European University Institute

DEPARTMENT OF LAW

EUI WORKING PAPERS

LAW 2017/13
Department of Law

Regulation through code as a safeguard for implementing smart contracts in no-trust environments

Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen

European University Institute
Department of Law

REGULATION THROUGH CODE AS A SAFEGUARD FOR IMPLEMENTING SMART CONTRACTS IN NO-TRUST ENVIRONMENTS

Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen

EUI Working Paper **LAW** 2017/13

ISSN 1725-6739

Printed in Italy
European University Institute
Badia Fiesolana
I-50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Abstract

Smart contracts, self-executing agreements based on blockchain technology, are a hotly debated topic in the tech community, among policy makers, industry stakeholders and in academia. They offer the prospect of cheaper, faster and better transactions. The hype around smart contracts is also viewed with caution. We contribute to the existing academic literature by addressing some of the concerns about the legal nature, anonymity and reliability of smart contracts.

Several contract law scholars argue that smart contracts cannot offer a superior solution to many problems addressed by traditional contract law, such as contract validity and legality. Furthermore, they argue that smart contracts cannot replicate the relational context which is essential for the day-to-day practice of contracting.

In this contribution, we firstly draw a distinction between smart contracts based on public blockchains and those based on private or permissioned blockchains. While all existing contributions develop their arguments implicitly assuming that smart contracts are based on public blockchains, much commercial experimentation with smart contracts is occurring on permissioned blockchains. Importantly, many of the mentioned problems do not arise on permissioned blockchains.

Secondly, we argue that there is a good reason to prefer public blockchains over permissioned blockchains for contracting, namely their capacity to create trust in otherwise no-trust contracting environments. This is the path to unleash the full potential of smart contracts. In contrast to critics, we argue that compared to traditional contract law, smart contracts potentially offer a superior solution for facilitating trade.

Keywords

smart contracts, blockchain, contracts, law and economics, trust

Authors' contact details:

Helen Eenmaa-Dimitrieva
JSD Yale Law School
Postdoctoral Researcher in IT law
Founder of the Research and Study Programme in IT Law
School of Law
University of Tartu
helen.eenmaa@ut.ee

Maria José Schmidt-Kessen
PhD Candidate
Law Department
European University Institute
maria.schmidt-kessen@eui.eu

Table of contents

1. INTRODUCTION 1

2. PUBLIC AND PERMISSIONED BLOCKCHAINS UNDERLYING SMART CONTRACTS 2

2.1. Nature of transactions and registration on public blockchains 2

2.2. Nature of anonymity on public blockchains 6

2.3. Smart contracts 7

2.4. Smart contracts on public and permissioned blockchains 10

3. SAFEGUARDS FOR IMPLEMENTING SMART CONTRACTS IN NO-TRUST ENVIRONMENTS 16

3.1. No-trust environment 16

3.2. Identification as a safeguard for implementing smart contracts 17

3.3. Regulatory challenges 19

3.4. Efficiency considerations regarding safeguards for implementing smart contracts 22

3.5. Efficient breach 26

3.6. Relational contracts and trustless reliability 27

4. CONCLUSION 30

BIBLIOGRAPHY 31

1. Introduction

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. In this paper, we discuss how one of such applications of distributed computing - smart contracts - could provide a possible alternative mechanism for ensuring cooperation in transactions between two or more parties.

Smart contracts, self-executing digital transactions using decentralized cryptographic mechanisms for enforcement,[1] are a hotly debated topic in the tech community, among policy makers, industry stakeholders and in academia, because they offer the prospect of cheaper, faster and better transactions. The term 'smart contract' was coined by Nick Szabo, a US computer scientist and legal scholar. 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'.[2]

While there are several debates about its nature, today a smart contract is mostly understood as an agreement that is encoded in computer code and placed on a decentralized virtual infrastructure which has become known as the blockchain (in short, a self-executing agreement based on blockchain technology). Computer protocols are there to verify and enforce the clauses and performance of a contract thus making some traditional contractual activities involved in the verification and enforcement of a contract unnecessary. The technology allows automatically implementing and enforcing the terms of an agreement. While smart contracts can represent the translation of a specific contractual agreement with legal force between two parties, they can also create relationships without underlying contractual rights and obligations.

The technology also makes it possible for parties to preserve their anonymity while contracting with each other. Until recently, complete anonymity between parties would provide for the paradigm set of circumstances where we would imagine needing contract law. This is because due to the anonymity the contract was not embedded in any social context that could work as an alternative enforcement mechanism to ensure that all parties cooperate.[3] Yet, smart contracts seem to be able to function in precisely such contracting environments where parties could meet in complete anonymity. **We claim that this feature sets smart contracts apart as new modes of contracting governance and as vehicles for contracting in no-trust environments**.

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 can. What we claim instead is that they are a tool which facilitates contracting in no-trust environments where due to the complete anonymity between parties one would need contract law or other enforcement mechanisms as tools for contracting governance, but those are not available or reliable for various reasons. 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 would thus not be able to find the defendant. This deters from contracting until a suitable and reliable contract enforcement mechanism is provided. Such a mechanism can be more efficient in settings where contracting is governed by formal contract law and possibly even

[1] We use the definition of Kevin Werbach and Nicolas Cornell. See Werbach K, Cornell N. Contracts Ex Machina. Duke Law Journal; Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed)

[2] Szabo N. Smart Contracts: Building Blocks for Digital Markets, Extropy 1996; 16 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (11 July 2017, date last accessed)

[3] 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

more so where it is not. Our focus is on explaining how smart contracts can provide such an alternative mechanism of contracting governance and analyzing the safeguards needed for implementing them - identification and regulation through code.

Our further hypothesis is that **in terms of both regulatory and economic implications it might be helpful to draw a distinction** between smart contracts based on public blockchains and smart contracts based on permissioned blockchains. The design of the underlying blockchain technology is a significant feature that needs to be factored into the discussion on smart contracts. This is a point generally overlooked by most legal academic literature.

2. Public and permissioned blockchains underlying smart contracts

2.1. Nature of transactions and registration on public blockchains

Blockchain technology, the technology underlying smart contracts, is one of the distributed ledger technologies (aka 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, including law.[5]

A distributed ledger is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions.[6] There is no central administrator or central data storage.[7] All distributed ledgers do not have to necessarily employ a chain of blocks to successfully provide secure and valid achievement of distributed consensus.[8] Blockchain technology is different from other familiar distributed computing technologies like torrents. Both are based on P2P technology for spreading information across nodes and neither of them uses a central server. However, while torrents are all about copying information, blockchains are about preventing copying while rather guaranteeing the integrity of information. While the bitcoin blockchain, which uses proof-of-work mining, is the most publicly proven method used to achieve distributed consensus, there are many other forms of distributed ledger consensus processes implemented in private blockchain projects such as Ripple, Hyperledger or MultiChain.[9]

In terms of technology, smart contracts are essentially pieces of code inside the blocks on the blockchain, which are available in all the nodes. But what does that mean? Let us get a high-level overview of the blockchain architecture in order to move on to other questions and use the example of bitcoin to see how

[4] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 4-5

[5] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 5

[6] UK Government. *Distributed Ledger Technology: Beyond Block Chain. A Report by the UK Government Chief Scientific Adviser*. Crown Copyright 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (July 11 2017, date last accessed)

[7] Scardovi C. *Restructuring and Innovation in Banking*. Springer, 2016 https://play.google.com/store/books/details?id=uNM0DQAAQBAJ (5 June 2017, date last accessed) 36

[8] Blockchain Technologies. *Blockchain Technology Explained.* http://www.blockchaintechnologies.com/blockchain-definition (5 June 2017, date last accessed)

[9] Blockchain Technologies. *Blockchain Technology Explained.* http://www.blockchaintechnologies.com/blockchain-definition (5 June 2017, date last accessed)

the transfer of control and registration in the database take place on a blockchain. We will assume a case of a bitcoin purchase and sale transaction.

Bitcoin is fundamentally different both from physical cash, as well as traditional virtual currency such as money on a bank account. In bitcoin, there is neither a central authority maintaining a central database of who owns what (money), nor are there any physical objects (like physical coins or money bills) whose ownership characterises the ownership of the bitcoins. Instead, there is a public ledger (inside the so-called blockchain) that contains a list of all transactions that ever occurred between any two bitcoin 'accounts'. Notice that no central authority is in place. The rules of the bitcoin system (e.g. who can transfer bitcoins to whom, etc.) are established by consensus and coded into the software that runs the bitcoin system. Aspects of the bitcoin system can be changed if a sufficiently large portion of the devices in the bitcoin network implement that change.[10]

In order to buy, receive or use bitcoins one must create one or many bitcoin addresses using the downloaded software or an online site. A bitcoin address is a virtual entity which is not necessarily bound to a particular person (and it is not necessarily stored on any server). In particular, no registration or authentication is necessary to create a bitcoin address. It is even possible for a piece of software to create and control new addresses without interaction with a human. Access to a bitcoin address is controlled purely by who has access to the corresponding secret key. In that sense, a bitcoin address is similar to a numbered bank account where anyone who knows the secret number can withdraw money from that account. Given the secret key, any entity (human or not) can make bitcoins move from one address to another by sending a digitally signed transaction to one of the many computers participating in the bitcoin network. The digital signature is placed using the secret key corresponding to the address.[11]

Bitcoins are purely virtual entities in the sense that they do not exist in any other way than by the fact that the public ledger says how many bitcoins have moved from which address to which address. The public ledger is itself maintained by a distributed process on the Internet, that is, many computers (so-called ‘nodes’) on the Internet will have a copy of the ledger. A mechanism is in place that ensures that all those copies of the ledger will agree with each other. To be precise, it is possible that the different copies will disagree on recently performed transactions (e.g. within the last hour). However, after a certain time, disagreements will be less and less likely.[12]

How do the transfer of control of the virtual currency and the registration take place? After the creation of a bitcoin wallet, a person obtains a multi-digit bitcoin address. An address is a hashed version of a public key. One person can obtain as many additional addresses as desired and one could use a unique address for each transaction. The information about the users and their transaction is recorded in a public ledger (inside the so-called blockchain) and is visible to all members of the network. No personal data of the users is included, therefore, the bitcoin system does not reveal any personal data. In the words of the creator of bitcoin: 'The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone'[13].[14]

[10] The analysis provided in parts 2.1, 2.2 and 3.2 is based on and cites a previously unpublished report written by Helen Eenmaa-Dimitrieva and Dominique Unruh on the architecture and anonymity of Bitcoin transactions for the Supreme Court of Estonia. See: Eenmaa-Dimitrieva H, Unruh D. *Report on the Architecture and Anonymity of Bitcoin Transactions for the Supreme Court of Estonia* (7 January 2016) (Here: Eenmaa-Dimitrieva and Unruh Report 2016)

[11] Eenmaa-Dimitrieva and Unruh Report 2016

[12] Eenmaa-Dimitrieva and Unruh Report 2016

[13] Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008. https://bitcoin.org/bitcoin.pdf (11 July 2017, date last accessed) 6. Of course, it is worth noticing, as we in length below, that while no personal data of the users is included in the transactions, this is not a guarantee of anonymity. As soon as a secret key is linked to an individual by other means, all his or her transactions can potentially be revealed.

[14] Eenmaa-Dimitrieva and Unruh Report 2016

Once connected to the network, there are three ways to obtain bitcoins.[15]

- First, a user can exchange conventional money (e.g. dollars, yen, and Euros) for bitcoins for a fee on an online exchange (e.g. Okcoin, Coinbase, and Kraken).
- Second, a user can obtain bitcoins in exchange for the sale of goods or services, as when a merchant accepts bitcoin from a buyer for the sale of his product.
- Third, users within the bitcoin network, known as miners, can gather together blocks of new transactions and compete to verify that the transactions are valid, i.e. that the buyer has the amount of bitcoins being spent and has transferred that amount to the seller's address. The miners are willing to do this work due to the bitcoin payment they receive once they succeed in verifying a particular transaction.[16]

Bitcoin transactions take place by digitally signing hashes of previous transactions (indicating the transactions through which the bitcoins were originally received) and the public key of the next owner (or entity which knows the secret key corresponding to the next owner's bitcoin address) and broadcasting these. The purpose of miners is to enter the transactions into the public ledger. For providing this service, miners that successfully verify a block of transactions are rewarded by the bitcoin network with newly created bitcoins. To transfer an amount x of bitcoins from one bitcoin address A to another bitcoin address B, the following steps take place:[17]

- Someone (presumably the 'owner' of address A, but it could be any entity which knows the secret key corresponding to address A) creates a digital signature that signs a message that essentially says 'Transfer x bitcoins from address A to address B'. This signature needs to be signed with the secret key of address A.
- That signature is sent to one or many entities participating in the bitcoin network. These entities further distribute the signature between themselves so that, barring network failures or similar problems, all entities have the same signatures. At this point, the signatures are not yet contained in the public ledger, but are candidates for inclusion.
- Many entities in the bitcoin network (so-called miners) continuously try to solve certain difficult computational problems. Whenever a miner solves such a problem, he can append a new block of data to the public ledger (which is why that ledger is called a blockchain). Once this has happened the transaction of x bitcoins from A to B will be in the public ledger. Addition of the new block to the ledger is subject to the acceptance of all contained signatures and transactions and the new block by the majority of the rest of the bitcoin network, and only if the address A had a sufficient balance.[18]

From that moment on, whoever has access to the secret key of address B will be able to transfer the bitcoins further. Also, from that moment on, next blocks can connect to the block containing the transaction between A and B. Invalid transactions will not be included in the blockchain and will not be accepted as the basis for next blocks. The more blocks are built after the block containing the particular transaction the smaller is the possibility of this transaction being wrong or fraudulent. Merchants usually wait until certain amount of blocks are built upon the block containing the payment for their goods or services to consider the payment completed. The miners clearly have an important role in verifying that

[15] It is worth noticing that operating a public blockchain relies on affordable and ubiquitous connectivity. Internet infrastructure is key to the use and operation of blockchain.

[16] Eenmaa-Dimitrieva and Unruh Report 2016

[17] Strictly speaking, the bitcoins are not transferred from the address A, but from the output of an earlier transaction that had address A as the recipient. For the purposes of this exposition, however, this distinction is immaterial.

[18] Eenmaa-Dimitrieva and Unruh Report 2016

the transactions are valid and are incentivised to do so with the bitcoins paid to them once they succeed in the verification process.[19]

On a higher level, a bitcoin transaction has the following properties:

- Anyone who knows the secret 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 between physical or legal persons and the bitcoin addresses is enforced or maintained.[20]

It is worth noting that the creator of bitcoin has suggested a simple method of verification whether the transfer of bitcoins took place. He points out that all blocks bear a proof of time when they were created (timestamp). A user needs to link the transaction to the block in which it is timestamped. He is not able to check the content of the transaction, but by linking it to a place in the chain, he can see that a network node has accepted it, and the blocks added after it further confirm that network has accepted it[21]. We could say, the transfer of control of bitcoins is recorded and verified by the means of blockchain protocol.[22]

Now let us see which information if any is visible to and can be inspected by the public or a facilitator of an exchange (e.g. a Bitcoin exchange or a currency exchange bureau). Let us assume for now that we talk about an exchange of a normal currency (e.g. EUR, USD, etc.) for bitcoins and vice versa. In such a case, the facilitator of the exchange has access to all data in the public ledger as any other user of bitcoin system. Facilitators of the exchange do not hold any privileged position within the bitcoin system which would allow them access to more information. In such cases of exchange, two processes happen:

- Real/normal currency is transferred from the client to the facilitator (or vice versa)
- Bitcoins are transferred from the facilitator to the client (or vice versa)[23]

The first of these transactions is independent of bitcoin. Since normal currency changes hands, the visible information depends on the method of transferring this currency. For example, if real currency is paid to the facilitator via credit card, then the facilitator will know the credit card number and whatever data is provided by the credit card company. If the facilitator pays the real currency to a bank account, the facilitator will know the bank account number. Thus, the first transaction involves external (i.e. imposed from the outside of the bitcoin system) obligation to collect certain information prior to the exercise of exchange.[24]

In the second transaction, the facilitator cannot check whether the bitcoins go to or come from the client. The facilitator will know from which bitcoin address the bitcoins come, or to which bitcoin address the bitcoins go. However, the facilitator cannot check whether this address belongs to the client. In the case where the facilitator receives bitcoins, he will of course know that the client has control over the address, since otherwise the client would not be able to pay the facilitator. The facilitator (and anyone else) can track the past and future flow of bitcoins from that bitcoin address (as well as any other bitcoin address). On the basis of this, statistical analysis of data may allow identifying the users of bitcoin addresses.

[19] Eenmaa-Dimitrieva and Unruh Report 2016

[20] Eenmaa-Dimitrieva and Unruh Report 2016

[21] Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. https://bitcoin.org/bitcoin.pdf (11 July 2017, date last accessed) 5

[22] Eenmaa-Dimitrieva and Unruh Report 2016

[23] Eenmaa-Dimitrieva and Unruh Report 2016

[24] Eenmaa-Dimitrieva and Unruh Report 2016

Methods of such analysis will be described in more detail immediately below when discussing the anonymity of parties.[25]

2.2. Nature of anonymity on public blockchains

Let us look into the nature of anonymity of the parties in case of public blockchains. We shall do this once again by using the example of Bitcoin. In a transaction which involves the exchange of bitcoins against normal currency, 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.[26]

The transfer of bitcoins is anonymous to some degree. While the bitcoin system does keep track of bitcoin addresses, it does not keep track of address ownership (whoever has the secret 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.[27]

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. However, 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. This allows obfuscating the money flow from one address to another, making the bitcoin address anonymous.[28]

In summary:

- Bitcoin addresses are not bound to user identities.
- The anonymity of bitcoin addresses can nevertheless be broken in some cases. This can be avoided by the use of mixing services.
- The facilitator of an exchange does not have the possibility to record *whose* bitcoin address he is transferring money to or from (i.e. the identities of the persons whose bitcoin addresses these are), but he can record *which* bitcoin address the money is transferred to or from (i.e. just the multi-digit bitcoin addresses, which are the hashed versions of the public keys).
- The facilitator of an exchange can 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. (e.g. with bank transfers it is possible, with cash payments it is not unless an ID is requested.)[29]

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[30]. 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

[25] Eenmaa-Dimitrieva and Unruh Report 2016

[26] Eenmaa-Dimitrieva and Unruh Report 2016

[27] Eenmaa-Dimitrieva and Unruh Report 2016

[28] Eenmaa-Dimitrieva and Unruh Report 2016

[29] Eenmaa-Dimitrieva and Unruh Report 2016

[30] Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds). *Security and Privacy in Social Networks*. New York: Springer, 2013, 197-223. https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (11 July 2017, date last accessed) 15

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.[31]

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.[32]

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. Despite the fact that the information is not linked to a particular user it could still be used to identify parties to the transaction. Possible ways to reveal the identity of the bitcoin users will be discussed in the section below.[33]

Would it be consistent with the bitcoin protocol and rules to implement a review procedure, which would require a decrease in the anonymity principle characteristic of bitcoin sales transactions? The bitcoin protocol requires full publicity in order to operate successfully and allow transaction verification. Each transaction with bitcoins is visible to each member of the network, i.e. to all other people/entities who own, accept as payment, and exchange bitcoins to other currencies. The bitcoin transactions can be reviewed to the extent that the amount of bitcoins which flows from certain address to another at a specific time is public. This is an inherent feature of the bitcoin system. However, as the identities of the users who initiate these transactions are not contained in the public ledger, all the information accessible in the system is of little use for the state authorities for the purposes of the review procedure.[34]

Theoretically, public authorities may require the bitcoin exchange service providers to check the identity of the person who wishes to open a bitcoin wallet or exchange bitcoin for conventional currency. However, the efficiency of such a review procedure is questionable. To be effective, such rules should be implemented globally. If the review procedure is implemented only in a few countries, the users will simply switch to the bitcoin exchange service providers in other countries where there is no review procedure in place. Bitcoin exchange services are provided via the Internet and any person is free to choose the provider regardless of the provider's place of establishment.[35]

The bitcoin protocol cannot be extended to keep track of users' identities without major changes. Those changes would need to be adopted by the majority of users in the worldwide bitcoin protocol. It is not possible to change the protocol only within a given jurisdiction. Since there is no central authority that performs the bitcoin transactions, no procedures can be imposed on such an authority.[36]

2.3. Smart contracts

Blockchain 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

[31] Eenmaa-Dimitrieva and Unruh Report 2016

[32] Eenmaa-Dimitrieva and Unruh Report 2016

[33] Eenmaa-Dimitrieva and Unruh Report 2016

[34] Eenmaa-Dimitrieva and Unruh Report 2016

[35] Eenmaa-Dimitrieva and Unruh Report 2016

[36] Eenmaa-Dimitrieva and Unruh Report 2016

operate over a network of computers without any human intervention as well as self-executing digital transactions (smart contracts).[37]

Based on the standard operating principles of markets and legal environments, the complete anonymity between parties, as illustrated by the description of the general operating mechanisms of public blockchain above, should be a red flag for anyone wishing to draw up and execute a contract. Until recently, such complete anonymity would provide for the paradigm set of circumstances where 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. This is because, due to anonymity, the contract was not embedded in any social context that could work as an alternative enforcement mechanism to ensure that all parties cooperate.

Yet, this is precisely the environment in which smart contracts seem to bring about a disruption. They seem to be able to function in such contracting environments where parties could meet in complete anonymity. We will explain below how this feature sets smart contracts apart as new modes of contracting governance and as vehicles for contracting in no-trust environments, possibly not relying on formal contract law. While the impact of smart is potentially broader, in this paper, we confine our argument solely to their effects on contracting and relations with contract law. **The argument is 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) (part 2.2, part 2.3 and part 2.4).**
2. **When you have anonymity you have a no-trust environment for contracting (part 3.1).**
3. **In order to contract in no-trust environments, there is a need for an enforcement mechanism which provides sufficient safeguards for contracting (part 3.1).**
4. **Smart contracts can provide sufficient safeguards for enforcement (part 3.2).**
5. **Such safeguards could be either invasive regarding anonymity (e.g. by using permissioned blockchains) (part 3.2) or, as a better alternative, be incorporated into smart contracts to avoid certain inefficiencies arising from their automated execution-(on public blockchain where the anonymity is defining feature) (part 3.3, part 3.4 and part 3.5).**

While developing this account, we also point out why it might be helpful to draw a distinction between smart contracts based on public blockchains and smart contracts based on permissioned blockchains. We also argue that we should not develop smart contracts exclusively based on permissioned blockchains. Public blockchains offer advantages over permissioned blockchains for the development of smart contracts, which should not be ignored.

There are several debates about the nature of smart contracts. Today, they are mostly understood as agreements that are encoded in computer code and placed on a decentralized virtual infrastructure (in short, a self-executing agreements based on blockchain technology). Computer protocols are there to verify and enforce the clauses and performance of a contract thus making some traditional contractual activities involved in the enforcement unnecessary. The technology allows automatically implementing and enforcing the terms of an agreement. It also makes it possible for parties to preserve their anonymity 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.[38] The common defining characteristic of smart

[37] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 1

[38] See a variety of different definitions e.g. in Szabo N. Smart Contracts: Building Blocks for Digital Markets, Extropy 1996; 16 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (11 July 2017, date last accessed); Buterin V. DAOs, DACs, DAs and More: An Incomplete

contracts is, however, that they are executed and enforced automatically without the need of human intervention.[39]

To illustrate the concept of smart contracts, let us look at a practical example of using it for renting a vacation home on the weekend at the beach in case of good weather. Landlord and tenant agree on the price for renting the home on the weekend to be a quarter of a bitcoin.[40] They also agree that in case of a bad weather forecast for the weekend on the preceding Thursday, the tenant will not come, and there will be no payment.

In a first step, all these clauses are translated into computer code and placed on a blockchain after having been validated in the consensus process.[41] From this moment, any tampering with the smart contract would probably be detectable. Assuming that the underlying blockchain is public, all users are able to observe and testify the correctness of the agreement.

In a second step, the smart contract will connect with an oracle,[42] in this case a specified database or website with weather forecasts on the Thursday preceding the vacation weekend. If the weather forecast predicts rain, the smart contract will stop at this point. In case the weather forecast predicts sunny and warm weather, the smart contract will proceed with the execution of the contract, which entails the processing of the rent payment and the release of the key on the weekend.

In a third step, the smart contract automatically evaluates whether the connected bitcoin wallet of the tenant actually contains the relevant amount of bitcoins. If the bitcoin wallet does not have sufficient funds to pay the landlord, the smart contract will not release the key of the vacation home (e.g. in the form a door code) to the tenant. In case the bitcoin wallet of the tenant contains the funds, the smart contract will, in a fourth step, self-execute the agreement. It will cause the transfer of the relevant amount of bitcoins from the tenant's bitcoin wallet to the landlord's bitcoin wallet, and it will release the key to the tenant on a specified date and time. In further steps, the contract will withdraw the key when the rental period is over. If the contract included clauses regarding a security deposit or the condition in which the vacation home needs to be returned, further transfers or connection with an oracle might take place as well.

This is an example of a smart contract implementing a traditional contract that intends to create binding rights and obligations between parties. While other types of automated contracts[43] also embody

Terminology Guide. *Ethereum Blog* (6 May 2014) https://blog.ethereum.org/2014/05/06/daos-dacsdas-and-more-an-incomplete-terminology-guide/ (14 April 2017, date last accessed); Marvin R. Blockchain in 2017: The Year of Smart Contracts. *PC MAG* (12 December 2016) http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts (12 June 2017, date last accessed); The Economist. *Not-so-clever Contracts.* (28 June 2016) http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted (11 July 2017, date last accessed).

[39] This definition is similar to the definitions provided in Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed), Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Social Science Research Network 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 10-11, and Raskin M. The Law and Legality of Smart Contracts. *Georgetown Law and Technology Review* 2017; 1: 305-341. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166 (11 July 2017, date last accessed) 309.

[40] The current value of one bitcoin is around USD 2800 (exchange rate on on 12 June 2017).

[41] A consensus process an algorithm that ensures that every next block on a blockchain is the one and single version of the truth and prevents any tampering by parties trying to corrupt the system. It is called consensus, because a majority of the nodes in the system has to confirm the correctness of the transactions included in a new block. The best known consensus algorithm is bitcoin's proof of work, further discussed below.

[42] Oracles are 'independent entities to inform contracts about the state of the outside world.' See: Thomas S, Schwartz E. *Smart Oracles: A Simple, Powerful Approach to Smart Contracts.* https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts (11 July 2017, date last accessed). For a further discussion of oracles see section 3.5 below.

[43] Surden H. Computable Contracts. *UC Davis Law Review* 2012; **46**: 629-700

agreements in software code and even perform automatically in limited circumstances, smart contracts are considered to be advanced in the sense that they handle the full lifecycle of contractual activity and their performance is final. Performance cannot be inhibited or undone within the system of the blockchain.[44]

There is also a good reason for the definitions to vary. Smart contracts indeed can have different functions as a smart contract in the technical sense is not necessarily the same as a contractual agreement. 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 enforced by code, but which are not linked to any underlying contractual rights or obligations'.[45] 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.[46] 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.[47] One-party smart contracts, and their underlying blockchain system, are therefore also technologically different from bilateral or multi-sided smart contracts.[48]

2.4. Smart contracts on public and permissioned blockchains

In general, one could build and use a public blockchain ('fully decentralized'), a consortium blockchain ('partially decentralized'), or a private blockchain ('centralized') for building smart contracts on top.[49] Consortium and private blockchains are usually referred to jointly as permissioned blockchains. The three core technologies that make up blockchain technology (a 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 mechanism, for example mining in the case of bitcoin)[50] 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 consensus mechanism and
4. The openness of the content of the blocks.

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

[44] For a more detailed discussion partially relativizing this statement see section 3.4.

[45] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 11

[46] Kim HM, Laskowski M. A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange. *Working Paper*. 2017 http://blockchain.lab.yorku.ca/files/2017/05/UBC_blockchain_paper_HK_and-Marek.pdf (11 July 2017, date last accessed)

[47] Kim HM, Laskowski M. A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange. *Working Paper*. 2017 http://blockchain.lab.yorku.ca/files/2017/05/UBC_blockchain_paper_HK_and-Marek.pdf (11 July 2017, date last accessed)

[48] Kim HM, Laskowski M. A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange. *Working Paper*. 2017 http://blockchain.lab.yorku.ca/files/2017/05/UBC_blockchain_paper_HK_and-Marek.pdf (11 July 2017, date last accessed)

[49] Buterin V. On Public and Private Blockchains. *Ethereum Blog* (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (11 July 2017, date last accessed)

[50] Coindesk. *How Does Blockchain Technology Work*. http://www.coindesk.com/information/how-does-blockchain-technology-work/ (12 July 2017, date last accessed)

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. As a result, for example, the identity behind a bitcoin public key can be difficult to establish.[51]
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.[52]
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,[53] 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. There are many blockchain entrepreneurs (including those working on smart contracts) who 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 mechanism, 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, then 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).[54]
4. **Openness**: Public blockchains also have a high degree of openness. Anyone can read the content of the blocks on the bitcoin blockchain. While this might not be problematic in case of bitcoin, the openness of public blockchain can pose a challenge if the content of blocks contains sensitive information.[55]

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. By allowing a countless number of parties to maintain a correct record of their transactions it also allows them to get rid of some centralized, powerful, corruptible middlemen with

[51] See discussion of bitcoin above for further details.

[52] Monax. *Explainer: Permissioned Blockchains.* https://monax.io/explainers/permissioned_blockchains/ (12 July, date last accessed)

[53] 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.

[54] BlockGeeks. *Proof of Work vs Proof of Stake: Basic Mining Guide.* https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/ (14 July 2017, date last accessed)

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

their own agendas and interests by replacing them with algorithms.[56] This is a nearly ideal setting for even bigger, better, faster, and cheaper transactions.[57]

One of the well-known platforms of smart contracts on public blockchains is Ethereum.[58] 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.[59]

In 2016, a decentralized autonomous organization project (the 'DAO') was launched on Ethereum's public blockchain using a nexus of smart contracts.[60] In the particular project, the idea was to have an investment entity which is fully controlled by shareholders, without a central management team.[61] The work of management was to be replaced by autonomously running smart contracts. The project received USD 150 million in Ether[62] in a crowdfunding initiative. Shortly after the project was launched, a hacker managed to divert Ether worth USD 50 million from the organization, which ultimately led to the collapse of the project.[63] An interesting open question is whether the taking, which simply exploited a weakness in the code, was breaching the contract or simply following the contract as implemented in the code.[64]

Consortium blockchains are blockchains that are used by a limited number of participants and designed to fit the needs of a particular industry.[65] Examples include the R3 Corda project[66] and Enterprise

[56] 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.

[57] It might be important to stress here that we talk about trust towards the technology underlying smart contracts. We do not talk about building trust among customers towards any particular service or other applications of blockchain technology or smart contracts.

[58] 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 (11 July 2017, date last accessed)

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

[60] For the general foundations, see Buterin V. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. *Ethereum Blog* (6 May 2014) https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ (12 July 2017, date last accessed)

[61] Raskin M. The Law and Legality of Smart Contracts. *Georgetown Law and Technology Review* 2017; **1**: 305-341. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166 (11 July 2017, date last accessed) 336

[62] Ether is Ethereum's cryptocurrency.

[63] Popper N. Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency. *New York Times* (16 June 2016) http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removedmore-than-50-million-from-experimental-cybercurrency-project.html (11 July 2017, date last accessed)

[64] Levine M. Blockchain Company's Smart Contracts Were Dumb. *Bloomberg View* (17 June 2016) http://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contractswere-dumb (11 July 2017, date last accessed)

[65] Buterin V. *On Public and Private Blockchains, Ethereum Blog* (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (11 July 2017, date last accessed)

[66] Brown RG. *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services, Blog Post* (5 April 2017) http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services (11 July 2017, date last accessed)

Ethereum Alliance.[67] 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.

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.[68] 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.[69]
4. **Openness:** 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.[70]

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'.[71] 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.[72][73]

[67] Enterprise Ethereum Alliance. https://entethalliance.org/about/ (11 July 2017, date last accessed)

[68] Buterin V. *On Public and Private Blockchains, Ethereum Blog* (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (11 July 2017, date last accessed)

[69] Monax. *Explainer: Permissioned Blockchains* https://monax.io/explainers/permissioned_blockchains/ (11 July 2017, date last accessed)

[70] Buterin V. *On Public and Private Blockchains, Ethereum Blog* (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (11 July 2017, date last accessed)

[71] Buterin V. *On Public and Private Blockchains, Ethereum Blog* (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (11 July 2017, date last accessed)

[72] JP Morgan. *Distributed Ledger Technology.* https://www.jpmorgan.com/global/distributed-ledger-technology (11 July 2017, date last accessed)

[73] It is yet to be confirmed whether we could consider the Keyless Signature Infrastructure (KSI) blockchain technology that has been used by the Estonian government next to the traditional public key infrastructure (PKI) as another example of private blockchain. The KSI is currently used to preserve the integrity of several vital registries (business registry, land registry, e-health records) in Estonia. Estonian government was the first government in the world to embrace the blockchain technology in its live production systems and the KSI lies at the foundation of Estonia’s digital society since 2007. The government provides scalable digital signature based authentication for electronic data, machines and humans to ensure the integrity of systems and data. 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

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

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[74] Ripple[75]
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[76]
Supply Chain	Loss of goods, insurance fraud, authenticity of high value goods, evaluation of provenance	Smart contract system would create immutable record of good along supply chain[77]	Everledger[78]
Music Royalties	Up to 50% of music royalty payments are not received by right owners[79]	Blockchain system could help to create a world-wide database of music metadata,[80] which could then in turn be used to trigger	So far only preliminary

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, Kroonmaa A, Laanoja R. Keyless Signatures Infrastructure: How to Build Global Distributed Hash-Trees. In: Riis Nielson H, Gollmann D (eds). *Secure IT Systems. NordSec 2013. Lecture Notes in Computer Science Vol 8208*. Berlin, Heidelberg: Springer, 2013, https://eprint.iacr.org/2013/834.pdf (11 July 2017, date last accessed)

[74] It should be noted that R3's CTP claims that Corda is *not* a blockchain. See Brown RG. *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services, Blog Post* (5 April 2017) http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services (11 July 2017, date last accessed). It could be argued, however, that it simply is a special type of permissioned blockchain.

[75] 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/ (11 July 2017, date last accessed)

[76] Kuo T, Hsu C, Ohno-Machado L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modelling Framework on Private Blockchain Networks. *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 (11 July 2017, date last accessed)

[77] Kim HM, Laskowski M. *Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance. Conference Paper for Workshop on Information Technology and Systems (WITS)* (15-16 December 2016) https://arxiv.org/abs/1610.02922 (11 July 2017, date last accessed)

[78] See for example London-based start up Everledger: https://www.everledger.io/ (11 July 2017, date last accessed)

[79] Botsford, L. *BerkleeICE's Rethink Music Releases Report on Transparency and Fairness in the Music Industry*. https://www.berklee.edu/news/fair_music_report (11 July 2017, date last accessed)

[80] Music Business Worldwide. *ASCAP, PRS and SACEM Join Forces for Blockchain Copyright System* (9 April 2017) https://www.musicbusinessworldwide.com/ascap-prs-sacem-join-forces-blockchain-copyright-system/ (11 July 2017, date last accessed)

		automatic royalty payments to rightholders through the deployment of smart contracts	proposals[81,82]

The financial services industry has been the most active in trying to make use of smart contract systems.[83] Two areas in which transaction costs could be significantly lowered by the use of smart contracts are the settlement of securities transactions and international remittances. The settlement of securities transactions takes currently three days (so-called 'T+3') for most types of securities, such as stock and corporate bonds, and still involves risks.[84] Smart contracts would increase the speed of such settlements, make intermediaries like clearing houses redundant, and eliminate risks. Similarly, international remittances, i.e. the international money transfers, usually necessitate intermediation by correspondent banks.[85] The current costs of sending a small international remittance is about 7.7 per cent.[86] Smart-contract based systems could do away with correspondent banking and could greatly reduce the cost, time and safety for sending international remittances.[87]

Cross-industry experimentation with smart contracts is just beginning. In February 2017, about thirty Fortune 500 companies, including financial institutions, media agencies and technology companies decided to join forces to develop a private version of the Ethereum blockchain.[88] The project takes place under a newly funded non-profit organization, the Enterprise Ethereum Alliance.[89] The goal of this project is to develop an open standard that could be appropriated by different industries for different uses. The project also aims at advancing in tandem with public Ethereum, with the possible future option of combining versions of private and public Ethereum.[90] It appears that Ethereum is set to evolve into the standard blockchain for smart contracts.

For the rest of our analysis, **we will focus on bilateral or multilateral smart contracts that represent a translation of a specific contractual agreement with legal force, as our focus is on legal implications of smart contracts. Furthermore, we will mainly focus on smart contracts on public**

[81] Wallach DA. Bitcoin for Rockstars. *Wired* (12 October 2014) https://www.wired.com/2014/12/bitcoin-for-rockstars/ (11 July 2017, date last accessed)

[82] Music Business Worldwide. *ASCAP, PRS and SACEM Join Forces for Blockchain Copyright System* (9 April 2017) https://www.musicbusinessworldwide.com/ascap-prs-sacem-join-forces-blockchain-copyright-system/ (11 July 2017, date last accessed)

[83] Cuccoro gives three reasons for why the financial services industry is an ideal testing ground for smart contracts: (i) financial institutions deal with standardized terms and objective variables, (ii) automation of transactions by computers is feasible and desirable, (iii) financial institutions operate in an already highly interdependent environment. See Cuccuru P. Beyond Bitcoin: An Early Overview on Smart Contracts. *International Journal of Law and Information Technology* 2017; **0**: 1–17

[84] IMF. *Virtual Currencies and Beyond: Initial Considerations. Staff Discussion Note SDN/16/03.* 2016 https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (11 July 2017, date last accessed) 22

[85] Correspondent banking services are offered by banks acting as intermediaries that enter into agreements to provide payment services to each other, which allows the provision of cross-border payments to their customers.

[86] IMF. *Virtual Currencies and Beyond: Initial Considerations. Staff Discussion Note SDN/16/03.* 2016 https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (11 July 2017, date last accessed) 22

[87] The Bitcoin-based remittance system is already being used in some jurisdictions for international remittances, e.g. Philippines and Kenya. A consortium system would allow for international remittances without having to resort to bitcoin.

[88] Popper N. Business Giants to Announce Creation of a Computing System Based on Ethereum. *New York Times* (27 February 2017) https://www.nytimes.com/2017/02/27/business/dealbook/ethereum-alliance-business-banking-security.html?_r=0 (12 July 2017, date last accessed)

[89] Enterprise Ethereum Alliance. https://entethalliance.org/about/ (11 July 2017, date last accessed)

[90] Enterprise Ethereum Alliance. https://entethalliance.org/about/ (11 July 2017, date last accessed) see also Peck M. Corporate Titans Unite to Build an Enterprise Version of the Ethereum Blockchain. *IEEE Spectrum* (2 March 2017) http://spectrum.ieee.org/tech-talk/computing/networks/enterprise-ethereum-alliance-launches (11 July 2017, date last accessed)

blockchains as they present more challenges from a regulatory perspective, in particular due to the possible anonymity or pseudonymity of public blockchain users. In order to still provide comprehensive picture of the blockchain landscape, discussions on private blockchains will be included in the analysis to illustrate some of their advantages over public blockchain from a regulatory perspective.

3. Safeguards for implementing smart contracts in no-trust environments

3.1. No-trust environment

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 will decide not to engage in economic transactions.

Prior to blockchain, there were two main mechanisms that helped to bring about the necessary trust for economic exchange: Peer-to-peer and Leviathan trust mechanisms.[91] In 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 fulfill their obligations.[92] 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, language, family ties or religious beliefs. Fear of losing reputation will cause members of such a community not to behave opportunistically towards other members.

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 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.[93]

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 themselves provide guarantees for performance. 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.[94]

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. How could blockchain's 'trustless trust' offer a new trust environment for trade?[95] How can smart contracts function in no-trust contracting environments which are characterized by parties meeting in complete anonymity and there being no formal contract law or institutionalized intermediaries for ensuring the enforcement of contracts? The answer lies in their technological nature. Due to the success of Bitcoin, the combination of

[91] This terminology is taken from Werbach K. Trustless Trust. https://ssrn.com/abstract=2844409 (14 August 2016, date last accessed) 4

[92] See also Section 3.6 below on relational theory of contracts.

[93] Werbach K. Trustless Trust. https://ssrn.com/abstract=2844409 (14 August 2016, date last accessed) 17. Putnam R. *Bowling Alone: The Collapse and Revival of American Community.* New York: Simon & Schuster, 2000, 135

[94] 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 landing 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.

[95] Werbach K. Trustless Trust. https://ssrn.com/abstract=2844409 (14 August 2016, date last accessed) 538

decentralization, cryptographic open source protocols, and crypto-proof consensus signals a high degree of reliability of blockchain technology.

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 enforcement.

3.2. Identification as a safeguard for implementing smart contracts

Let us discuss the first option on the basis of considering possible higher standards for identification on public blockchain. We shall use the example of bitcoin assuming that the general underlying principles of operating smart contracts on public blockchains are sufficiently similar. We analyzed earlier whether it would be possible for the facilitator of the exchange of bitcoins to save data about its clients and verify the identity of the clients and whether it would be consistent with the bitcoin protocol and rules to implement a review procedure, which would require a decrease in the anonymity principle characteristic of bitcoin sales transactions. During the discussion we concluded that the facilitator is indeed able to record to which and from which bitcoin address the bitcoins flow, and while the information is not linked to a particular user it could still be used to identify parties to the transaction. At the same time, the bitcoin protocol cannot be extended to keep track of users' identities without major changes. Accordingly, there are significant difficulties in implementing any review procedures (e.g. where public authorities require the bitcoin exchange service providers to check the identity of the person who wishes to open a bitcoin wallet or exchange bitcoin for conventional currency).

While we do not advocate them, one could consider the following tracks for responding to the difficulties with implementing bitcoin specific review procedures. **First,** transactions that involve both bitcoins and normal currencies could be regulated. Countries tend to opt for subjecting bitcoin exchanges to the existing regulation on financial services. In order for the facilitators of the bitcoin exchange to be fully compliant with the regulations governing other financial intermediaries i.e. anti-money laundering laws, they could be required to collect some personal data about their customers.[96]

For example, whenever someone facilitates an exchange of goods or normal currencies for bitcoins, he could be required to keep a record of that transaction, together with the data about the person who provided or received the goods or normal currency (for example, the shipping address for the goods could be recorded). It is also possible to require vendors and facilitators of exchange to require IDs from their clients whenever a transaction is performed (e.g. login via ID card). However, that would:-

1. make the transactions more complicated because it involves an additional step of authentication;
2. exclude clients who do not have the means to identify themselves (e.g. clients who do not have an ID card or opt not to use it for security reasons); and
3. make it very difficult for vendors and facilitators of exchange to have clients from other jurisdictions where other means of identification are used.[97]

[96] Eenmaa-Dimitrieva and Unruh Report 2016

[97] Eenmaa-Dimitrieva and Unruh Report 2016

This does not fully eliminate jurisdictional issue explained above, but stays in line with the recent legal positions adopted in the United States (US) and the European Union (EU).[98] In sum, the option of subjecting bitcoin exchanges to the existent regulation on financial services does not interfere with the blockchain protocol. Applicable legal rules would rather add several more obligations on the top.[99]

Second, regardless of any review procedure, each bitcoin transaction leaves a digital trace which is recorded in the public ledger. Because of the public ledger, using sophisticated analysis, transactions involving large quantities of bitcoin can be tracked and if paired with current law enforcement tools it would be possible to gain a lot of information on the persons involved in the transactions with bitcoins[100]. This information can be used in order to analyse certain information about the users, particularly considering that the information is shared by users voluntarily.[101]

Several methods of analysing this data are described below. It should be noted that all of them rely on certain set of circumstances and do not guarantee 100% traceability of the given transaction or the identities of people connected with particular addresses.

- Order books for bitcoin exchanges are typically available to support trading tools. As orders are often placed in bitcoin values converted from other currencies, they have a precise decimal value

[98] Treatment of bitcoins like other currencies seems to gain international recognition at least for the purposes of tax and anti-money laundering. The US was the first to take steps towards the application of existing laws and regulations to bitcoins. This is illustrated by cases like (1) Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust, and (2) US v. Faiella and Shrem. In the first, the court entered judgment against Trendon T. Shavers and Bitcoin Savings and Trust ('BTCST') and found the violations of Securities Act of 1933 and Securities Exchange Act of 1934 (See: U.S. Securities and Exchange Commission Litigation Release No. 23090 from September 22, 2014 on Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust. Civil Action No 4:13-CV-416. https://www.sec.gov/litigation/litreleases/2014/lr23090.htm (12 July 2017, date last accessed).) This is considered the first case addressing the question of whether digital currency issued without the backing of a government or other official entity is to be legally considered money. In this case investment of bitcoins was declared equivalent to the investment of money. A similar statement regarding considering bitcoins money was issued in US v. Faiella and Shrem, where Charlie Shrem and Robert Faiella were charged of operating an unlicensed money transmitting business, money laundering conspiracy and wilful failure to file a suspicious activity report (See: Macheel T. 4 Court Cases Helping Shape the US Stance on Bitcoin. *Coindesk* (28 September 2014) http://www.coindesk.com/4-court-cases-helping-determine-us-stance-bitcoin/ (12 July 2017, date last accessed).) US anti-money laundering law and money transmission law were also invoked in cases US v. Ross William Ulbricht and State of Florida v. Espinoza. In the recent US Congressional Research Service's publication on bitcoins researchers stated that they: '[…] have identified some federal statutes and regulatory regimes that may have some applicability to digital currency, although none contains explicit language to that effect or explicitly mentions currency not issued by a government authority. […] For example, courts are likely to hold that the federal criminal mail and wire fraud statutes apply to fraudulent schemes designed to result in monetary losses in connection with buying, selling, or trading digital currencies.' (Murphy EV, Murphy MM, Seitzinger MV. *Bitcoin: Questions, Answers, and Analysis of Legal Issues. Congressional Research Service Report* (13 October 2015) https://fas.org/sgp/crs/misc/R43339.pdf (11 July 2017, date last accessed) 9) Another set of examples of regulations applicable to the virtual currencies is provided by tax regulations. (See: IRS. *Notice 2014-36. IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes. General Rules for Property Transactions Apply.* https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance (11 July 2017, date last accessed)) In this context it is also worth noting that the European Banking Authority (EBA) has recommended subjecting virtual currency exchanges to the anti-money laundering and counter-terrorist financing requirements. (See: European Banking Authority. *EBA Opinion on 'virtual currencies'* (4 July 2014) https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (11 July 2017, date last accessed) 6)

[99] Eenmaa-Dimitrieva and Unruh Report 2016

[100] Murphy EV, Murphy MM, Seitzinger MV. *Bitcoin: Questions, Answers, and Analysis of Legal Issues. Congressional Research Service Report.* (13 October 2015) https://fas.org/sgp/crs/misc/R43339.pdf (11 July 2017, date last accessed) 3

[101] Eenmaa-Dimitrieva and Unruh Report 2016

with eight significant digits. It may be possible to find transactions with corresponding amounts and thus map public-keys and transactions to the exchanges;[102]

- Over an extended time period, several public-keys, if used at similar times, could in a great likelihood belong to the same user. It may be possible to construct and cluster a co-occurrence network to help deduce mappings between public-keys and users;[103]
- Security researcher Dan Kaminsky has performed an analysis of the bitcoin system, investigating identity leakage at the TCP/IP layer. He found that by opening a connection to all public peers in the network at once, he could map IP addresses to bitcoin public-keys, working from the assumption that 'the first node to inform you of a transaction is the source of it. . . [this is] more or less true, and absolutely over time'. Using this approach it is possible to map public-keys to IP addresses unless users are using an anonymising proxy technology such as TOR[104]. The approach may not be feasible via a government or facilitator because it involves active hacking (not just the evaluation of public data). Biryukov et al. showed that such attacks are even possible when the users are behind NAT (Network Address Translation) (the most common case in the current bitcoin network)[105].[106]

The first and second option (regulating transaction together with identification, and tracking) suggested above approach the issue from two different stances. Their combined and simultaneous application might bring results. Such a review procedure would combine technical methods in data analysis with the existing legal rules regulating the provision of financial services, supplementing them in limited spheres, as the case may be, by the specific virtual currency regulations.[107] Such safeguards for enforcement are certainly invasive regarding anonymity and essentially create an overwhelming need to use permissioned blockchains for smart contracts.

3.3. Regulatory challenges

While we claim that smart contracts can provide sufficient safeguards for enforcement in no-trust environment, we do not mean to say that such safeguards could only be invasive regarding anonymity. We analyzed this possibility above, but this is not the only available option. A more democratic alternative, as we claim, is providing such safeguards by incorporating them into the code of smart contracts. In this manner, we avoid certain inefficiencies arising from the automated execution of smart contracts and mimic the efficiency-enhancing features of contract law while preserving the anonymity of parties, the essential (i.e. the central characteristic) feature of operating on a public blockchain.

What are the regulatory challenges that we need to meet when considering the regulation of smart contracts? The questions of what is the applicable law and what the law should be, become vividly

[102] Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds). Security and Privacy in Social Networks. New York: Springer, 2013, 197-223 https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (11 July 2017, date last accessed) 25

[103] Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds). Security and Privacy in Social Networks. New York: Springer, 2013, 197-223 https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (11 July 2017, date last accessed) 25

[104] Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds). Security and Privacy in Social Networks. New York: Springer, 2013, 197-223. https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (11 July 2017, date last accessed) 17

[105] Pustogarov I. Informal description of the client deanonymization attack on the Bitcoin P2P network. *CryptoLUX* https://www.cryptolux.org/index.php?title=Bitcoin&oldid=1257 (11 July 2017, date last accessed). Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. *ArXiv e-prints* https://arxiv.org/pdf/1405.7418.pdf (11 July 2017, date last accessed)

[106] Eenmaa-Dimitrieva and Unruh Report 2016

[107] Eenmaa-Dimitrieva and Unruh Report 2016

apparent and urgent in case of smart contracts that operate on public blockchains. This derives from the facts that:

- 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 conflict of laws;
- Consensus: Being immutable, blockchain transactions, by definition, cannot be changed. Accordingly, new processes need to be introduced for making alterations in parties' relations with each other, if needed;
- Openness: Since the transactions are also transparent, they pose a potential privacy threat.

In contrast, when we take a look at the regulatory challenges for smart contracts operating on permissioned blockchains, we see that they might possibly raise less challenges thanks to the fact that:

- 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
- Openness: Content of blocks can be hidden avoiding confidentiality issues.

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 in 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 democratic 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.[108] 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 the 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. For example, we need to think whether and how to defend markets and other aspects of good life when we use blockchain instead of central organizations. Additionally, we need to think how to implement safety-measures or procedures when they are needed, considering that the

[108] Reijers W, O'Brolcháin F, Haynes P. Governance in Blockchain Technologies & Social Contract Theories. *Ledger* 2016; 1: 134-151. https://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62/51 (11 July 2017, date last accessed) 134

technologies could operate without central authorities like central registries,[109] central adjudication,[110] or intermediaries such as banks, brokers, custodians.[111] There may be continued interest in a number of safety-measures, which the markets together with the governmental institutions are currently providing us. 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;[112]
- Protection mechanisms like consumer protection, investor protection, protection of competition on the market;
- Measure for keeping certain activities within the socially permitted boundaries (boundaries to terrorist financing or money laundering);
- Responses to social needs, including censorship needs, asset location important for seizing.[113]

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.[114] 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.'[115] 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.[116] 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.'[117] 'Smart contracts are unprecedented methods of ensuring contractual compliance, including social contracts.'[118] 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

[109] E.g. see: Wong JI. Sweden's blockchain-powered land registry is inching towards reality. *Quartz Daily Brief* (3 April 2017) https://qz.com/947064 (12 June 2017, date last accessed)

[110] Buterin V. Decentralized Court. *Reddit*. https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/ (12 June 2017, date last accessed). Kaminska I. Decentralised courts and blockchains. *FT Alphaville* (9 May 2016) https://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/ (12 June 2017, date last accessed)

[111] Veerpalu A. *Regulation of Blockchain Technology and its Challenges. Presentation at the ELSA Colloquium of IT LAW for PhD students and researchers. University of Aix-Marseille. 17 February 2017*

[112] See for further analysis in Sections 3.4 and 3.5 below.

[113] This is developed based on a previous similar list created by Anne Veerpalu.

[114] See: Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books, 1999. Werbach K, Cornell N. Contracts Ex Machina. Duke Law Journal; Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed)

[115] Reyes CL. Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. *Villanova Law Review* 2016; 61 http://ssrn.com/abstract=2766705 (11 July 2017, date last accessed) 230

[116] See: Latour B. On Technical Mediation. *Common Knowledge* 1994; 3 (2): 29. Cohen JE. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press, 2012. Werbach K, Cornell N. Contracts Ex Machina. Duke Law Journal; Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed)

[117] Savelyev A. *Contract Law 2.0: 'Smart' Contracts As the Beginning of the End of Classic Contract Law.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 (11 July 2017, date last accessed)

[118] Tapscott D, Tapscott A. *Blockchain Revolution: How The Technology Behind Bitcoin is Changing Money, Business and The World*. UK: Penguin Random House, 2016, 47

of the court system.[119] 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 still kept available at the moment as a backstop.[120]

This should not keep us from analyzing what should the law that operates as part of the code be like. Let us take a look at the regulatory challenges of smart contracts from the perspective of law and economics.

3.4. Efficiency considerations regarding safeguards for implementing smart contracts

The discipline of law and economics takes legal reality and analyses it from an economic efficiency perspective.[121] 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.[122] The economic function of contract law is considered to be the prevention of inefficient opportunistic behavior 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.[123] Further studies 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 a subset in the studies of social cooperation mechanisms which is generally referred to as relational theory of contract.[124]

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.[125] Twenty years ago, Szabo expected smart contracts to improve four basic contract objectives: the observability (both parties can observe each other's performance), the verifiability (easy verification if and when contract has been performed),

[119] Marvin R. Blockchain in 2017: The Year of Smart Contracts. *PC MAG* (12 December 2016) http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts (June 12, 2017, date last accessed)

[120] 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 wave 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/ (12 June 2017, date last accessed)

[121] Posner R. *Economic Analysis of Law. 8th edition*. New York: Aspen Publishers, 2011, 29

[122] Hermalin BE, Katz AW, Craswell R. Contract Law. In: Polinsky R, Shavell S. *Handbook of Law and Economics.* Amsterdam: Elsevier, 2007 http://www.sciencedirect.com/science/handbooks/15740730 (11 July 2017, date last accessed) 7

[123] 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 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: Cooter R, Ulen T. *Law and Economics. 6th ed.* Essex: Pearson, 2012, 285

[124] Important foundational works for the relational theory of contract are Macaulay S. Non-Contractual Relations in Business: A Preliminary Study. *American Sociological Review* 1963; 28 (1): 55-67 and Macneil I. Relational Contract: What We Do and Do Not Know. *Wisconsin Law Review* 1985; 4: 483-525

[125] Werbach K, Cornell N. Contracts Ex Machina. Duke Law Journal; Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed)

privity (only the necessary details for completion of the contract are revealed) and enforceability (automatic self-enforcement).[126] Werbach and Cornell conclude their recent study on the potential and the limitations of smart contracts with 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.

When we look into how smart contracts operate below, 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. 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. After that, we will discuss how to overcome some of these criticisms through the design of smart contracts.

This section is based on arguments provided in recent literature on smart contracts that tries to evaluate them from a contract law perspective.[127] In this literature, shortcomings of smart contracts compared to traditional, court-enforced contracts are highlighted. Some of the claimed advantages of traditional contracts over smart contracts are also advantages from an efficiency perspective. In a first step, we will therefore pick up the criticisms of smart contracts and translate them into an efficiency account. Most of these criticisms implicitly assume smart contracts on public blockchains. We will therefore, in a second step, show that these criticisms are less justified when using smart contracts on permissioned systems. Lastly, we will provide arguments showing the advantages of smart contracts 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.

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[128] provide excuses for non-performance and defenses 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).[129] As smart contracts are self-enforcing, performance of the contract will occur even though from a legal perspective the contract is invalid.[130] 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.[131]

[126] Szabo N. Smart Contracts: Building Blocks for Digital Markets, Extropy 1996; 16 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (11 July 2017, date last accessed).

[127] Savelyev A. *Contract Law 2.0: 'Smart' Contracts As the Beginning of the End of Classic Contract Law.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 (11 July 2017, date last accessed). Werbach K, Cornell N. Contracts Ex Machina. Duke Law Journal; Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed). Raskin M. The Law and Legality of Smart Contracts. *Georgetown Law and Technology Review* 2017; 1: 305-341 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166 (11 July 2017, date last accessed)

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

[129] Cooter R, Ulen T. *Law and Economics. 6th ed.* Essex: Pearson, 2012, 294-299

[130] Savelyev A. *Contract Law 2.0: 'Smart' Contracts As the Beginning of the End of Classic Contract Law.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 (11 July 2017, date last accessed) 19. Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 46

[131] Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 46

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.[132] As in the case of other formation defenses and excuses, smart contracts cannot account for whether a party had the capacity to enter into a contract, unless an identity 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. 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.[133] Consequently, it is also difficult or impossible to establish whether the party had legal capacity to enter into the contract.

Certain protections awarded under contract law to consumers have also been mentioned as a challenge for smart contracts.[134] Consumer protection measures in contract law remedy market failures of a monopoly type and of asymmetric information between consumers and businesses.[135] It is claimed that these protection measures could only be implemented with great difficulty by smart contracts.[136]

Lastly, courts will not enforce contracts that have an illegal purpose. A smart contract programmed to enforce a price-fixing cartel,[137] or to transfer illegal drugs or arms, imposes externalities on society. While enforcement agencies would take action in such cases, they would powerless in trying to stop the execution of the smart contract, due to its self-enforcing nature.[138] The example of The DAO is a vivid example of what happens when the blockchain and smart contract system do not provide safeguards against illegality due to a weakness in the smart contracts' code.[139]

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.[140]

[132] Cooter R, Ulen T. *Law and Economics. 6th ed.* Essex: Pearson, 2012, 342

[133] Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 49

[134] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 26

[135] Cooter R, Ulen T. *Law and Economics. 6th ed.* Essex: Pearson, 2012, 297-298

[136] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 26

[137] On algorithmic collusion see Ezrachi A, Stucke ME. *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Cambridge: Harvard University Press, 2016

[138] Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 50

[139] Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 50. See also section 2.4 above.

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

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.[141] Filippi and Wright argue the same in relation to consumer protection provisions.[142]

Nonetheless, consumer protection, for example could actually be enhanced in different ways by smart contracts. In contrast to critics, Fairfield emphasises that the gains in consumer protection through use of smart contracts would be superior to consumer protection provided by courts.[143] 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.[144] 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.

Permissioned blockchain: Another more general point could be made in relation to traditional ex-post correction mechanisms regarding to contract formation and validity (mistake, fraud, duress, necessity). If parties chose to implement their smart contracts on a permissioned blockchain, it could be possible to reach a consensus to reverse smart contract transactions on a permissioned blockchain that have been made on the basis of a mistake or other flaw. As the identities of parties to smart contracts would be known (i.e. there would be no anonymity), this would also make the implementation of a corresponding court order possible. Furthermore, users' identities could be verified when registering with the system, curing some problems with capacity.

Public blockchain: In relation to traditional ex-post mechanism, 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).[145] In a goods sale, for example, a multisig smart contract could e.g. require the signature of two 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.

In relation to possible illegal transactions through smart contracts, the openness of public blockchains could be an advantage. As all blocks 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

[141] Savelyev A. *Contract Law 2.0: 'Smart' Contracts As the Beginning of the End of Classic Contract Law.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 (11 July 2017, date last accessed) 19. Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 47

[142] 'Although implementing basic contractual safeguards and consumer protection provisions into smart

contracts is theoretically possible, in practice, it may prove difficult given the formalized and deterministic character of code.' Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 26

[143] Fairfield J. Smart Contracts, Bitcoin Bots, and Consumer Protection. *Washington and Lee Law Review Online* 2014; 71: 35-50

[144] Fairfield J. Smart Contracts, Bitcoin Bots, and Consumer Protection. *Washington and Lee Law Review Online* 2014; 71: 35-50 at 46

[145] Werbach K, Cornell N. Contracts Ex Machina. Duke Law Journal; Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 25. Buterin V. Bitcoin Multisig Wallet: The Future of Bitcoin. *Bitcoin Magazine* (13 March 2014) https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504/ (11 July 2017, date last accessed)

already provide a deterrent for entering into illegal smart contracts.[146] 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.[147]

3.5. Efficient breach

A defining feature of smart contracts is that they are self-enforcing, which gives a different meaning to breach of contract. While the self-enforcing 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 cost of performing the contract turn out to outweigh its value are viewed as a common practice and are deemed acceptable (even if wrongful nevertheless)[148] as long as the breaching party pays damages to the victim.[149]

In a way, traditional contract law in common law provides an avenue for parties to walk away from their contractual promises, and take advantage of more beneficial alternatives to promise-keeping, as long as the victim of the breach is fully compensated for the costs of non-performance by the breacher 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.[150]

The fact that due to automatic enforcement 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.[151] From the point of view of efficiency, the result of automatic enforcement of smart contracts could lead to excessive enforcement of contracts, 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.[152] 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,[153] this argument does not work in the case of smart contracts. Since they are automatically enforced once placed on the blockchain, automated performance would not allow for renegotiation to achieve more efficient outcomes.[154]

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

[146] See on this point also Werbach K. Trustless Trust. https://ssrn.com/abstract=2844409 (14 August 2016, date last accessed) 63

[147] See Section 3.2 above.

[148] See Coleman J, Kraus J. Rethinking the Theory of Legal Rights. *Yale Law Journal* 1986; 95: 1335-71

[149] Posner R. *Economic Analysis of Law. 8th edition*. New York: Aspen Publishers, 2011, 149. See also Holmes OW. The Path of the Law. *Harvard Law Review* 1897; 10: 457, 462

[150] Posner R. *Economic Analysis of Law. 8th edition*. New York: Aspen Publishers, 2011, 151

[151] Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 44

[152] Cooter R, Ulen T. *Law and Economics. 6th ed.* Essex: Pearson, 2012, 328. Posner R. *Economic Analysis of Law. 8th edition*. New York: Aspen Publishers, 2011, 164

[153] Shavell S. Specific Performance Versus Damages for Breach of Contract: An Economic Analysis. *Texas Law Review* 2006; 84: 831-876

[154] Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed) 45

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 are external to a blockchain system and provide information as to whether certain conditions have been met.[155] 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 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 about the same state of the outside world.[156] 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.

3.6. Relational contracts and trustless reliability

Cooperation in contracting can also be achieved without relying on formal contract law. In his work 'Lawlessness and Economics', the 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.[157] 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.

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.[158] 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. The shorthand used by economists for such relational contracts is to define them as 'informal agreements sustained by the value of future relationships'.[159]

In both Dixit’s 'lawless' contracting environment and a relational contracting environment,[160] there exist social mechanisms that function as alternatives to formal contract law, which rely mainly on trust,

[155] Thomas S, Schwartz E. *Smart Oracles: A Simple, Powerful Approach to Smart Contracts.* https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts (11 July 2017, date last accessed)

[156] To see how Thomas and Schwartz explain how multi-signatures schemes could enhance the objectivity of the information provided by oracles, see: Thomas S, Schwartz E. *Smart Oracles: A Simple, Powerful Approach to Smart Contracts.* https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts (11 July 2017, date last accessed)

[157] Dixit A. *Lawlessness and Economics: Alternative Modes of Governance*. Princeton University Press, 2007

[158] Dixit A. *Lawlessness and Economics: Alternative Modes of Governance*. Princeton University Press, 2007. Macneil I. Contracts: Adjustment of Long-Term Economic Relations under Classical, Neoclassical, and Relational Contract Law. *Northwestern University Law Review* 1978; 72 (6): 854-905. Feinman JM. Relational Contract Theory in Context. *Northwestern University Law Review* 2000; 94(3): 737-48

[159] Baker GP, Gibbons R, Murphy KJ. Relational Contracts and the Theory of the Firm. *Quarterly Journal of Economics* 2002; 117: 39, 39

[160] Let us remind the reader that, in our understanding, in a lawless environment, there is no law available to the parties. In a relational environment, contract law is available but not used.

honesty or reputation among the parties of a business community to enforce agreements. Under certain conditions, these can prove to be more efficient than relying on formal contract law.[161]

When it comes to assessing smart contracts from a relational perspective, Levy (2017) criticizes that they cannot replicate the design of relational context in which contracts are usually concluded.[162] She argues, in line with relational contract theory, that contracts are social tools and are not always meant to be enforced according to their letter. At times parties include deliberately unenforceable and vague terms in their contracts which are only meant as rough guidelines for behavior. The inclusion of vague terms that give no clear 'if..then' instructions are very difficult to translate into the language of code as required by smart contracts. Furthermore, parties sometimes decide willfully not to enforce a contract that has been breached by the other party in order to ensure a continued relationship. Automated enforcement of smart contracts might foreclose such relational uses of contract.

From our point of view, smart contracts nonetheless present an improvement for contracts which would be concluded in an environment with no particular pre-existing social context in which they are embedded. 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. In such a setting, contract law 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 in such a setting. Parties can avoid traditional contract law doctrines as tools for sustaining efficient exchange (or mandatory for other reasons) and favor smart contracts because of the combination of unique features of these contracts which help to avoid efficiency losses and increase reliability. These features include automatic enforcement, 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 no-trust mechanism provided by blockchain technology.[163] 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. In this case smart contracts could prove to be the only instrument available to ensure cooperation thanks to automatic enforcement.

When discussing the no-trust environment, 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 paradigmatic 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

[161] Macaulay S. Relational Contracts Floating on a Sea of Custom? Thoughts About the Ideas of Ian Macneil and Lisa Bernstein. *Northwestern University Law Journal* 2000; 94: 775-804

[162] Levy KEC. Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law. *Engaging Science, Technology and* Society 2017; 3: 1-15 https://doi.org/10.17351/ests2017.107 (11 July 2017, date last accessed)

[163] On blockchain’s trustless architecture see Section 3.1 above and Werbach K. Trustless Trust. https://ssrn.com/abstract=2844409 (14 August 2016, date last accessed)

reliable fashion.'[164] '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.'[165] As Anne 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'[166] and 'everything is based on crypto proof instead of trust'[167] as we have known it so far.[168]

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. Trusting the other contracting party is not necessary, because the technology will take care that the other party performs her obligation. Trusting a central authority is not necessary, because public blockchains escape any central control due to their decentralized nature. And 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.

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,[169] 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 blockchain leaves (the 'logs' created on 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 the blockchain technology that it provides foundations for consistent, public and shared transactions thereby using data integrity for guaranteeing higher data security than previous technologies.[170]

In such a manner, trust between parties would not be replaced by but supported by the trust in the technology powering smart contracts.[171] We call it the 'trustless reliability' of smart contracts. It is built on the automatic enforcement, decentralization, proofing mechanism underlying smart contracts, which provide the transparency and integrity of data. These important properties help us to put smart contracts

[164] UK Government. *Distributed Ledger Technology: Beyond Block Chain. A Report by the UK Government Chief Scientific Adviser*. Crown Copyright 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (July 11 2017, date last accessed) 13

[165] UK Government. *Distributed Ledger Technology: Beyond Block Chain. A Report by the UK Government Chief Scientific Adviser*. Crown Copyright 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (July 11 2017, date last accessed) 13

[166] Tapscott D, Tapscott A. *Blockchain Revolution: How The Technology Behind Bitcoin is Changing Money, Business and The World*. UK: Penguin Random House, 2016, 41

[167] Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed) 9

[168] Veerpalu A. *Regulation of the Use of Blockchain Technology in Creating Decentralized Organizations and Digital Identities: Comparative Study. PhD Research Proposal*. 2016

[169] See Section 3.4.

[170] Guardtime. *An Industrial Blockchain for IoT.* https://guardtime.com/solutions/internet-of-things (11 July 2017, date last accessed)

[171] Raskin M. The Law and Legality of Smart Contracts. *Georgetown Law and Technology Review* 2017; 1: 305-341. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166 (11 July 2017, date last accessed) 317-319

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.

4. Conclusion

The regulatory challenges facing smart contracts based on public blockchains and smart contracts based on permissioned blockchains are decidedly different. We compared these two different types of smart contracts based on four different features (the identifiability of persons transacting on blockchain, the selection of nodes and size of network together with the related expenses, the particularities of consensus mechanism, and the openness of the content of the blocks) ultimately focusing on anonymity for the following reasons.

On public blockchains, the users are able to remain anonymous to a significant extent. When you have anonymity you have a no-trust environment for contracting. Until recently, complete anonymity between parties would provide for the paradigm set of circumstances where we would imagine needing contract law. This is because due to the anonymity the contract was not embedded in any social context that could work as an alternative enforcement mechanism to ensure that all parties cooperate. In order to contract in no-trust environments, there is a need for an enforcement mechanism which provides sufficient safeguards for contracting.

Smart contracts seem to be able to function in contracting environments where parties could meet in complete anonymity. Interestingly, they can provide sufficient safeguards for enforcement. However, there is an important choice to be made in this regard. The safeguards could be either invasive regarding anonymity (e.g. direct to using permissioned blockchains) or they could be incorporated into the code of smart contracts to avoid certain inefficiencies arising from their automated execution (thus remaining on the public blockchain where the anonymity is defining feature). We have argued in this paper that the latter is a better alternative. It is applicable to all blockchains and provides grounds for developing smart contracts which are compatible with the central features of broadly accessible public blockchain - its anonymity and transparency. The latter are also some of the most important guarantees for the trustworthiness and security of data next to confidentiality.

As such, smart contracts offer a new mode of contracting governance, a vehicle for contracting while not relying on formal contract law, and an alternative mechanism for ensuring cooperative outcomes in transactions between two or more parties.

Bibliography

Agrello. https://www.agrello.org/ (12 June 2017, date last accessed)

Guardtime. *An Industrial Blockchain for IoT*. https://guardtime.com/solutions/internet-of-things (11 July 2017, date last accessed)

Baker GP, Gibbons R, Murphy KJ. Relational Contracts and the Theory of the Firm. *Quarterly Journal of Economics* 2002; 117: 39

Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. *ArXiv e-prints* https://arxiv.org/pdf/1405.7418.pdf (11 July 2017, date last accessed)

BlockGeeks. *Proof of Work vs Proof of Stake: Basic Mining Guide.* https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/ (14 July 2017, date last accessed)

Blockchain Technologies. *Blockchain Technology Explained.* http://www.blockchaintechnologies.com/blockchain-definition (5 June 2017, date last accessed)

Botsford L. *BerkleeICE's Rethink Music Releases Report on Transparency and Fairness in the Music Industry*. https://www.berklee.edu/news/fair_music_report (11 July 2017, date last accessed)

Brown RG. *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services, Blog Post* (5 April 2017) http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services (11 July 2017, date last accessed)

Buldas A, Kroonmaa A, Laanoja R. Keyless Signatures Infrastructure: How to Build Global Distributed Hash-Trees. In: Riis Nielson H, Gollmann D (eds). *Secure IT Systems. NordSec 2013. Lecture Notes in Computer Science Vol 8208*. Berlin, Heidelberg: Springer, 2013 https://eprint.iacr.org/2013/834.pdf (11 July 2017, date last accessed)

Buterin V. Bitcoin Multisig Wallet: The Future of Bitcoin. *Bitcoin Magazine* (13 March 2014) https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504/ (11 July 2017, date last accessed)

Buterin V. DAOs, DACs, DAs and More: An Incomplete Terminology Guide. *Ethereum Blog* (6 May 2014) https://blog.ethereum.org/2014/05/06/daos-dacsdas-and-more-an-incomplete-terminology-guide/ (14 April 2017, date last accessed)

Buterin V. Decentralized Court. *Reddit*. https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/ (12 June 2017, date last accessed)

Buterin V. Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. *Bitcoin Magazine* (23 January 2014) https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/ (11 July 2017, date last accessed)

Buterin V. On Public and Private Blockchains. *Ethereum Blog* (7 August 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (11 July 2017, date last accessed)

Cohen JE. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press, 2012

Coindesk. *How Does Blockchain Technology Work*. http://www.coindesk.com/information/how-does-blockchain-technology-work/ (12 July 2017, date last accessed)

Coleman J, Kraus J. Rethinking the Theory of Legal Rights. *Yale Law Journal* 1986; 95: 1335-71

Cooter R, Ulen T. *Law and Economics. 6th ed.* Essex: Pearson, 2012

Cuccuru P. Beyond Bitcoin: An Early Overview on Smart Contracts. *International Journal of Law and Information Technology* 2017; 0: 1–17

Dixit A. *Lawlessness and Economics: Alternative Modes of Governance*. Princeton University Press, 2007

The Economist. *Not-so-clever Contracts.* (28 June 2016) http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted (11 July 2017, date last accessed)

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

Eenmaa-Dimitrieva H, Unruh D. *Report on the Architecture and Anonymity of Bitcoin Transactions for the Supreme Court of Estonia* (7 January 2016)

Enterprise Ethereum Alliance. *https://entethalliance.org/about/ (11 July 2017, date last accessed)*

Ethereum White Paper. A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper (11 July 2017, date last accessed)

Ethereum. https://www.ethereum.org/ (12 July 2017, date last accessed)

European Banking Authority. *EBA Opinion on 'virtual currencies'* (4 July 2014) https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (11 July 2017, date last accessed)

Everledger. https://www.everledger.io/ (11 July 2017, date last accessed)

Ezrachi A, Stucke ME. *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Cambridge: Harvard University Press, 2016

Fairfield J. Smart Contracts, Bitcoin Bots, and Consumer Protection. *Washington and Lee Law Review Online* 2014; 71: 35-50

Feinman JM. Relational Contract Theory in Context. *Northwestern University Law Review* 2000; 94(3): 737-48

Hermalin BE, Katz AW, Craswell R. Contract Law. In: Polinsky R, Shavell S. *Handbook of Law and Economics.* Amsterdam: Elsevier, 2007 http://www.sciencedirect.com/science/handbooks/15740730 (11 July 2017, date last accessed)

Holmes OW. The Path of the Law. *Harvard Law Review* 1897; 10: 457

Ripple. *Technology.* https://ripple.com/technology/ (11 July 2017, date last accessed)

IMF. *Virtual Currencies and Beyond: Initial Considerations. Staff Discussion Note SDN/16/03.* 2016 https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (11 July 2017, date last accessed)

IRS. *Notice 2014-36. IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes. General Rules for Property Transactions Apply.* https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance (11 July 2017, date last accessed)

JP Morgan. *Distributed Ledger Technology.* https://www.jpmorgan.com/global/distributed-ledger-technology (11 July 2017, date last accessed)

Kaminska I. Decentralised courts and blockchains. *FT Alphaville* (9 May 2016) https://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/ (12 June 2017, date last accessed)

Kim HM, Laskowski M. *Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance. Conference Paper for Workshop on Information Technology and Systems (WITS)* (15-16 December 2016) https://arxiv.org/abs/1610.02922 (11 July 2017, date last accessed)

Kim HM, Laskowski M. *A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange. Working Paper.* 2017 http://blockchain.lab.yorku.ca/files/2017/05/UBC_blockchain_paper_HK_and-Marek.pdf (11 July 2017, date last accessed)

Kuo T, Hsu C, Ohno-Machado L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modelling Framework on Private Blockchain Networks. 2016 https://www.healthit.gov/sites/default/files/10-30-ucsd-dbmi-onc-blockchain-challenge.pdf (11 July 2017, date last accessed)

Latour B. On Technical Mediation. *Common Knowledge* 1994; 3 (2): 29

Lessig L. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999

Levine M. Blockchain Company's Smart Contracts Were Dumb. *Bloomberg View* (17 June 2016) http://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contractswere-dumb (11 July 2017, date last accessed)

Levy KEC. Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law. *Engaging Science, Technology and* Society 2017; 3: 1-15 https://doi.org/10.17351/ests2017.107 (11 July 2017, date last accessed)

Macaulay S. Non-Contractual Relations in Business: A Preliminary Study. *American Sociological Review* 1963; 28 (1): 55-67

Macaulay S. Relational Contracts Floating on a Sea of Custom? Thoughts About the Ideas of Ian Macneil and Lisa Bernstein. *Northwestern University Law Journal* 2000; 94: 775-804

Macheel T. 4 Court Cases Helping Shape the US Stance on Bitcoin. *Coindesk* (28 September 2014) http://www.coindesk.com/4-court-cases-helping-determine-us-stance-bitcoin/ (12 July 2017, date last accessed)

Macneil I. Contracts: Adjustment of Long-Term Economic Relations under Classical, Neoclassical, and Relational Contract Law. *Northwestern University Law Review* 1978; 72 (6): 854-905

Macneil I. Relational Contract: What We Do and Do Not Know. *Wisconsin Law Review* 1985; 4: 483-525

Marvin R. Blockchain in 2017: The Year of Smart Contracts. *PC MAG* (12 December 2016) http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts (June 12, 2017, date last accessed)

Monax. *Explainer: Permissioned Blockchains.* https://monax.io/explainers/permissioned_blockchains/ (11 July 2017, date last accessed)

Murphy EV, Murphy MM, Seitzinger MV. *Bitcoin: Questions, Answers, and Analysis of Legal Issues. Congressional Research Service Report* (13 October 2015) https://fas.org/sgp/crs/misc/R43339.pdf (11 July 2017, date last accessed)

Music Business Worldwide. *ASCAP, PRS and SACEM Join Forces for Blockchain Copyright System* (9 April 2017) https://www.musicbusinessworldwide.com/ascap-prs-sacem-join-forces-blockchain-copyright-system/ (11 July 2017, date last accessed)

Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008 https://bitcoin.org/bitcoin.pdf (11 July 2017, date last accessed)

Peck M. Corporate Titans Unite to Build an Enterprise Version of the Ethereum Blockchain. *IEEE Spectrum* (2 March 2017) http://spectrum.ieee.org/tech-talk/computing/networks/enterprise-ethereum-alliance-launches (11 July 2017, date last accessed)

Popper N. Business Giants to Announce Creation of a Computing System Based on Ethereum. *New York Times* (27 February 2017) https://www.nytimes.com/2017/02/27/business/dealbook/ethereum-alliance-business-banking-security.html?_r=0 (12 July 2017, date last accessed)

Popper N. Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency. *New York Times* (16 June 2016) http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removedmore-than-50-million-from-experimental-cybercurrency-project.html (11 July 2017, date last accessed)

Posner R. *Economic Analysis of Law. 8th edition*. New York: Aspen Publishers, 2011

Pustogarov I. Informal description of the client deanonymization attack on the Bitcoin P2P network. *CryptoLUX* https://www.cryptolux.org/index.php?title=Bitcoin&oldid=1257 (11 July 2017, date last accessed)

Putnam R. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000

Raskin M. The Law and Legality of Smart Contracts. *Georgetown Law and Technology Review* 2017; 1: 305-341. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166 (11 July 2017, date last accessed)

Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A (eds). *Security and Privacy in Social Networks*. New York: Springer, 2013, 197-223. https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (11 July 2017, date last accessed)

Reijers W, O'Brolcháin F, Haynes P. Governance in Blockchain Technologies & Social Contract Theories. *Ledger* 2016; 1: 134-151. https://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62/51 (11 July 2017, date last accessed)

Reyes CL. Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal. *Villanova Law Review* 2016; 61 http://ssrn.com/abstract=2766705 (11 July 2017, date last accessed)

Savelyev A. *Contract Law 2.0: 'Smart' Contracts As the Beginning of the End of Classic Contract Law.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 (11 July 2017, date last accessed)

Scardovi C. *Restructuring and Innovation in Banking*. Springer, 2016 https://play.google.com/store/books/details?id=uNM0DQAAQBAJ (5 June 2017, date last accessed)

Shavell S. Specific Performance Versus Damages for Breach of Contract: An Economic Analysis. *Texas Law Review* 2006; 84: 831-876

Surden H. Computable Contracts. *UC Davis Law Review* 2012; **46**: 629

Szabo N. Smart Contracts: Building Blocks for Digital Markets, Extropy 1996; 16. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (11 July 2017, date last accessed)

Tapscott D, Tapscott A. *Blockchain Revolution: How The Technology Behind Bitcoin is Changing Money, Business and The World*. UK: Penguin Random House, 2016

Thomas S, Schwartz E. *Smart Oracles: A Simple, Powerful Approach to Smart Contracts.* https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts (11 July 2017, date last accessed)

UK Government. *Distributed Ledger Technology: Beyond Block Chain. A Report by the UK Government Chief Scientific Adviser*. Crown Copyright 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (July 11 2017, date last accessed)

US Securities and Exchange Commission. *Litigation Release No. 23090 from September 22, 2014 on Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust. Civil Action No 4:13-CV-416.* https://www.sec.gov/litigation/litreleases/2014/lr23090.htm *(12 July 2017, date last accessed)*

Veerpalu A. *Regulation of the Use of Blockchain Technology in Creating Decentralized Organizations and Digital Identities: Comparative Study. PhD Research Proposal.* 2016

Veerpalu A. *Regulation of Blockchain Technology and its Challenges. Presentation at the ELSA Colloquium of IT LAW for PhD students and researchers. University of Aix-Marseille. 17 February 2017*

Wallach DA. Bitcoin for Rockstars. *Wired* (12 October 2014) *https://www.wired.com/2014/12/bitcoin-for-rockstars/ (11 July 2017, date last accessed)*

Werbach K, Cornell N. Contracts *Ex Machina*. *Duke Law Journal*. Forthcoming. https://ssrn.com/abstract=2936294 (11 July 2017, date last accessed)

Werbach K. *Trustless Trust*. https://ssrn.com/abstract=2844409 (14 August 2016, date last accessed)

Wong JI. Sweden's blockchain-powered land registry is inching towards reality. *Quartz Daily Brief* (3 April 2017) https://qz.com/947064 (12 June 2017, date last accessed)

Wright A, De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network* 2015 http://papers.ssrn.com/abstract=2580664 (July 11 2017, date last accessed)