The Limits of Smart Contracts

by

Jens Frankenreiter*

This essay investigates the potential of smart contracts to replace the legal system as an infrastructure for transactions. It argues that (contract) law remains relevant in most transactions even if they are entirely structured by way of smart contract. The reason for this is that the power of smart contracts to create and enforce obligations against attempts by the legal system to thwart their execution is limited. These limitations are most relevant for obligations to perform certain actions outside the blockchain, but also apply to other obligations contingent on facts outside the records stored on the blockchain.

Keywords: blockchain, cryptocurrency, tokens, smart contracts, distributed ledgers, Bitcoin, Ethereum, open source, contract law, regulability

JEL classification code: K12, K24, K42, L14, O33

1 Introduction

Cryptocurrencies and the blockchain technology underlying them have received an unprecedented amount of attention in recent months. Much of this attention seems to be related to the fact that Bitcoin and other tokens were discovered as an investment opportunity by a broader set of investors in late 2016 and 2017, and by the fact that an increasing number of actors have released tokens in so-called initial coin offerings (ICOs) to finance the development of new services and other projects. Simultaneously, it has become increasingly clear that the blockchain technology, which makes it possible to create cryptocurrencies in the first place, can be used to enable various other uses as well, ranging from self-executing "smart contracts" to decentralized file-storage systems (Johnson, 2018). These visionary technologies have convinced some observers that blockchains will power a new generation of decentralized infrastructure that will take the place of services which have until now been provided by centralized actors. Maybe the most prominent target of these endeavours is the

[*] The author is a Senior Research Fellow at the Max Planck Institute for Research on Collective Goods, Bonn, Germany, and a Visiting Associate Professor of Law at the University of Virginia School of Law. I am grateful to Yoan Hermstrüwer, Justin McCrary, and Julian Nyarko for useful comments. Any errors and omissions are solely mine.

state (*see also* Raskin 2017, 335; Werbach 2018, 498; Werbach/Cornell 2017, 315). In particular, smart contracts are heralded by some as providing a more efficient alternative to contract law (Savelyev, 2017, 132).

This essay inquires about the potential of blockchains and smart contracts to replace the legal system (more precisely, the courts and contract law) as an infrastructure for transactions.[1] Other authors have raised the question whether such an alternative infrastructure is normatively desirable (Savelyev 2017; Verstraete 2018; Werbach/Cornell 2017). This essay does not comment on this question. Instead, it inquires to which extent smart contracts' properties allow them to "enforce obligations in place of—or even despite—the legal system" (Verstraete 2018, 12; *see also* Savelyev 2017, 132). This essay puts a particular focus on obligations that run counter to the values of the legal system. It asks whether smart contracts, as some assume (Holden/Malani, 2018), can enforce such obligations in a way that makes it impossible for the legal system to stop them from being executed.

The main argument of this essay is that (contract) law remains relevant for many transactions even if they are entirely structured by way of smart contract. The main reason for this is that the power of smart contracts to create and enforce obligations against attempts by the legal system to thwart their execution is limited. Obligations requiring the obligated party to perform or abstain from certain actions outside of the blockchain can generally not be enforced by such smart contracts in a way that makes it impossible for courts to prevent or undo them. Similar limitations apply to obligations contingent on facts outside of the records stored on the blockchain. These considerations primarily apply to smart contracts designed to operate decentrally, i.e., without the need to rely on trusted actors. In principle, smart contracts can be modified so that they allow for a more effective enforcement of obligations. However, such modifications almost always require the involvement of trusted central actors. Yet the involvement of trusted players in turn increases the power of the legal system to regulate smart contracts (*see also* Greenspan 2016).

Of course, even if smart contracts are not able to create obligations beyond the reach of the legal system, they might in the future become an important part of contracting infrastructure. Also, even if the legal system retains the power to revert the effects of smart contracts, it might not be able to enforce its rules in each and every case in which a transaction is at odds with its values. Still, if the legal system in principle retains this power, transacting parties relying

[1] The analysis views the legal system as one of a range of possible arrangements which allows parties to transact in situations in which they otherwise would face incentives not to do so (*see also* Bernstein 1992). Naturally, not all transactions require such an infrastructure. Cash transactions in which a good or service is exchanged against an immediate transfer of money can be executed on the spot, without a need for enforceable obligations. This is however different for more complex transactions in which parts of the obligations are to be fulfilled in the future. In such a case, agents in principle have an incentive to cheat on each other, which might keep them from transacting in the first place. Even then, however, the legal system might not always be required for transactions to occur. In particular, in environments where agents interact repeatedly or where social norms govern their behavior, agents might face incentives to keep promises irrespective of the existence of legally enforceable obligations.

on smart contracts to enforce contractual obligations cannot ignore the legal implications of a transaction. Therefore, predictions that smart contracts will be the basis of a full-fledged alternative infrastructure for transactions that spelled "the beginning of the end of classic contract law" (Savelyev, 2017) seem exaggerated at least.

The rest of this essay is structured as follows: Section 2 provides a brief introduction to blockchains and smart contracts, highlighting those features that are important for assessing the potential of these technologies to establish alternative infrastructures for market transactions. Section 3 lays out the main argument of this essay, namely that the potential of decentralized blockchains to structure offline transactions against the opposition of the legal system is limited. Section 4 briefly discusses why blockchain technology nevertheless might in the future play an important role in structuring transactions. Section 5 concludes.

2 A short introduction to blockchains and smart contracts

The concept of a blockchain was first proposed as part of Satoshi Nakamoto's description of Bitcoin as a fully decentralized electronic payment system (Nakamoto, 2008). For years, researchers and activists had attempted to create such a system. Advances in cryptography, particular the discovery of asymmetric cryptography, had provided some of the most important parts of the puzzle. Most importantly, cryptography provided a way for everyone to verify whether a monetary transfer was in fact approved by the sender of the money. One of the problems that was still unsolved was the so-called "double-spending" problem. Without a central entity to keep records of all transactions that occurred in the system, it seemed impossible to verify that a former owner of an electronic asset had not transferred this asset to a third party and was therefore still authorized to transfer this asset to another party.

Bitcoin solved this problem by establishing the first blockchain. In principle, a blockchain is nothing more than a decentralized database which purports to record and store information in a transparent and tamper-proof way (Catalini/Gans, 2017). In the case of bitcoin, the blockchain stores information about past transactions of bitcoins. Whether the architecture of public blockchains in fact achieves this goal is not entirely clear (*see* Hermstrüwer 2019); however, it is beyond the scope of this essay to discuss this potential limitation of blockchain technology.

The central innovation of this technology is that it allows to create such a database without the need to rely on a centralized entity. At the core of any truly decentralized ("public") blockchain like the one powering Bitcoin is an open source algorithm which achieves a number of things at the same time.

First, it determines the rules that lay down under which condition and in which form information is to be recorded on the blockchain. For example, the Bitcoin blockchain records only transactions that are signed by the private key belonging the account sending blockchains to another account, and only under the condition that the number of bitcoins this account has available is sufficient to cover the transaction. Second, the algorithm provides for a mechanism that incentivizes so-called miners to update the database in an way that makes it possible for anyone to identify the “true” version of the blockchain.[2] A public blockchain is available for everybody to download, and there are no central entities which would control participation in the blockchain. Anyone with the right hardware and an internet connection can participate, both as a normal user and as a miner.

A second important feature of a public blockchain is that actions on the blockchain are exclusively governed by computer code. As mentioned before, code executed by a computer-like system, and not rules applied by humans, decides over which information gets stored on the blockchain, and in what way.

These two features together make it challenging for governments to regulate public blockchains in an effective way. Because no central actor has the power to change the code governing the interactions of agents on the blockchain, it is hard for governments to influence the architectural choices that allow agents to interact in a certain way. And if the blockchain algorithm sets the right incentives for individuals and organizations to participate, it is hard for governments in societies which allow the free use of the internet to keep them from doing so.

It is important to note that not all blockchains are public blockchains (*see* Eenmaa-Dimitrieva/Schmidt-Kessen 2017). After witnessing the potential of the blockchain technology in the rise of Bitcoin, various organizations have started building databases that resemble public blockchains, but that change one or a number of their features to make them better suited for their respective uses. Most importantly, “private” and “permissioned” blockchains restrict the possibilities to participate in operating and/or accessing the records stored on a blockchain (Seth, 2018). This makes it possible to maintain a higher level of privacy than with public blockchains as well as a higher level of control over the blockchain algorithm, and potentially also to effectuate changes to the records stored on the blockchain. At the same time, because such blockchains are controlled by one or a number of identifiable organizations, the government does not face the same obstacles when attempting to regulate them.

The features of public blockchains in particular make them a seemingly ideal environment for the use of so-called smart contracts (Cassano, 2014). The idea of smart contracts was formulated more than a decade before the invention of the blockchain by Nick Szabo, who defined a smart contract as a “computerized transaction protocol that executes the terms of a contract” (Szabo, 1994). At that point in time, however, the infrastructure needed to implement smart contracts was lacking (Werbach/Cornell, 2017, 330). Smart contracts as they exist today on a blockchain can be described as computer programs that trigger certain prespecified actions (such as sending a certain amount of tokens to a specific address in the network) if the conditions set out in the code are met.[3]

[2] For a description of the so-called consensus mechanism that governs the updating of the blockchain, *see* Hermstrüwer (2019).

[3] Whether smart contracts are contracts in the legal sense and to what extent they create

While the Bitcoin blockchain can only accommodate a narrow range of smart contracts, other blockchains such as Ethereum were designed with the express goal to enable the creation of a large range of different (and potentially very complex) smart contracts (Buterin, 2014).

3 The limited power of smart contracts to enforce unenforceable agreements

3.1 General considerations

The main topic of this essay is whether blockchains and smart contracts can serve as an alternative infrastructure for the creation of enforceable obligations which lessens the power of governments to impose limits on market transactions. In order to shed light on this question, this section analyzes in which ways these technologies as they exist today can help enforce agreements which would not be enforceable in courts, and whether governments have any options to limit the support the blockchain lends to such agreements. For this analysis, the exact reasons why the legal system refuses to enforce an agreement are irrelevant. One potential for not enforcing a contract might be its outright illegality (for example, in case of an agreement to fix prices). But outright illegal behavior is not the only case in which the legal system refuses to enforce contractual obligations. Other examples exclude breaches of rules outlawing certain forms of obligations or excluding certain goods and services from being bought and sold. In the following, I will refer to any such agreement as unenforceable without meaning to specify a specific reason for the decision by the legal system not to enforce it.

This analysis does not attempt to cover all the ways in which blockchain technology can facilitate illegal transactions. It seems reasonable to assume that there are various ways in which blockchain technology can support illegal behavior, and mechanism to enforce unenforceable agreements might not even be the most important phenomenon in this regard. Particularly worrying is the use of cryptocurrencies in illegal activities like money laundering and drug trafficking. In fact, the availability of a decentralized electronic payment system like Bitcoin greatly facilitates the possibility for actors to engage in activities that require the transfer of monetary values across jurisdictions or payments in exchange for the provision of illicit goods. The most important reason for this is that traditional electronic payment providers such as banks have an obligation to inquire about the identity of their customers, to monitor their behavior, and to report suspicious activity. Of course, it remains possible to use cash instead of (centralized) electronic payment systems, but this brings with it a number of other problems (e.g., it is non-trivial to provide proof of payment, and involves the risk of theft). Just like obligations to perform actions on the blockchain which do not depend on any conditions outside the blockchain (see below), payments using cryptocurrencies cannot be easily prevented by the legal

legal obligations is not yet entirely clear (*see* De Filippi/Wright 2018, 72-88; Werbach/Cornell 2017, 340). Note that different jurisdictions might decide this question differently.

system.

Similarly, this analysis does not attempt to cover all the ways in which governments can regulate blockchains. Others have made the case that, despite their decentralized nature, even fully decentralized public blockchains are not beyond the reach of the legal system (*e.g.*, De Filippi/Wright 2018, 173-192). In particular, the legal system can target intermediaries such as internet service providers and cryptocurrency exchanges in an attempt to discourage individuals from using certain blockchains. Besides, using such tools, the legal system might be able to put pressure on those maintaining the algorithms running the blockchain to change the rules governing the blockchain in a way that is in line with the goals of the legal system. This analysis takes a slightly different angle, asking to which degree decentralized blockchains can create enforceable obligations relating to offline behavior even if the legal system does not interfere with the operations of a blockchain in such a way. In other words, the main analysis in this essay presumes that there are no obstacles created by the legal system to access such blockchains, and also that there are cryptocurrency exchanges that allow individuals to exchange tokens created on such blockchains into fiat money. This does of course not suggest that governments will not in the future use their power to regulate blockchains to pressure the architects of blockchains into modifying the blockchain algorithm so that it includes safeguards against sustaining unenforceable agreements. Rather, the analysis will show that, even if governments do not move to limit the use of blockchains in general, the nature of the blockchain leaves the legal system with significant leverage to thwart the support that blockchains can lend to unenforceable agreements.

There are two main reasons why the potential of decentralized smart contracts to create enforceable obligations is limited when it comes to obligations relating to offline behavior. Both these limitations are intricately linked to the fact that a blockchain, at its core, is a database managed by computer code.

First, the rules laying down what information is stored on a blockchain and in which form (including the operations performed by a smart contract) are governed by computer code running on a blockchain. As will be shown in more detail below, in order to create enforceable obligations relating to offline behavior, smart contracts need to be able to determine whether conditions related to events occurring outside of the blockchain are met. Yet, at least at the present state of the technology, the potential of computer programs to make sense of information about the offline world is fundamentally limited. Besides, because of technical features of blockchain technology, smart contracts cannot directly access information not stored on a blockchain (Ellis 2017, 3; Greenspan 2016; Zhang 2016, 1).

Second, blockchains are (just) databases. Smart contracts and other blockchain algorithms will only ever be able to directly affect what is registered on a blockchain. Smart contracts can in principle only effectuate future transfers of tokens, for example as a consideration for goods or services, or as prespecified damages for breaches of obligations. In order for a smart contract to ensure that such a transfer will take place, the transferor has to have enough tokens to cover the transaction and has to lock them away as long as it is possible that the transfer will occur. By contrast, smart contracts on their own cannot create obligations which are backed up by real-world assets. Blockchains will not evict homeowners who default on mortgages from their houses or make debtors turn over valuable physical assets. In order to bring about such effects, blockchains will need to obtain the assistance of real world entities such as government agencies, which ultimately answer (either directly or because they are subject to government jurisdiction) to the commands of the law. This severely limits the use of smart contracts in transactions such as loan contracts.

In principle, most or all of these limitations can be overcome. So-called "oracles" transform information obtained from various data sources into information that can be used by smart contracts (*see* Orcutt 2018). In order to bring about effects in the real world, smart devices can be programmed so that they perform certain actions depending on information recorded on the blockchain (Kolber, 2018, 212). Lastly, it seems possible that the legal system itself accepts information stored on a blockchain as binding information about property rights or obligations that it is willing to enforce.

However, all these possibilities open up a way for the legal system to influence which obligations on a blockchain can be enforced and which cannot. This result is most obvious for the scenario in which the legal system itself is called upon to enforce obligations created on a blockchain. But it also applies to the use of oracles and smart devices. If input by oracles is required to create an enforceable obligation on the blockchain, the identity of individuals or organizations operating oracles is likely known to the participants in the blockchain. Otherwise, who would trust them to deliver correct input (*see also* Zhang 2016, 1)? Then, the legal system can target oracles in an attempt to prevent them from transmitting certain information on the blockchain. If smart devices are needed to enforce obligations, the legal system can ban such devices or target those individuals and organizations who deploy them.[4]

3.2 Different types of agreements and different challenges

The analysis above suggests that the level of support blockchains and smart contracts can lend to unenforceable agreements depends on two factors in particular: whether an agreement contains obligations which are to be performed only in case certain conditions relating to facts outside of the blockchain are met, and whether it contains obligations to perform or abstain from certain actions outside of the blockchain. It is possible to differentiate between three

[4] Note also that these possibilities do not only allow the legal system to combat obligations that run counter to values enshrined in the law. Oracles and smart devices also potentially open up ways for the obliged party to evade obligations, or for the beneficiary to obtain a benefit even though the relevant conditions set by the contract were not met. For example, a contracting party looking for a way not to comply with a smart contract might pressure the operator of an oracle or a data source used by an oracle into confirming that the contractual obligations of this party have been met. Smart devices might be destroyed, hacked or simply disabled by aggrieved parties.

different types of agreements depending on whether agreements contain such obligations.

The first type of agreement consists of obligations to perform future actions on the blockchain which do not depend on any conditions that pertain to information other than records stored on the blockchain. Such transactions can be executed by means of a smart contract in a way that makes it almost impossible for the legal system to prevent them from happening. As an example, consider a simple lottery in which all participants pay a certain number of tokens into an escrow account controlled by a smart contract, and the tokens are subsequently paid out to one participant in the lottery who is randomly chosen from among all participants. Smart contracts like this one are the ones that are truly self-executing. Even for contracts of this sort (as well as for all other smart contracts), the legal system could order the parties (provided they are known and within jurisdictional reach) to transfer tokens back to the sender or reimburse a party for a loss in fiat currency.

Agreements including obligations to perform actions on the blockchain which depend on conditions related to facts outside of the records stored on the blockchain constitute the second type of agreement. It is technically challenging to implement such an agreement relying exclusively on smart contracts. The reason for this is the so-called “oracle problem” (Orcutt, 2018). To understand what that means, consider that the smart contracts must be structured so that the blockchain algorithm can ascertain whether the condition is met. As an example, consider the equivalent of an insurance contract in which the insurance provider puts tokens in an escrow that are to be released in case of certain adverse events. How does the blockchain know whether such an event occurred? As mentioned before, a public blockchain does not rely on centralized actors to verify that a transaction complies with the rules set by the blockchain algorithm. This means that everybody willing to participate in maintaining the blockchain needs to be able to verify whether the conditions set in a smart contract are met. Insofar as conditions relate to records stored on the blockchain, this is not a problem, as all information on the blockchain is stored in an immutable way and is publicly available. This is however different for external information, including information available online. Asm mentioned before, such information cannot be accessed by smart contracts directly, but has to be fed onto the blockchain oracles, accounts on the blockchain that make information about real-world events available for smart contracts.

The need to rely on oracles to feed information on the blockchain entails a number of problems. Oracles can either be individuals or computer programs who use their control over accounts on the blockchain to transmit information about the real world onto the blockchain (De Filippi/Wright, 2018, 75). Whether oracles are operated by computer programs or not, they operate at least partly outside of the blockchain, and the decentralized nature of the blockchain cannot guarantee that they perform as intended. Importantly, this means that the operators of oracles are potential targets of governments or aggrieved parties who could prevent them from transmitting certain information onto the blockchain.[5]

Besides, while the use of computer programs as oracles prima facie obviates the need to rely on human judgments, the information that can be obtained by such oracles on their own is limited. This is because they can only verify conditions amenable to verification by computer code (for example, whether a certain website on a specific day features a prespecified headline). But in most cases, the parties to a smart contract will not be interested in verifying the contents of information made available online, but in establishing whether a real world event occurred. If an oracle is designed to query certain websites for information, the parties need to rely on the accuracy of this information (Ellis, 2017, 10).[6] For many real world events, however, there will be no unambiguous information available online. In the future, it might be possible that oracles combine information from various sensors and website to assess whether real world events happened. But the ability of computers to "understand" the offline world is limited, and it is not clear that every event in the offline world is reflected in information available online in a way that is sufficiently predictable to be captured by a computer program.

Agreements of the third type include obligations to perform or abstain from certain actions outside of the blockchain (whether or not these actions also depend on conditions related to facts outside of the blockchain). Naturally, such agreements cannot be directly executed by way of a smart contract. A smart contract can only ever bring about a certain effect itself if the action specified can be performed on the blockchain (Greenspan, 2016). The most important example of such an action is a transfer of tokens to another account.[7] There is simply no way in which a smart contract in itself can force the seller of a book to hand over this book to the buyer.

Rather, without relying on the legal system, the only way to ensure that actors perform certain actions in the offline world is to execute a smart contract that effectively penalizes the obligated party in case of nonperformance.

[5] Recently, a number of new technologies have been proposed that might make it possible to overcome some of the limitations pertaining to the use of oracles, for example by providing cryptographic proof that information provided by an oracle was generated by means of applying a specific piece of computer code (Zhang, 2016), or by sourcing data from various oracles and data sources at the same time (Ellis, 2017). None of these proposals seems able to overcome the fundamental challenge that the ability of computer code to generate meaningful information about the offline world is limited. Other suggestions envision a reliance on data generated by a larger number of randomly selected individuals who are provided with financial incentives to give an accurate estimate of whether certain statements about the real world are true (*e.g.*, Ellis 2017, 26). While this concept potentially solves some of the problems associated with oracles, it is not only slow and resource intense, but also limited to facts that can be verified by large numbers of individuals on the basis of information available to them.

[6] Besides, those operating the data sources become additional targets of governments and aggrieved parties.

[7] A second possibility exists if the desired effect can be brought about by a smart device. However, as mentioned before, I assume that the government will retain some amount of control over what devices can be bought and sold, and will be able to outlaw devices that enable a private system of contract enforcement that does not implement safeguards against abuses.

Put differently, such smart contracts perform a certain action on the blockchain depending on whether conditions pertaining to actions in the real world are met. This implies that smart contracts attempting to enforce an obligation to perform an action or omission in the offline world in principle mirror smart contracts like the ones discussed above, with the exception that the condition stipulated is related to the actions that are to be undertaken by the obligated party. Such a configuration can be described as a self-enforcing penalty clause. Importantly, such a penalty clause still leaves the respective party with the option not to perform the action and incur the penalty implemented by means of smart contract. This might be particularly relevant if the legal system threatens the obligated party with sanctions the cost of which outweigh the costs of paying the ("smart-contractual") penalty. Besides, for the same reason that smart contracts face challenges to implement certain conditions relating to the offline world, the potential for automated penalty clauses to understand whether an obligation has been performed or not performed is limited, and governments might use their power to exert pressure on any oracle or data source to keep a penalty from being triggered.[8]

As mentioned before, another limitation of smart contracts is that courts can revert their effects by ordering the recipient of tokens to transfer them back to the sender, or by ordering that a party that lost tokens is compensated in fiat currency. Some have argued that this effect can be avoided by structuring a smart contract so that additional payments are triggered in case courts take such measures (Holden/Malani, 2018, 25). Of course, such a smart contract faces the same challenges as any smart contract of the second type. It has to overcome the oracle problem, and courts could enjoin oracles and data sources to ensure that the penalty clause is not triggered. Besides, the only way to guarantee that subsequent payments can be triggered is to set aside a respective amount of tokens, for example by putting them in the equivalent of an escrow (Holden/Malani 2018, 28; *see also* Greenspan 2016). This means that parties who are involved in many transactions of this form might need to lock up large amounts of tokens. Also, this solution runs into trouble if the legal system reacts

[8] In a recent paper, Holden and Malani arrive at a different conclusion from the one presented here (Holden/Malani, 2018). They investigate whether smart contracts can provide a solution to the hold-up problem in contracts by allowing parties to effectively commit not to renegotiate a contract. For this, they look to construct a "penalty provision [..] that cannot be undone by courts or the parties through renegotiation" (Holden/Malani, 2018, 24). The authors argue that it is possible to structure a smart contract that does not only trigger a penalty payment in case of an attempt to renegotiate the contract, but that also triggers additional payments in case a court later decides that the affected party had to be indemnified by the other party, or in case the parties negotiated a contract that would make the affected party whole. They acknowledge that it is challenging for the blockchain to ascertain whether the conditions triggering the penalty clauses are met. However, they argue that it is possible to overcome this issue by allowing the blockchain to access the parties' bank and email accounts (Holden/Malani, 2018, 26-27). This argument seems not to take into account that a blockchain cannot access such information without using an oracle which could be enjoined by a court or targeted by an aggrieved party. Also, it potentially overstates the potential of computer code to make sense of such information.

to each penalty by requiring the penalized party to be indemnified.[9]

In sum, the power of blockchains to create effective commitment devices for obligations that would not be enforced by the legal system seems to be limited. In particular, contrary to some commentators, the legal system seems to by and large retain the power to thwart transactions in which either the execution of the smart contract depends on events happening in the offline world and/or in which the obligation pertains to behavior in the offline world.

4 Why smart contracts might still matter

The previous section has shown that the power of smart contracts to support agreements in a way that makes it impossible for the legal system to thwart the execution of such an agreement is limited when it comes to obligations related to offline behavior. It is important to note that these findings do not imply that blockchain will not in the future become a fundamental part of the infrastructure enabling transactions between agents. First, most of the limitations described in this essay pertain mostly to obligations related to facts about the offline world or offline behavior. Already now, as the example of Bitcoin shows, agents ascribe value to tokens stored on the blockchain even if they these tokens do not represent assets in the offline world, so obligations related to actions that play out only on a blockchain do matter. It seems possible that in the future, just as much of our lives has moved online, much of our lives will play out in an environment regulated by rules laid down by blockchain algorithms. In such a world, it might not simply be possible for individuals to "flip off" the blockchain-powered systems (*see* Pogue 2000) and not participate in blockchain transactions if they do not want to.

Second, resource constraints in the legal system might limit its potential to regulate transactions in an environment in which agreements enforced by smart contracts become widespread. If smart contracts deliver on the promise of creating an infrastructure for contracting that allows agents to enter into enforceable agreements at much lower costs than the legal system, they might be widely adopted. This might get to point at which the legal system, although it in principle has the power to correct outcomes which are not in line with the legal system, lacks the capacity to do so. This concern seems to be a real one; court proceedings in the U.S., for example, are so expensive that it seems hard to imagine that an aggrieved party would file a lawsuit to revert a transaction enforced by a smart contract but for cases in which the stakes are high.

Third, resource constraints and the costs of legal proceedings are likely not the only factors weakening the potential of legal systems to revert transactions enforced by smart contracts. The transnational nature of blockchains and the

[9] Holden and Malani propose an alternative solution for this problem: They argue that smart contracts could be authorized to take out loans on behalf of the penalized party (Holden/Malani, 2018, 28). This solution seems promising in principle, but it would require the approval of the legal system without which the obligation to repay the loan could not be enforced.

possibility for agents to interact using pseudonyms might have similar effects. More precisely, blockchains allows transactions between individuals located in different jurisdictions and without them revealing their real identities to each other.[10] In many cases, it will be even more costly for parties to attempt to revert a transaction if they first need to ascertain the identity of the other party. And jurisdictional boundaries will equally make it more burdensome and potentially even impossible for the legal system to counter the effects of an agreement enforced by smart contract in which some of the actors involved reside in other jurisdictions.

Yet the fact that the legal system might not be able to revert transactions in every single case does not mean that the legal system cannot exert influence over the blockchain and the smart contracts operating on it. The analysis in the preceding section has revealed that an effective infrastructure for transactions requires the collaboration of various actors. Each of these actors can be targeted by the legal system alongside intermediaries such as ISPs and cryptocurrency exchanges in an attempt to thwart the operations of a system which produces results that are fundamentally at odds with its values, for example because it supports markets for market-inalienable goods such as organs. Although such measures will likely not succeed in shutting down such services completely, it seems reasonable to assume that blockchains tolerated by the legal system because they implement certain safeguards against unwanted outcomes will ultimately become more attractive for users.[11]

5 Conclusion

This essay posits that the potential of blockchains and smart contracts to erect an alternative infrastructure replacing contract law and courts as an infrastructure for transactions is limited. The reason for this is that there is a fundamental trade-off between designing blockchain-based transaction infrastructures in a way that champions a decentralized architecture and ensuring its effectiveness as an infrastructure for contracts.

In other words, the power of smart contracts to create enforceable obligations relating to offline behavior is limited as long as the smart contract is constructed with the aim to eliminate the need to rely on trusted intermediaries and thereby make it as independent from the legal system as possible. Such a smart contract suffers from limitations of computer programs to make sense of real-world events, and from limitations due to the fact that blockchains cannot directly effectuate changes in the offline world. Notably, these limitations are not just design flaws that can be remedied in future iterations of blockchain technology. Rather, the very features that guarantee that smart contracts can operate in-

[10] Whether blockchains will allow participants in transactions to remain fully anonymous seems questionable at least. In particular, the transaction history of an account can potentially be used to establish a party's identify (*see* De Filippi/Wright 2018, 38-39).

[11] Werbach (2018, 543-550) provides an overview of potential safeguards that could be implemented in a blockchain-powered system.

dependently from the influence of both governments and powerful individual actors are also directly responsible for these limitations. While various technological improvements such as oracles and smart devices allow smart contracts to at least partly overcome these limitations, these innovations entail a move away from a fully decentralized system in which individual actors or organizations do not have the power to influence the operations of the system, and open up ways for the legal system to effectively regulate smart contracts.

This does not mean, however, that smart contracts will not become an important part of the infrastructure used for transactions between private parties in the future. If this technology delivers on its promise to enable a more efficient infrastructure for transactions, it seems likely that market participants will make use of this opportunity. Also, while smart contracts will not put an end to the legal system's control over market transactions, they might lessen the power of the legal system to regulate such transactions in the future. However, if such a change occurs, it will not be due to the fact that the legal system is incapable of reigning in smart contracts, but more likely due to other constraints of traditional modes of law enforcement ranging from capacity constraints to jurisdictional considerations.

References

Lisa Bernstein (1992), "Opting out of the Legal System: Extralegal Contractual Relations in the Diamond Industry ," *Journal of Legal Studies*, 21(1), 115-157.

Vitalik Buterin (2014), "Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform," *Bitcoin Magazine*, https://bitcoinmagazine.com/articles/ethereum-next-generation- cryptocurrency-decentralized-application-platform-1390528211/.

Jay Cassano (2014), "What Are Smart Contracts? Cryptocurrency's Killer App," *Fast Company*, https://www.fastcompany.com/3035723/smart-contracts-could-be-cryptocurrencys-killer-app.

Christian Catalini and Joshua S. Gans (2017), "Some Simple Economics of the Blockchain," Research Paper 5191-16, MIT Sloan, Cambridge (MA).

Primavera De Filippi and Aaron Wright (2018), *Blockchain and the Law: The Rule of Code* .

Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen (2017), "Regulation Through Code as a Safeguard for Implementing Smart Contracts in No-Trust Environments," *EUI Working Paper*, 2017/13.

Steve Ellis, Ari Juels and Sergey Nazarov (2017), "ChainLink: A Decentralized Oracle Network," https://link.smartcontract.com/whitepaper, accessed November 23, 2018.

Gideon Greenspan (2016), "Why Many Smart Contract Use Cases Are Simply Impossible," *coindesk*, April 17, https://www.coindesk.com/three-smart-contract-misconceptions, accessed November 22, 2018.

Yoan Hermstrüwer (2019), "Democratic Blockchain Design," *Journal of Institutional and Theoretical Economics (JITE)*, 175(1), forthcoming.

Richard Holden and Anup Malani (2018), "Can Blockchain Solve the Holdup Problem in Contracts?," *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, 846.

Steven Johnson (2018), "Beyond the Bitcoin Bubble," *New York Times*, Jan. 16, 2018.

Adam J. Kolber (2018), "Not-So-Smart Blockchain Contracts and Artificial Responsibility," *Public Law & Legal Theory Research Paper Series Working Paper*, 18-44.

Satoshi Nakamoto (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System."

Mike Orcutt (2018), "Blockchain smart contracts are finally good for something in the real world," *MIT Technology Review*, November 19, https://www.technologyreview.com/s/612443/blockchain-smart-contracts-can-finally-have-a-real-world-impact/, accessed November 23, 2018.

David Pogue (2000), "Don't Just Chat, Do Something," *New York Times*, Jan. 30, 2000.

Max Raskin (2017), "The Law and Legality of Smart Contracts," *Georgetown Law Technology Review*, 1(?), 304.

Alexander Savelyev (2017), "Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law," *Information & Communications Technology Law*, 26(2), 116.

Shobhit Seth (2018), "Public, Private, Permissioned Blockchains Compared," *Investopedia*, April 10, https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/, accessed December 2, 2018.

Nick Szabo (1994), "Smart Contracts," http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/ szabo.best.vwh.net/smart.contracts.html.

Mark Verstraete (2018), "The Stakes of Smart Contracts," *Loyola University Chicago Law Journal*, 50(*?*), forthcoming.

Kevin Werbach (2018), "Trust, but Verify: Why the Blockchain Needs the Law," *Berkeley Technology Law Journal*, 33(2), 487.

Kevin Werbach and Nicolas Cornell (2017), "Contracts *Ex Machina*," *Duke Law Journal*, 67(*?*), 313.

Fan Zhang et al. (2016), "Town Crier: An Authenticated Data Feed for Smart Contracts," https://eprint.iacr.org/2016/168.pdf, accessed November 23, 2018.

Jens Frankenreiter
MPI Collective Goods, Kurt-Schumacher-Str. 10, 53113 Bonn, Germany
frankenreiter@coll.mpg.de