz explain how multi-signatures schemes could enhance the objectivity of the information provided by oracles.

[151] Reijers W, O'Brolcháin F, Haynes P. Governance in blockchain technologies & social contract theories. Ledger 2017;1:134 https://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62/51. accessed 11 July 2017.

[152] See, for example, Wong JI. Sweden's blockchain-powered land registry is inching towards reality. Quartz Daily Brief 2017. 3 April 2017 https://qz.com/947064. accessed 12 June 2017.

[153] Buterin V. Decentralized court. Reddit, https://www.reddit.com/r/ethereum/comments/4igyd/decentralized_court/; 2016 accessed 12 June 2017; Kaminska I. Decentralised courts and blockchains. *FT Alphaville* 2016. 9 May 2016 https://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/. accessed 12 June 2017.

[154] Anne Veerpalu, 'Regulation of Blockchain Technology and its Challenges' (2017) Presentation at the ELSA Colloquium of IT LAW for PhD students and researchers. University of Aix-Marseille 17 February 2017.

- Responses to social needs, including censorship needs, asset location important for seizing.[155]

How could we respond to these challenges when operating on blockchains? What would it mean to provide sufficient safeguards for contract enforcement in such an environment, if we leave the possibilities of identification and tracking discussed above aside?

Many have suggested that technologies can operate as a kind of law, regulating behavior of their users.[156] According to Lawrence Lessig '[i]f the system incorporates regulation-through-code, self-executing code will be regulatory-compliant, and the choice presented to individual actors will no longer be whether to comply or not, but will merely be whether or not to use the system.' [157] It has been recognized in the legal academy that technology could have a constitutive role, following a similar broader understanding within science and technology studies.[158] There are hopes that this vision might particularly be able to materialize with the help of blockchain and smart contracts. We see statements that 'Smart contracts don't have a need in a legal system to exist: they may operate without any overarching legal framework. De facto, they represent a technological alternative to the whole legal system.'[159] 'Smart contracts are unprecedented methods of ensuring contractual compliance, including social contracts.'[160] Or, smart contracts are computerized versions of an English language paper contract, with a level of automation that essentially provides 'adjudication-as-a-service', a hyper real-time version of the court system.[161] At the same time, we should be clear that while there is great potential in blockchain, judging on the basis of several new developments in the area of smart contracts, traditional legal enforcement seems to be necessary[162] and is still kept available at the moment as a backstop.[163]

In essence, in order to contract in no-trust environments, there is a need for an enforcement mechanism which provides sufficient safeguards for contracting. If smart contracts on public blockchain (where anonymity is part of the essence) want to operate in such environments they need to incorporate safeguards in enforcement. There are two possible tracks in establishing such safeguards.

- First, we could set higher standards for identification when providing platforms for smart contracts and thus be more invasive regarding the anonymity of parties. Using permissioned blockchains or creating better mechanisms for tracking transactions and participants on the blockchain are some of the options.
- Second, and a more democratic alternative, as we claim, is incorporating such safeguards into smart contracts through remedying some of the inefficiencies arising from automated performance.

4. Conclusion

Most of the disruption in law comes from other business sectors – the computer engineers or business people who use legal services and want to change the industry. One track in these changes belongs to the opportunities created by disintermediation. Smart contracts, one of the applications of distributed computing, provide an opportunity to use technology for ensuring a consistent application of rules and agreements. Thanks to automated performance, they are expected to reduce the need to resort to legal or relational contract enforcement mechanisms e.g seeking protection from legal institutions (courts, bailiffs) or social circles (family, community).

The underlying technology makes it possible for parties to preserve their anonymity to a certain extent while contracting with each other and smart contracts seem to be able to function in precisely such contracting environments where parties, in the absence of reliable legal or social enforcement mechanisms, could engage in economic exchange anonymously. We claimed that this feature sets them apart as new modes of contracting governance particularly because they have the capacity to create trust in what we term no-trust contracting environments. We explained how these environments differ from legal or relational contracting environments and why using them in such environments is the path to unleash the full potential of smart contracts. In essence, for contracting in no-trust environments, there is a need for an enforcement mechanism which provides sufficient safeguards

[155] This is developed based on a previous similar list created by Anne Veerpalu, see ibid.

[156] See Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999). Werbach and Cornell, 'Contracts Ex Machina' (n 1).

[157] Carla L. Reyes, 'Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal' (2016) 61 *Villanova Law Review* 230 <http://ssrn.com/abstract=2766705> accessed 11 July 2017.

[158] See Bruno Latour,'On Technical Mediation' (1994) 3 *Common Knowledge* 29; Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. (Yale University Press 2012); Werbach and Cornell, 'Contracts Ex Machina' (n 1).

[159] Savelyev, 'Contract Law 2.0' (n 41).

[160] Tapscott and Tapscott, *Blockchain Revolution* (n 120) 47.

[161] Marvin, 'Blockchain in 2017' (n 8).

[162] See for example Stephen Mason, 'Artificial intelligence: Oh really? And why judges and lawyers are central to the way we live now – but they don't know it' (2017) 23 *Computer and Telecommunications Law Review* 213.

[163] For example, in case of Agrello, the developers suggest the following line of action for concluding smart contracts on the platform that they provide: 'Your agreement is automatically translated to smart-contract code and stored on the blockchain, with payments, obligations and rights triggered automatically according to the contracts terms and user input. In parallel, a legally binding document is created, written in natural legal English, and signed off digitally. This Document can, in corner cases, be presented to court if traditional legal action is needed. All Agrello agreements are immutable, yet open to adjustment and future renegotiation. Throughout the contract's life cycle, an AI counselor guides you through your agreement and notifies you on your legal obligations and rights. At any stage you remain in control of your privileges and duties, able to waive and manage them according to the potential benefits and consequences, as presented to you by your AI counselor. This way, simple p2p agreements, as well as complex, multi-party business processes can be automated and orchestrated at a fraction of the standard legal and operational costs. Continuously update your contract according to real-world input and evolving mutual agreements.' Agrello, https://www.agrello.org/; 2017 accessed 22 November 2018.

for contracting. When enforcement through law or social relations is unavailable or inconvenient, smart contracts allow us to rely on enforcement through technology. Trade relies on trust and while other enforcement mechanisms support trade through other trust mechanisms (first-personal, peer-to-peer, or Leviathan trust mechanisms), smart contracts offer a new mechanism characterized by trustless trust.

Based on the potential efficiency gains and losses from contracting in no-trust environments, there could be reasons to prefer smart contracts to other methods of contract governance. Compared to the contract enforcement mechanisms characterised by traditional contract law or relational contracts, smart contracts could, at times, offer a superior solution for facilitating trade in no-trust contracting environments.

Additionally, technological innovation gives rise to new opportunities for law and economics. The existing literature on the law and economics of contracts discusses on the one hand the efficiency and costs of existing contract law regimes providing normative ideals for efficiency enhancing contract law design. On the other hand, it tackles the area of contractual practices outside the strict confinements of the legal system. We have suggested that smart contracts could open up a third field of inquiry within the law and economics of contracts, characterized by the study of new modes of contract enforcement through technology as source of market creation.

Acknowledgement

We would like to thank Giorgio Monti, Alexander Stremitzer, Roger Brownsword, Massimiliano Vatiero, Francisco Alves Da Costa-Cabral and Hossein Nabilou for valuable insights and feedback on the earlier versions of this paper. We are very grateful to Stephen Mason, Luca Belli, Rafaela Nogueira, Barrie Sanders, Stanley Shanapinda, Thomaz Pereira, as well as the participants of the FGV Research Seminar and the 13th Annual Conference of the Italian Society for Law and Economics for helping us in developing and clarifying our argument. We are extremely grateful to Fundação Getulio Vargas, FGV Direito Rio, for provoking us to explore new technologies together and for creating an excellent research environment for us. During the course of writing this article we have also benefited from the Dora Plus programme funded by the European Regional Development Fund and the Republic of Estonia.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.clsr.2018.09.003.