scripted

Volume 13, Issue 1, May 2016

Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement

Riikka Koulu [*]

Abstract

As cross-border online transactions increase the issue of cross-border dispute resolution and enforcement becomes more and more topical. Disputes arising from e-commerce are seldom taken into the public courts and therefore online dispute resolution (ODR) is becoming a mainstream solution for resolving them. Simultaneously, different applications and possibilities of blockchain technologies such as cryptocurrencies have caught the attention of both computer scientists and legal scholars, increasingly gaining momentum. However, the potential of blockchains reach further than their use as a currency: they can be used for the decentralised execution of programmable contracts known as smart contracts, completely without the need for intermediaries like e-commerce sites, credit card companies or courts. These possibilities have not previously been discussed in relation to dispute resolution. This article provides an introduction to this new technological possibility by examining self-executing smart contracts that utilise novel blockchain technologies. To demonstrate the logic behind smart contracts more concretely, a weather bet (i.e. a bet on what the weather is going to be in a given location) is translated into a programmable smart contract and then discussed in lines of code with further explanations. In addition to this, the author suggests that smart contracts could also be employed for the purposes of dispute resolution, which might provide a solution for the problem of enforcing ODR decisions. Instead of normative analysis, the article provides an introductory analysis of the legal implications that the blockchain technology has outside its application as virtual currency.

DOI: 10.2966/scrip.130116.41

[*] Riikka Koulu, Doctoral Candidate in Procedural Law, University of Helsinki, Finland, Visiting Researcher, the Cyberjustice Laboratory, University of Montreal. I wish to express special thanks to software developer Tom Eklöf for his irreplaceable contribution to this article, both in drafting the Ethereum smart contract depicted in section 2.3 and in commenting this paper. The whole code is available at https://github.com/ORBAT/solidity-tryout/blob/master/bet.sol. All errors and misconceptions in this article are mine only.

1. From Online Dispute Resolution to Blockchains?

1.1. Introduction

The prolific rise of cross-border transactions, *e.g.* e-commerce, is rapidly changing both dispute resolution and enforcement. The dominance of the Internet means that individuals are more often entering into contractual relations regardless of geographical locations or jurisdictional boundaries. Undoubtedly, the increase in online transactions has also caused an upsurge of disputes; in order to preserve consumers' trust in the online market, such disputes need to be resolved.[1] However, these disputes, which are characterised by their low intensity nature, seldom surpass the relatively high threshold of cross-border litigation in public courts, leading to the development of alternative methods of conflict management, namely online dispute resolution (ODR).[2]

In this article I approach the challenge of online disputes, an issue that ODR aims to address. Whereas ODR provides a model for resolving online disputes there remains the problem of enforcing these decisions. The alternative approach suggested here focuses on conflict prevention facilitated by the technological infrastructure itself. By examining the possibilities of blockchain technologies, I introduce a different way of assessing technologically augmented dispute resolution and enforcement, which could potentially signify the newest chapter in the on-going debate of combining conflict management and technology.

This article begins with the same problem that ODR has originally addressed: how do we provide efficient redress in cross-border, online transactions between unknown parties where a dispute arises from their contract? How do we organise dispute resolution and facilitate enforcement of the decision in order to preserve the trust placed in the online market?

In this article, I first examine the possibility of harnessing technological infrastructure to address the needs of dispute resolution and technology. In order to take on this task, a

---

[1] This is also the starting point of EU's digital agenda. European Commission, "A Digital Single Market Agenda for Europe" (2015) 4-5, available at http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf (accessed 5 Nov 2015).

[2] In the literature, e-commerce disputes have usually been described as low value high volume disputes. However, this characterisation is very much entwined with e-commerce and may overlook other applications of dispute resolution and technology. The University of Montreal's Laboratory of Cyberjustice uses the term *low intensity disputes* to describe the characteristics of disputes that would be suitable for ODR. This terminology has the advantage of summing up the relatively low and simple interests of the parties without labelling them simply as e-commerce disputes. See e.g., K Benyekhlef, V Callipel and E Amar, "La médiation en ligne pour les conflits de basse intensité" (2015) 135 *Gazette du Palais* 17-22.

brief overview of the evolution of ODR and its current challenges is required, as advances in this field constitute the practical background for my examination of blockchains. After this, I briefly describe how blockchains are providing tools for solving the problem of reliability without resorting to centralised authorities. I consider whether a similar structure could be employed to solve the problem of enforcing dispute resolution outcomes without relying on enforcement through state courts or centralised alternatives such as escrows, chargebacks or reputational sanction mechanisms e.g. user reviews or their predecessor, industry black lists.[3] Can an infrastructure based on the blockchain adopt the role of enforcement?

In the second part of this article, I examine the *Ethereum* blockchain platform, which enables the execution of so-called smart contracts through a decentralised technological infrastructure. By the simple example of a weather bet I demonstrate how smart contracts function: how the contract itself allocates winning to one of the parties after assessing the evidence (what the weather was) and how the bets are then transferred to the winner.

Third, I assess the implications of such mechanisms for the future of dispute resolution and technology. In conclusion, I present concluding remarks for future research about bridging the gap between our understanding of law and the potential of technology.

The methodological framework of this article is conflict management. This translates into a specific focus placed on institutionalised conflict prevention, different forms of dispute resolution and enforcement. On the level of fields of law, my starting point is that of procedural law but private and/or pre-emptive enforcement interfaces with contractual law, Internet governance and law and technology studies.

1.2. Online Dispute Resolution and Enforcement

Despite, or more likely due to its origins in the 1990s, ODR still lacks a uniform definition.[4] Some use the term to refer only to privately organised models of technology-augmented dispute resolution, while others include courtroom technology, e.g. e-filing and case management systems, videoconferencing and automated document generation .In short, ODR tools, models and applications vary significantly, but they all have in common the implementation of technology to dispute resolution in order to provide more efficient conflict management.[5] ODR applications may exist separately, linked with

---

[3] G-P Calliess, "Lex mercatoria" (2015) 12 available at http://ssrn.com/abstract=2597583 (accessed 4 Nov 2015).

[4] See e.g. R Koulu, "Three Quests for Justification in the ODR Era: Sovereignty, Contract and Quality Standards" (2014) 19 *Lex Electronica* 43-71, at 45-49.

[5] ODR has often been considered as online alternative dispute resolution (ADR), which, instead of being pronouncedly legal, has focused on the ideals of ADR, i.e., reaching a genuine, tailored solution to the

public courts or as an integral part of e-commerce sites, as is the case with eBay's Resolution Center.[6]

Due to the constraints of territorial jurisdiction, state sovereignty and the newness of ODR, there are no global legal instruments for regulating legal issues related to cross-border ODR. This means that the choice of law or jurisdiction, or the recognition and enforcement of ODR decisions, are all determined based on national law, which may often lead to complications in cross-border situations. In response to these challenges, the EU has created a union-wide ODR platform with translation services through the ODR Regulation (524/2013) and ADR Directive (2013/11/EU).[7] Also, the United Nations Commission on International Trade Law (UNCITRAL) has attempted to draft uniform procedural rules for ODR but the work has come to a relative standstill.[8]

---

parties' conflict instead of resolving the legally framed dispute through evaluation of rights and obligations. See, e.g., A R Lodder and J Zeleznikow, *Enhanced Dispute Resolution through the Use of Information Technology* (Cambridge: CUP, 2010) at 12-13; C Rule, *Online Dispute Resolution for Business: B2B, e-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts* (San Francisco: Jossey-Bass, 2002), at 13. Kaufmann-Kohler and Schultz highlight that ODR's definitions usually depict it either as a *sui generis* dispute resolution method or as online ADR. As they point out, both perspectives have their issues. See, G. Kaufmann-Kohler and T. Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice* (The Hague: Kluwer Law International, 2004) at 5-10. The need for ODR theory has also been acknowledged. See, L Wing and D Rainey, "Online Dispute Resolution and the Development of Theory", in M S A Wahab, M E Katsh and D Rainey (eds), *Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution* (The Hague: Eleven International Publishing, 2012) at 35-50.

[6] eBay's Resolution Centre is an often quoted example of successful ODR. This success is difficult to contradict, as eBay resolves over 60 million e-commerce disputes annually. See, E Katsh, "ODR: A Look at History", in Wahab et al. 2012, at 2. A point of interest is that the service has been renamed as Money Back Guarantee in late 2014/early 2015. However, Vermeys and Benyekhlef argue that public courts could also benefit from implementation of ODR methods. See N W Vermeys and K Benyekhlef, "ODR and the Courts", in Wahab et al. 2012 at 307-324 (see note 5 above).

[7] The Regulation establishes an EU-wide portal for consumers and traders, who can submit complaints through the platform. The platform then directs the complaint to the suitable national ADR entity, which helps the parties in reaching an out-of-court settlement in accordance with the entity's own procedural rules. Full text of the Regulation available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0001:0012:EN:PDF (accessed 5 Nov 2015). The platform, which was launched in January 2016, is available at https://webgate.ec.europa.eu/odr/ (accessed13 Apr 2016).

[8] The objective of UNCITRAL's Working Group III has changed since it started working on ODR in 2010. The stumbling block has been the fundamental difference between different jurisdictions regarding the acceptance of binding pre-dispute arbitral clauses in consumer cases. In July 2015, the Commission further specified the Working Group's mandate to focus on the "elements of an ODR process, on which elements the Working Group had previously found consensus". The Working Group will continue for one year, until the summer of 2016, after which it will be terminated regardless of the outcome. See, United Nations Commission On International Trade Law, Working Group III (Online Dispute Resolution), Thirty-second session, 'Annotated Provisional Agenda' (18 Sept 2015) at 4 available at https://documents-dds-ny.un.org/doc/UNDOC/LTD/V15/066/23/PDF/V1506623.pdf?OpenElement (accessed 21 Apr 2016).

In addition to the lack of uniform due process standards, another unsolved problem regarding ODR is that of enforcement.[9] Without a way to force compliance with a decision, the decision is mainly without effect.[10] Although voluntary compliance is possible, an effective redress mechanism is needed to force compliance in case the final decision reached in the ODR process is not voluntarily followed.[11] Several solutions for enforcing ODR decisions have been developed in practice. One much discussed option would be to enforce ODR decisions as arbitral awards through the public courts. Other, softer options of forcing compliance range from user reviews to chargebacks and escrow services. A more intrusive solution is direct enforcement by the e-commerce site, which requires a close interface between the marketplace, the payment method and the ODR service. In the following section, I briefly describe these options, against which the potential of blockchain technologies need to be evaluated.

It has been suggested that decisions reached in ODR procedures could be enforced as arbitral awards using the widely applied New York Convention of 1958. Enforcement as arbitral awards would mean that ODR decisions would be enforced through the official enforcement mechanism of each nation state. Before granting access to enforcement, the national court summarily examines the award and enforcement may be refused on certain grounds.[12] However, it is unclear, whether ODR could in fact be interpreted as arbitration.[13]

---

[9] This is also linked to the UNCITRAL debate, as the question of the acceptance of binding pre-trial arbitration clauses in consumer relationships is linked with the possibility of enforcing these arbitral awards in accordance with the provisions of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958). See further, R Koulu, "One Click Too Much? – Thoughts on UNCITRAL's Work on ODR Draft Rules, Part II" (2015), available at http://www.cyberjustice.ca/actualites/2015/03/13/one-click-too-much-thoughts-on-uncitrals-work-on-odr-draft-rules-part-ii/ (accessed 13 Oct 2015).

[10] Enforcement is considered to be necessary for efficient access to justice. The case law of the European Court of Human Rights (ECtHR) highlights the importance of enforcement as a part of fair trial provided for in Article 6 of the European Convention on Human Rights. See ECtHR, 'Guide on Article 6: Right to Fair Trial (civil limb)' (2013) at 23-24 available at http://www.echr.coe.int/Documents/Guide_Art_6_ENG.pdf (accessed 13 Oct 2015).

[11] I use a broad definition of enforcement in this article. Traditionally, enforcement has referred to the authority of nationally regulated debt recovery procedures and the authority of the enforcement officials in conducting foreclosure. However, I use the term inclusively to refer to different mechanisms of providing compliance with decisions reached in different dispute resolution procedures.

[12] For example, the recognition may be refused based on Article V of the New York Convention, if the party against whom it is invoked can prove that he was not given proper notice of the proceedings or was otherwise unable to present his case. A similar summary procedure of recognition was formerly in place for enforcing judgments of national courts within EU. However, this *exequatur* procedure has been abolished in the recast Brussels I Regulation (1215/2012) on the jurisdiction, recognition, and enforcement of judgments in civil and commercial cases. It should be noted that arbitration is excluded from the scope of the Regulation. This means that if ODR decisions were considered arbitral awards, the only method of enforcing them through public courts would be through the New York Convention. A related issue is, whether ODR decisions could be considered to be judgments of national courts and hence enforced as judgments through the Regulation. The answer to this depends on future ODR applications within the

Alternative ways of encouraging compliance have developed:[14] for example, many e-commerce sites operate through user review systems, where buyers and sellers may leave public feedback about their transaction after it is completed. The logic is that buyers and sellers with the best user reviews receive more future transactions. The downside of user review systems is that they do not provide redress for individual cases but try to modify future behaviour. The possibility of false reviews or bad faith also needs to be considered.

In addition to user review systems, chargebacks are another mechanism for encouraging compliance. In chargeback mechanisms, the credit card company reimburses payments made by credit card in case the transaction has gone awry. The credit card company makes the decision on reimbursement and thus the mechanism is connected with the payment method. The system is funded without consumer payments: sellers with repeated chargebacks are charged higher fees. The difficulty with chargebacks is that they are most often used in the USA and the UK, and likely require modifications before being suitable for application in financial markets and in legislation in other jurisdictions.[15]

However, the most interesting example of forcing compliance with ODR decisions is the mainly unexplored possibility of direct private enforcement, which is integrated with the marketplace and the payment method.[16] In private enforcement, technological

---

national court systems. One possible conclusion could be that private ODR decisions are seen as arbitral awards and court-based ODR decisions as judgments.

[13] This discussion is ongoing within UNCITRAL's Working Group III. For an overview, see, United Nations Commission On International Trade Law, Working Group III (Online Dispute Resolution) "Report of Working Group III (Online Dispute Resolution) on the work of its thirtieth session (Vienna, 20-24 October 2014)" (4 November 2014) at 8 available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/V14/073/90/PDF/V1407390.pdf?OpenElement (accessed 21 Apr 2016).

[14] For an overview of these mechanisms see, R Koulu, "Where Law, Technology, Theory and Practice Overlap: Enforcement Mechanisms and System Design" in C Adamson (ed), *Online Dispute Resolution. An International Approach to Solving Consumer Complaints* (Author House Publishing/ NetNeutrals, 2015) at 57-68.

[15] Within the EU, there is a legal right to demand a chargeback based on Directive (2007/64/EC) on payment services in the international market (PSD) and on the basis of Directive (2008/48/EC) on credit agreements for consumers, both of which have been implemented in all EU Member States. However, this right is limited to unauthorised payments, trader's violation of consumer's rights and bankruptcy situations. In some EU States, there exists a voluntary chargeback system based on card companies' own operating rules. See, The European Consumer Centre's Network, "Chargeback in the EU/EEA: A solution to get your money back when a trader does not respect your consumer rights", (undated) available at http://ec.europa.eu/consumers/ecc/docs/chargeback_report_en.pdf (accessed13 Oct 2015).

[16] Some scholars have touched upon the private enforcement of ODR decisions. For example, Cortés argues that self-enforcement mechanisms should be complemented with public enforcement mechanisms. See, P Cortés, *Online Dispute Resolution for Consumers in the European Union* (New York: Routledge, 2010) at 82, 204. Kaufmann-Kohler and Schultz argue that self-enforcement is the best option for ODR when voluntary compliance is not possible. They make a distinction between so-called indirect self-enforcement, which refers to trust marks, reputation systems, punitive exclusion from the marketplace and other modes

infrastructure is harnessed to allocate responsibility and liability without human intervention, in automated procedures. What defines private enforcement is the non-interference of traditional enforcement authorities, most importantly the absence of the nation state's monopoly on violence. Private enforcement is also the connection point between ODR and the potential of blockchain technologies: no interface with the public courts is needed and the enforcement forms an integral part of the contractual relationship itself.

An example of private enforcement in ODR can be found in eBay's "Money Back Guarantee", although the e-commerce giant accentuates this as an insurance-type safeguard in case the buyer does not receive the ordered item or the item does not match the listing description.[17] Based on the guarantee, eBay's system refunds a dissatisfied buyer in case the seller and buyer are unable to reach resolution themselves. After reimbursement to the consumer, the seller is then responsible for reimbursing the amount to eBay. Based on eBay's User Agreement of 19.5.2016, eBay may request the interfaced payment operator PayPal to hold the funds on the seller's account to enforce this responsibility.[18]

Although eBay's mechanism is not referred to as enforcement, it operates based on a similar logic as that of private enforcement. Still, it is one of the first examples of creative use of technological infrastructure and the possibilities this example depicts are various. From the perspective of conflict management, such mechanisms function similarly to pre-emptive negotiation: they prevent the conflict from escalating into a full-scale dispute that requires a resolution procedure and separate enforcement of the resolution.

---

of directing behaviour, and direct self-enforcement, which includes escrows, chargebacks, insurance mechanisms and "judgment funds" established by ODR providers or third parties. See, G. Kaufmann-Kohler and Schultz 2004, at 168, 223-233 (see note 5 above). See also, R Koulu, *Dispute Resolution and Technology: Revisiting the Justification of Conflict Management* (Helsinki: University of Helsinki Conflict Management Institute, 2016, forthcoming). It should be noted that private enforcement itself is by no means a new phenomenon, as several scholars have pointed out. See e.g., E Stringham, *Private Governance. Creating Order in Economic and Social Life* (New York: Oxford University Press, 2015). However, technological advances and globalisation have further strengthened the emergence of private regimes and created new prospects for such regimes. See e.g., G Teubner and A Fischer-Lescano, "Regime-Collisions: The Vain Search for Legal Unity in the Fragmentation of Global Law" (2004) 25 *Michigan Journal of International Law* 999-1046.

[17] eBay, "eBay Money Back Guarantee" (no date) available at http://pages.ebay.com/help/policies/money-back-guarantee.html (accessed 13 Oct 2015).

[18] eBay amends its user agreement on regular intervals. For this article, I have used the user agreement effective from 19 May 2016. The authorisation given by the user to eBay to remove funds from the user's PayPal account remains unchanged compared to earlier versions.. eBay, 'eBay User Agreement' (2016) available http://pages.ebay.com/help/policies/user-agreement.html (accessed 26 Apr 2016).

However, as private enforcement bypasses the nation state's monopoly on violence, it is controversial.[19] Still, by combining an e-commerce site, an ODR process and a payment mechanism, private enforcement enables forcing compliance without resorting to the time-consuming and uncertain option of seeking enforcement through public courts.[20] However, as private enforcement requires an interface with a payment method, it may only be possible for market leaders. Another downside is that private enforcement bypasses the summary state control on the fairness of the decision, which has been essential for ascertaining that only those decisions that are reached in private resolution processes respecting due process are granted enforcement through the public enforcement mechanism.[21] The question is challenging: what happens to due process, to the fundamental right for a fair trial, when we remove the nation state from the enforcement equation? Although the question is impossible to answer to any satisfactory end, it is probable that as a last resort, control of due process is shifted from the state to private actors.

As this brief description shows, all alternatives of enforcing ODR decisions have their shortcomings. Could the blockchain, the technology behind modern cryptocurrencies, provide another perspective to this issue? Before evaluating this, it is necessary to explain how blockchains work. If this technological solution is to take the place of enforcement, it needs to include an interface with a payment mechanism and be able to force compliance. *Prima facie,* blockchain-based smart contracts seem to meet both

---

[19] The state's monopoly on violence has received much scholarly attention, starting from the early work on sovereignty by Jean Bodin and Thomas Hobbes. In 1919, The German sociologist Max Weber conceptualised the monopoly on violence as the defining concept of the state. According to Weber, "[a] compulsory political organization with continuous operations will be called a State insofar as its administrative staff successfully upholds the claims to the monopoly of the legitimate use of physical force in the enforcement of its orders…" See, M Weber, G Roth and C Wittich (eds), *Economy and Society: An Outline of Interpretive Sociology. Volume 2* (Oakland: University of California Press 1978), at 54. Since Weber, several scholars have discussed the changes in the state's monopoly on violence caused by technology. See e.g., M Castells, *Power of Identity: The Information Age: Economy, Society, and Culture Volume II* (Malden, MA: Wiley-Blackwell, 2009). For an application of Weber's definition to the Internet see, R W Rijgersberg, *The State of Interdependence: Globalization, Internet and Constitutional Governance* (The Hague: TMC Asser Press, 2010), at 16.

[20] On fair grounds, criticism is voiced against this platform-oriented model, which is based on full integration of payment mechanism and dispute resolution. The basis of such criticism is the partiality embedded in full integration, as it forces the users of the platform (i.e. the sellers and buyers) to accept the platform's authority over the contractual relation both in the transaction phase and in a potential dispute resolution phase (followed by enforcement). Thus, the users have no other feasible option than to accept the platform's user terms, such as direct debit from an account. Florian Glatz uses the apt description of this as "the governance of both the pre and post contractual phase on the platform's terms". See closer, F Glatz, " Smart Contracts, Platforms and Intermediaries" (2015) available at https://medium.com/@heckerhut/smart-contracts-platforms-and-intermediaries-c3d30f5182a6 (12 Sept 2015).

[21] It should be noted that state control before enforcement is by no means the principal method of safeguarding due process. However, the grounds for refusal to recognise arbitral awards stated in the New York Convention demonstrate that grave due process violations may be taken into account at the enforcement stage. Similarly 45 of the Brussels I Regulation (1215/2012) enables the refusal of recognition in case the defendant is not served the documents which instituted the proceedings.

requirements. As virtual currency the interface with a payment method is guaranteed and the smart contract executes itself without the need for additional intervention.

2. Smart Contracts Embedded with Conflict Management?

2.1. Harnessing Infrastructure

Traditionally, ways of conducting cross-border transactions have been limited by the non-existence or lack of predictable and trustworthy modes of dispute resolution and enforcement. The lack of dispute resolution as an obstacle for well-functioning markets has been acknowledged since the Middle Ages and obstacle which continues into the present day. This need for reliable governance[22] led to the emergence of medieval *lex mercatoria*,[23] the loose private regime of shared guild practices, market courts and customs procedures, as well as to the modern versions of these, in the development of online dispute resolution for e-commerce. This is to say that private governance in itself is nothing new.

Institutionalised legal regimes are a method of providing soft law instruments, e.g. contractual practices, codes of conduct, methods of conflict management, that aim at reducing the risks of cross-border commerce. Furthermore, the same issue of allocating risk has taken new forms in the online context. It has transformed into a question of who do you trust online, into an issue of security, privacy and fairness of conflict management. Furthermore, what do you do when something goes wrong, how do you get a third party decision if negotiations fail and how do you execute that decision if there is no voluntary compliance?

Up until now trust has been a focal concept in cross-border commerce and in resolving disputes arising from it. Potentially, the blockchain infrastructure of cryptocurrencies

---

[22] Economist Avinash Dixit points out that the economy assumes the existence of sufficient governance, which is regarded as necessary for successful markets. Governance has traditionally been provided by the nation state or the sovereign. See, A K Dixit, *Lawlessness and Economics. Alternative Modes of Governance* (Princeton and Oxford: Princeton University Press, 2004), at 2-3.

[23] On lex mercatoria see note 3 above, Calliess 2015. Calliess further discusses the development of transnational contractual law and suggests gradual codification and consent-based implementation as the solution to the decreasing importance of the nation state. See, G-P Calliess, "Making of Transnational Contractual Law" (2007) 14 *Indiana Journal of Global Legal Studies* 469-484. In his examination of transnational legality Thomas Schultz argues the importance of distinguishing between law and non-law, as recognising private regimes as law empowers these regimes. See, T Schultz, *Transnational Legality. Stateless Law and International Arbitration* (Oxford: Oxford University Press, 2014), at 11. Schultz's stance also has relevance in relation to blockchain applications. Undoubtedly smart contracts are a part of a normative system but the question remains open, whether they should be recognised as law. Recognising smart contracts as law would empower the blockchain infrastructure and grant it a role in law making. The question is therefore highly controversial.

may change this. Self-executing smart contracts already enable trustless contractual relationships. It is possible that their applications in dispute resolution signify private governance that not only replaces state control with private third party control but completely obviates the need to place trust in any third party, be it the state, the market court, the ODR provider, the escrow service etc. Simply put, there would no longer be the need to allocate trust. This gradual decline of trust is the difference between older models of private governance and blockchain technologies.

2.1.1. How Blockchains and Cryptocurrencies Work

Instead of placing trust in centralised authorities like the state, some initiatives have been taken towards using the technological infrastructure itself to allocate trust - *by* the infrastructure *to* the infrastructure. This method can be employed instead of or in addition to reputation-based methods of forcing compliance, which focus on improving trust between e-commerce users, the sellers and the buyers.

Blockchains and the decentralised digital currencies known as cryptocurrencies based on them are a solution to this end. Cryptocurrencies are defined by their inherent decentralisation, which enables the development of smart contracts and escrow services without the necessity of a trusted institutional third party. Whereas traditional currency operates by the authority of central banks and the credibility placed therein, cryptocurrencies achieve credibility by authenticating the ownership of currency by the technical protocol itself. The value of cryptocurrencies is seldom connected with denominations of traditional currencies although some attempts of this do exist.[24]

The first and most famous example of blockchain technology is the Bitcoin cryptocurrency, which was invented and released as open source software by Satoshi Nakamoto in 2008.[25] The objective of the Bitcoin infrastructure was to overcome the inherent weaknesses of centralised models of digital currencies, namely the need to trust centralised institutions to serve as trusted third parties to transactions to prevent double spending.[26] By solving this issue in a decentralised fashion, Bitcoin enabled the processing of online transactions without the need to resort to third-party intermediaries

---

[24] See e.g., J Wilmoth, "NuBits Seeks to End Cryptocurrency Volatility with USD Peg" (2014) available at https://www.cryptocoinsnews.com/nubits-seeks-to-end-cryptocurrency-volatility-with-usd-peg/ (accessed 5 Nov 2015).

[25] A point of interest is the debate about the elusive identity of Satoshi Nakamoto, who has kept his personal information and identity completely private during the development and adaptation of Bitcoin. The veil of mystery has gained further interest by his disappearance from the Bitcoin context in April 2011. See closer, J Davis, "The Crypto-Currency, Bitcoin and its mysterious inventor"(2011) available at http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency (accessed 27 Oct 2015).

[26] See closer Nakamoto's seminal white paper, S Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) available at http://nakamotoinstitute.org/bitcoin/ (accessed 14 Oct 2015).

such as PayPal or credit card companies.[27] Although Bitcoin is primarily used for online transactions, there are also ATMs that allow the withdrawing or depositing of Bitcoins.[28]

Cryptocurrencies bypass the claimed shortcomings of traditional financial institutions by including a cryptographically secure ledger, a *blockchain* of earlier transactions, which provides both information security and transparency. The ledger of past transactions is public and shared,[29] and after being added no transaction can be altered or removed.

A transaction can be added to the blockchain only when it includes a solution to a specific mathematical problem. These mathematical problems are designed to be computationally difficult and time-consuming to solve, but simple to verify. This means that the creation of cryptocurrency transactions, or in other words confirmation of transactions before they are added to the blockchain, is by default difficult and expensive. This validation process is called "mining", which produces new Bitcoins as an incentive to the "miner". There is no central registry of transactions or other centralised authorities, to which the trust on the currency's reliability would be assigned. Instead, all participating nodes in the Bitcoin network maintain a copy of the blockchain and all nodes verify transactions before they are added to the blockchain. As François Velde describes, "Bitcoin solves two challenges of digital money – controlling its creation and avoiding its duplication – at once".[30] In other words, in addition to providing future prospects both for contractual arrangements and for dispute resolution, blockchains provide a solution to the vulnerability of computer platforms to outside influence, such as fraud or hacking. This is achieved by the design of the infrastructure, by the rules that define how a transaction can be added to the blockchain.

---

[27] J Brito, H Shadab and A Castillo examine Bitcoin from a policy perspective in their comprehensive article "Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling" (2014) 6 *The Columbia Science and Technology Law Review* 144-221, at 148.

[28] The up-to-date map of Bitcoin ATMs is available at: "Bitcoin ATM Map" (2016) http://www.coindesk.com/bitcoin-atm-map/ (accessed 23 Oct 2015).

[29] Professor Joshua Fairfield describes the ledger through the following example: "For example, imagine a list on a whiteboard in a dormitory floor, keeping track of who paid for pizza last time. The advantages to such a list – public availability and ease of editing – are clear. The disadvantages are equally clear. Someone might attempt to edit the list to their personal advantage. A solution that immediately suggests itself is that the dorm RA might be entrusted to keep the list. Yet then there is the concern that the RA may make a mistake, or be unavailable over the weekend, or be untrustworthy and edit the list to benefit himself. What is needed is a public ledger that is constrained by rules of consensus to prevent individuals from modifying the list to their exclusive benefit. That is the central technology underlying Bitcoin: the 'trustless public ledger' (TPL)." See, J Fairfield, "Smart Contracts, Bitcoin Bots, and Consumer Protection" (2014) 71 *Washington & Lee Law Review Online Edition* 35-50.

[30] F R Velde, "Bitcoin: A primer" (2013) available at https://www.chicagofed.org/publications/chicago-fed-letter/2013/december-317 (accessed 30 Oct 2015).

2.1.2. Legal Reactions to Bitcoin

The emergence of Bitcoin has led to a rapid change in the field of financial markets, and it has caught the attention of policy makers, courts, and legal scholars. However, the legal discussion on cryptocurrencies has focused on questions of qualification and regulation, and smart contracts are still in the margin of this debate. In the following section, I shortly describe the existing body of work.

From the legal perspective, an important step was taken in October 2015, when the European Court of Justice stated in its preliminary ruling that Bitcoins are exempt from value added tax, which creates a correlation between the traditional and virtual currencies in the application of EU legislation.[31]

Courts are not the only ones who have faced the need to address the issue of cryptocurrencies. Bitcoin has also received attention from legal scholars as well. Much of this discussion has taken place within the domain of public law, asking questions of qualification of virtual currencies, taxation and regulatory proposals, as Bayern states.[32] Bitcoin poses a challenge for policy recommendation and regulation, as the decentralised infrastructure is difficult to regulate, but at the same time the infrastructure includes transactions that traditionally have been considered necessary to regulate, e.g. consumer cases. It has been pointed out that Bitcoin infrastructure is most often used as a currency and thus the policy setting has also focused on these forms of use, disregarding the other possibilities.[33]

In addition to discussion on future policy, lawyers' reactions to Bitcoin have also addressed its elusive qualification within the legal framework. As it happens, Bitcoin's novelty is that it cannot be directly compared to traditional currency, or commodities, or investment vehicles, although it has similar functions. To this end, it has also been suggested that cryptocurrencies could be seen as *sui generis* digital assets,[34] although others consider this interpretation to create unnecessary complications.[35] On the other

---

[31] See closer the judgment *Skatteverket v David Hedqvist*, Case C-264/14, [2015] available at http://curia.europa.eu/juris/document/document.jsf?text=bitcoin&docid=170305&pageIndex=0&doclang=EN&mode=req&dir&occ=first&part=1&cid=775272#ctx1 (accessed 22 Oct 2015).

[32] S Bayern, "Dynamic Common Law and Technological Change: The Classification of Bitcoin" (2014) 71 *Washington & Lee Law Review Online Edition* 22-50, at 22; R Grinberg, "Bitcoin: An Innovative Alternative Currency" (2011) 4 *Hastings Science and Technology Law Journal* 160-208.

[33] See note 27 above, at 147.

[34] On this debate, see e.g. E Howden, "The Crypto-Currency Conundrum: Regulating an Uncertain Future" (2015) 29 *Emory International Law Review* 741-798.

[35] For example, E P Pacy, "Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes" (2014) 49 *New England Law Review* 121-144.

hand, it has also been claimed that for the purposes of civil jurisdiction Bitcoin ought to be evaluated as tangible property.[36]

So, why is Bitcoin infrastructure relevant to law, regulation and enforcement? Bitcoin has adopted the role of a legal irritant; it is a disruptive technology that changes the legal practice one way or the other, to borrow the terminology of Richard Susskind.[37]

To this end, blockchain technologies could have serious implications for the future of the legal profession. Pasquale and Cashwell examine the possible scenarios of legal automation and its impact on the legal profession depending on the low or high level of regulation and high or low susceptibility of automation. Bitcoin infrastructure is given as an example of the scenario of low regulation, where public functions are outsourced beyond human intervention to computation with a high level of automation. Some predict that (blockchain-based) distributed trust networks could replace traditional legal authorities; others predict enforcement of decisions entrusted to decentralised government-like organisations that could be governed by software code. [38]

However, the promise of cryptocurrencies cannot be reduced to the alternative they provide for traditional currency. This is already apparent in the existing discussion about Bitcoin, where the infrastructure's potential includes the possibility of discarding the traditional intermediaries of e-commerce, such as institutional banks, credit card companies, escrow services and such. Instead of simply bypassing the intermediaries, as Bitcoin enthusiasts suggest, the infrastructure may be employed to take on even more interesting and legally complicated functions, as Pasquale and Cashwell pointed out in passing.[39] According to Fairfield, "it is time to start looking past routine financial applications of such [trustless public] ledgers as currencies".[40]

Following Fairfield's lead, our attention is refocused towards these further applications built on blockchain technology,[41] and most importantly to smart contracts. Still, the

---

[36] See, M I Raskin, "Realm of the Bitcoin: Bitcoin and Civil Procedure" (2015) 20 *Fordham Journal of Corporate and Financial Law* 969-1011.

[37] R Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford and New York: Oxford University Press, 2010), at 93.

[38] F Pasquale and G Cashwell, "Four Futures of Legal Automation" (2015) 63 *UCLA Law Review Discourse* 26-48.

[39] See note 38 above at 37.

[40] See note 29 above at 38.

[41] P Vigna and M J Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (New York: St Martin's Press, 2015) at 9-10.

question here is about the possibilities of using the blockchain for conflict prevention purposes.

2.2. What are Smart Contracts?

The introduction of the blockchain has given rise to the actualisation of smart contracts. The blockchain enables the development of complex transactions of digital assets as well as decentralised autonomous organisations.[42] Smart contracts are an application of the blockchain that go beyond the first phase of Bitcoin, which was mainly focused on its uses as currency. This means that the blockchain, the trustless public ledger, can be used in organising contractual relationships.

In the following section, I examine smart contracts within a specific platform called Ethereum. It should be noted that it is also possible to create smart contracts using the Bitcoin infrastructure; due to technological limitations it is, however, much more complicated and therefore this function is seldom used. The Ethereum platform is designed specifically for smart contracts and has caught the interest of market leaders such as Microsoft,[43] IBM and Samsung,[44] UBS and Barclays[45].

A smart contract is an automated software program built on a blockchain protocol; basically smart contracts are made possible by general-purpose computation that takes place "on" the blockchain. They can be used for allocating digital currency between two parties, when the requirements established in the program/contract are fulfilled. In short, smart contracts are programmable contractual tools, they are contracts embedded in software code. Thus, a smart contract can include the contractual arrangement itself, governance of the preconditions necessary for the contractual obligations to take place and the actual execution of the contract.

---

[42] The white paper on the Ethereum platform provides further technical information about applications of the block chain infrastructure. C Cheng Liang, "A Next-Generation Smart Contract and Decentralized Application Platform" (2016) available at https://github.com/ethereum/wiki/wiki/White-Paper (accessed 25 Apr 2016).

[43] G Prisco, "Microsoft Partners with Ethereum Company, Offers Cloud-Based Blockchain Application Development Platform to Its Clients" (2015) available at https://bitcoinmagazine.com/articles/microsoft-partners-with-ethereum-company-offers-cloud-based-blockchain-application-development-platform-to-its-clients-1446484607 (accessed 4 Nov 2015).

[44] S Higgins, "IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things" (2015) available at http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/ (accessed 4 Nov 2015).

[45] J Wilmoth, "UBS and Barclays Experimenting with Ethereum Platform" (2015) available at https://www.cryptocoinsnews.com/nubits-seeks-to-end-cryptocurrency-volatility-with-usd-peg/ (accessed 5 Nov 2015).

The approach to smart contracts is still unclear because this second generation of blockchain technologies is only beginning to gain traction. There are no policy recommendations, legal literature on smart contracts is still scarce, the case-law is non-existent and even the exact definition of smart contracts is lacking. However, the term itself is by no means new. Legal scholar Nick Szabo defined them already in 1995 as follows:

> A set of promises, including protocols within which the parties perform on the other promises. The protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are "smarter" than their paper-based ancestors. No use of artificial intelligence is implied.[46]

Part of the ambiguity around smart contracts results from the relationship between the legal concept of contract and the element of "smart", i.e. the fact that the contract could be embedded within and defined by software. However, it is clear that smart contracts have to be seen as legally relevant actions.[47] One of the most interesting aspects of smart contracts is the possibility of self-enforcement: self-execution adopts the role of conflict prevention, as it limits the scope of potential disputes arising from the transaction.

To say that smart contracts are self-enforceable means that the software executes the contract, e.g. allocates digital assets autonomously and regardless of trust between the parties. Receiving a payment for sold goods is then no longer dependent on the willingness of the debtor to make the payment nor affected by bankruptcy proceedings that take place after entering the contract. The contract executes its content autonomously according to the embedded contract terms e.g. the digital assets placed within the contract are allocated by the software and no external monitoring of contractual obligations or enforcement is needed.

Smart contracts have the potential to change the current status quo of online contracts, an issue that intersects several fields of law from e-commerce to ODR and beyond. By allocating trust only to the decentralised infrastructure, we can take a step closer to Lawrence Lessig's impression about software code as a regulatory concept.[48] This means

---

[46] N Szabo, "Smart Contracts Glossary" (1995) available at http://szabo.best.vwh.net/smart_contracts_glossary.html (accessed 30 Oct 2015).

[47] F Glatz, "What Are Smart Contracts? In search of a consensus" (2014) available at https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad#.hlgo86909 (accessed 30 Oct 2015).

[48] L Lessig, *Code version 2.0* (New York: Basic Books, 2006) at 5-6 available at http://codev2.cc/download+remix/Lessig-Codev2.pdf (accessed 4 Nov 2015).

that the infrastructure itself replaces the need for trusting traditional third parties, e.g. escrow services or credit card companies.

Fairfield examines this potential from the perspective of consumer protection in online transactions, where consumers' possibilities of negotiating their own contract terms has otherwise become compromised.[49] He suggests that automated agents could help in restoring consumers' bargaining power by searching and concluding an online contract on their behalf without relying on e-commerce intermediaries' standard terms or revealing the consumers' identity beyond their capability to pay for the transaction. However, Fairfield identifies several challenges for actualising the potential of smart contracts: the technology is not yet commoditised, it is unclear, how companies will react to consumer-oriented contract terms and how individualised contract negotiations will affect overall transaction costs.[50]

As Fairfield's analysis depicts, the future of smart contracts is still very much unclear. Their potential may become reality or then again some other application of software and law could become the mainstream solution. The task at hand for legal scientists is to map out the legal implications of blockchain architectures and to conceptualise them for future policy recommendations. The unavoidable fact is that technology has a tendency to develop faster than the legal system can react. Still, technological applications do not wait for the legal system to catch up.

Programmable contracts unavoidably change our understanding of contracts. As contractual relations become autonomous, the role of dispute resolution also changes. Although a change is almost inevitable, its appearances are not. As smart contracts blur the boundaries between the original contract and its execution, the demarcation between contractual law and procedural law also becomes more difficult to ascertain. For example, the role of dispute resolution clauses must be reassessed when the contract is enforced automatically. It is probable that dispute resolution clauses lose at least some of their current importance in cross-border commercial contracts. Furthermore, the resolution of possible conflicts arising from the executed contract may be automated.

Self-executing contracts might significantly alter dispute resolution, although it is unlikely that disputes will disappear completely. It is more likely that disputes themselves

---

[49] According to Fairfield's analysis, courts have the tendency to not enforce contractual terms that are defined by consumers on online contracts. Although this stance has no basis in law and is denied by the courts themselves, it corresponds with the court practice. Also e-commerce platforms limit consumers' possibilities to express their preferences, for example at Amazon a consumer may only affect the quantity of the product she buys. In other words, consumers' negotiation leverage has been reduced to agreeing to businesses' terms. See note 29 above at 43.

[50] *Ibid*, at 47-48.

will change in step with the change of the methods for resolving them. Therefore, the challenge created by smart contracts is not directed simply to contractual law but is also relevant to dispute resolution and due process. Self-enforcement may prevent conflicts as trust is no longer an issue. Also, self-enforcement is not limited to smart contracts; we can also imagine self-enforcing ODR decisions to solve the dilemma of accessing the enforcement mechanism of the nation state, the issue that relates to the difficulties of UNCITRAL's Working Group III.

To further elaborate how smart contracts function and what self-enforcement exactly entails, I depict an example of a smart contract in the subsequent section. The scenario is intentionally a simple one: two parties place a bet about the weather for the following weekend. They draft the bet in the form of a smart contract and decide how the contract resolves the winner based on verified facts. They place the agreed sum of digital assets within the contract and the contract itself allocates these funds to the winner after the facts are verified. It is noteworthy that the normal vocabulary of voluntary compliance, user reviews, escrows, chargebacks and ODR does not actualise in this situation, but instead the contract itself adopts the role usually given to these trust-based models of e-commerce and intermediaries.

The objective of this example is to demonstrate, how legally relevant information is disguised in the lines of code. Additionally, a concrete example substantiates the disruptiveness of this method of drafting contracts.[51] Such examples are often hard to find in jurisprudence.

One might ask, how a betting example sheds light on the use of the blockchain for dispute resolution, or why lawyers should understand the intricacies of smart contracts. The example here is chosen for several reasons. A weather bet is easy to comprehend and simple enough in code, unlike an example of a blockchain-based dispute resolution scheme. Still, the dynamics of weather bets and dispute resolution are to some extent similar: two parties agree on a method to solve their difference of opinion, the verification of data is conducted through certain rules from an external source and the funds are allocated to the winning party after the verification.

Also, similar examples have been used in discussions about cryptocurrencies in general, which makes this case study more comparable. Current weather bet schemes are centralised and use cryptocurrencies solely as currency. The case study of Ethereum, in turn, provides insight into a decentralised contractual arrangement which goes beyond these other examples.

---

[51] Here, disruptiveness refers to the terminology used by Richard Susskind to describe technologies that fundamentally challenge the existing status quo. See note 37 above at 99.

Lastly, I suggest that smart contracts are further blurring the distinction between private autonomy and conflict management. The self-execution of smart contracts can be interpreted both as the execution of contractual obligations and as the mechanism for conflict prevention, depending on the chosen perspective. In other words, an example of automated contracts improves our comprehension about automation of conflict management.

2.3. Case Example: A Smart Contract for Betting on the Weather

Ethereum is an interesting example of a blockchain-based, decentralised platform for smart contracts. It combines the contractual platform, its own digital currency (called 'ether' that can be exchanged for e.g. Bitcoins or traditional currencies) and a way of incorporating the execution of the contract and assessment of external facts into the contract itself. At the moment the use of the Ethereum platform does require some programming skills, which is the reason why I proceed with the case example through the lines of software code. It should be noted that once the technology becomes commoditised, web-based applications that can be used without specialised programming knowledge will emerge.[52]

Before this commoditisation takes place, the creation of smart contracts within Ethereum requires understanding of *Solidity*, the object-oriented programming language[53] used within the Ethereum platform to draft smart contracts. Object-oriented programming is based on "objects", that are data structures containing both data fields (attributes) and procedures (methods). The procedures of a software program can access and modify the data fields of other programs that they interact with. Objects are created based on templates called classes that define the initial values and methods or functions for the program. Fields are data organised within the classes or objects. Regular fields are also called instance variables, where there is a different variable for different instances (e.g. a class called "student" includes a field called "name" and each student has a distinct name). There are also static fields, where the field only has one variable that stays the same in all instances of the object (e.g. all students have the right to study).

Smart contracts written with Solidity govern the behaviour of different accounts within Ethereum and the language is designed to correspond with such external concepts as ownership and identity. The basic structure of Solidity is the contract, which also forms a

---

[52] Some web-based applications already exist, e.g. Augur provides a web-based prediction tool for future events. The system runs on Ethereum. "Markets" (2016) available at http://www.augur.net/ (accessed 25 Apr 2016).

[53] On object-oriented programming see e.g., E Kindler and I Krivy, "Object-oriented simulation of systems with sophisticated control" (2011) 30 *International Journal of General Systems* 313-343, at 314.

separate object on the blockchain.[54] A contract deployed on the blockchain can be seen as an instance of a class.

In my test-case smart contract, Adeline from Montreal (Bettor1) and Bob from Helsinki (Bettor2) place a bet of 100 ether about the weather in New York, where both of them are staying the next weekend. Adeline believes that the weather is going to be good; that the temperature will be at least twenty-five degrees Celsius at 20:00 on Saturday evening. Bob is more sceptical and predicts the temperature to only be fifteen degrees. They agree that the actual weather at the set time is verified using official weather reports that are provided by a third party.[55] They create a smart contract and "deploy" it on the Ethereum blockchain. Both parties transfer money from their respective accounts and this money is then allocated by the contract to the winner. In a way, the smart contract serves the same purpose as procedural law in court proceedings: it defines the rules for resolving the difference of opinion between the parties.

From a legal perspective the situation is simple: parties enter into a binding contractual relationship that obliges the losing party to pay the winner a certain amount of money after the facts have been established by a third party. However, this legal perspective cannot be found in the actual lines of Solidity code, as the programming language structures the data differently. How then is a smart contract created? How does the relatively simple legal example transform into lines of code?[56]

An individual smart contract is a class and within the blockchain the contract is an instance. Here, our smart contract is titled `WeatherBet`. First, we define a data structure that belongs to the contract. The structure has no methods but only includes fields, and instances of it are used to hold data about the bettors. These fields are an address to an Ethereum account (`address addr;`), the temperature as a positive whole number (`int8 temperature;`), and the bet amount of the bettor (`uint value;`).

```
contract WeatherBet {
```

[54] "The Solidity Programming Language" (2016) available at https://github.com/ethereum/wiki/wiki/The-Solidity-Programming-Language (accessed 25 Apr 2016).

[55] On information provided by a third party see e.g., T Bertani, "Oraclize, the provably-honest oracle service, is finally here!" (2015) available at http://blog.oraclize.it/2015/11/04/oraclize-official-launch/ (accessed 10 Nov 2015).

[56] For the sake of argument, the code lines in this paper are simplified on purpose. The code is also available at https://github.com/ORBAT/solidity-tryout/blob/master/bet.sol. The same simplification applies to the case itself and legal nuances are therefore ignored in order to display how a simple scenario is translated into a software program.

```
struct Bettor {
  address addr;
  int8 temperature;
  uint value;
}
```

After this data structure has been defined we proceed to defining a new field. This field tells whether the bet has been allocated or not. If the variable is 'yes', it means that the bet has already been paid. It serves the purposes of the program itself; it has no external corresponding meaning in the legal sense. Nonetheless, the variable reveals whether the contractual obligations have been executed. Simply put, this variable would correspond with the parties' knowledge that the bet is over.

```
bool private winnerPaid;
```

A point of interest is that this line of code above is connected with the irreversibility of transactions within the blockchain. The keyword `private` defines that only the contract itself can affect that specific field. It closes the contract from external influence: it establishes that neither of the parties nor anyone outside the *inter partes* relationship may change these variables within the contract. Only the contract itself can determine whether the bet has ended. The parties cannot affect this and may only know that the bet has ended by following the bet end time or by receiving the payment due to the winner.

After this, we introduce other variables to the contract. These include fields of the smart contract, of the class `WeatherBet`. We declare the fields of bettors (`Bettor private bettor1;` and `Bettor private bettor2;`), the bet end time (`uint private betEndTime;`), and the external source for verifying the temperature (`TemperatureOracle private tempOracle;`). Now we have described the data structures of the smart contract.

```
Bettor private bettor1;
Bettor private bettor2;

uint private betEndTime;

TemperatureOracle private tempOracle;
```

The next lines present a function, a method. From the legal perspective, this part of the smart contract is especially interesting. The method is related to the question of whether the smart contract allows the parties to change their minds regarding the bet, whether either one of them can end the bet before its end time, regardless of the other. The way the code is written for this example, either one of the parties is allowed to change their mind and end the bet.

It should be noted that this could be arranged differently. The contract could be written in a way that does not allow the parties to change their minds at all once the bet is placed, or we could allow someone outside the *inter partes* relationship to take part in the bet. What makes this legally relevant? These lines depict how the creation of the code corresponds with legal assumptions. If we want to disable the parties' possibility to change their minds, the lines of code would be different.

```
  // end bet and reimburse both bets
  function kill() external {
    // only bettor1 or bettor2 can end the bet
    if(msg.sender != bettor1.addr && msg.sender != bettor2.addr)
return;
    bettor1.addr.send(bettor1.value);
    bettor2.addr.send(bettor2.value);
    suicide(msg.sender);
  }
```

Next we have the method that is used to initialise instances of the contract. This method is called a *constructor*, and it is given the same name as to the class we created at the beginning (`WeatherBet`), a naming practice typical to object-oriented programming. The method has parameters that are defined within the parentheses. Here we define the time when the bet ends (`betEndTime = _betEndTime;`) and the account numbers of Adeline and Bob that function as identification markers (`bettor1.addr = _bettor1;` and `bettor2.addr = _bettor2;`).

```
  // Create a new weather bet between bettor1 and bettor2 that
  will be resolved at _betEndTime
  // using temperature oracle at `_tempOracle`.
  function WeatherBet(uint _betEndTime, address _tempOracle,
  address _bettor1, address _bettor2) {
```

```
    betEndTime = _betEndTime;
    tempOracle = TemperatureOracle(_tempOracle);
    bettor1.addr = _bettor1;
    bettor2.addr = _bettor2;
    bettor1.temperature = 0;
    bettor2.temperature = 0;
  }
```

Now, we have created the structure for our bet. The objective of the next method to be defined is the actual bet. The first lines ascertain that no money can be paid to the contract after the bet end time. Through these lines the boundaries of the bet are created.

```
  function betOn(int8 temperature) external {
    if(winnerPaid || now > betEndTime) {
      // bet already over, reimburse sent value
      msg.sender.send(msg.value);
      return;
    }
```

Smart contracts, like any computation that takes place in the blockchain that *changes* the blockchain, are created by transactions. In order to change the blockchain, digital assets (in this case ether), must be sent to the smart contract. This means that each message sent to a contract requires a transfer of ether to be concluded. Simply put, a message is a transaction, a transaction is a message.

The following lines effectively create the bet. If money is sent to the contract and the sender is the account of Adeline (`if(msg.sender == bettor1.addr)`), the value is then placed within the bet. The same goes for Bob (`else if(msg.sender == bettor2.addr)`). If someone else sends money to the contract, the money is not placed within the bet but the transaction is aborted (`else { throw;`). A point of interest is that the transaction, in the money sent by each party to the contract, is a declaration of intent. By making the transaction, each party enters into a contract.[57]

[57] There is a possibility that only one party enters into the contract and the other forgets to send the money or otherwise decides not to. It should be noted that in case only Adeline is active and Bob remains inactive, Bob does not become bound to the contract and cannot lose money (as it has not been placed within the contract). From Adeline's perspective the worst-case scenario is that she loses the money she has paid to

```
    if(msg.sender == bettor1.addr) {
      // message was sent by bettor 1
      bettor1.temperature = temperature;
      bettor1.value += msg.value;
    } else if(msg.sender == bettor2.addr) {
      // message was sent by bettor 2
      bettor2.temperature = temperature;
      bettor2.value += msg.value;
    } else {
      // message wasn't sent by either bettor, abort the
transaction.
      throw;
    }
  }
```

However, the next lines of code are the most interesting for the objective of this article. Here we define the method for allocating the money paid to the contract to the winner of the bet. The contract itself cannot check whether the bet time has run out. Instead, it needs a message to activate. As discussed earlier, this requires a transaction to the contract, as no computation is possible without a transaction. It is noteworthy that anyone can call the function (`function payWinner() external`). The keyword `external` means that the call needs to come from outside the bet: there has to be a transaction to activate the function. This activation from outside the contract may be either one of the parties, someone else or another program encoded to call this contract.

It is possible to limit the scope of who can activate the function. On the level of code, we might regulate that the activation for the function comes only from the parties. Or, we might set a limitation that only a specific third party is entitled to make the transaction so that the function activates. The implications of this are extensive. Such a structure would make it possible to use the structure of smart contracts to create escrows or to take place of a decision in a dispute resolution procedure.

---

the contract. This is possible if Bob does not place the money nor make a suggestion about the temperature, which means Bettor2's suggestion then obtains the value of 0, and if the temperature actually happens to drop to zero or below, he then wins the bet. Such a possibility can be prevented. However, this scenario has not been taken into consideration, in this example, in order to keep the lines of code as simple as possible.

When this method (`function payWinner() external`) is called by a transaction and the bet time has ended, the method accesses the third party information about the factual temperature at the bet end time (`int8 temperature = tempOracle.get(betEndTime)`). Then, it compares the differences between Adeline and Bob's guesses and what the temperature actually was.

```
function payWinner() external {
  // the bet still has time left
  if(now < betEndTime) return;
  // the bet's already over and winner has been paid
  if(winnerPaid) return;

  int8 temperature = tempOracle.get(betEndTime);

  int8 bet1Diff = abs(temperature - bettor1.temperature);
  int8 bet2Diff = abs(temperature - bettor2.temperature);
```

In the following line, the whole balance of the smart contract is allocated to the winner.

```
  // the winner gets the whole balance of the contract
  uint payOut = address(this).balance;
```

If there is no winner, meaning if Adeline and Bob's guesses were equally far from the actual temperature, then both would have their bets reimbursed (`if(bet1Diff == bet2Diff)`). If Adeline's bet was closer, then the whole balance is paid to her account `(else if(bet1Diff < bet2Diff) {` and `bettor1.addr.send(payOut).` If Bob's was closer, then the balance is paid to him (`else { bettor2.addr.send(payOut)`). The last line of this block (`winnerPaid = true;`) signifies that the bet has been ended and disables new bets under the same contract.

```
  // both bets are equally close, reimburse bets
  if(bet1Diff == bet2Diff) {
    bettor1.addr.send(bettor1.value);
    bettor2.addr.send(bettor2.value);
```

```
    // bet 1 is closer
    } else if(bet1Diff < bet2Diff) {
      bettor1.addr.send(payOut);
    // bet 2 must be the closest
    } else {
      bettor2.addr.send(payOut);
    }

    winnerPaid = true;
  }
```

The last lines of code deal with the possibility that someone else, other than Adeline or Bob, has transferred money to this bet. In this example the possibility to place a bet is limited to the parties. However, another solution would also be possible, but in order to do this, the implications would need to be taken into consideration.

```
  // abort all transactions sent to the contract outside of
  betOn()
  function() {
    throw;
  }
}
```

As the example demonstrates, a relatively simple contract between two parties can be turned into lines of code, into a blockchain-based smart contract. Still, this transformation differs significantly from the lawyer's impression about contracts. This example raises several questions on the interface between law and the blockchain architecture. It is clear that legally relevant occurrences take place in smart contracts: they cater to expectations that are to some extent linked with those created by the legal system.

3. Implications of Smart Contracts to Law

3.1. How Should a Lawyer Read a Smart Contract?

Reviewing a smart contract's code is difficult and time-consuming for a lawyer. The logic required for translating a legal contract to a programming language differs significantly from the lawyer's perspective to the contractual obligations. Still, there are

several reasons why such an exercise is beneficial and why the logic of smart contracts is interesting beyond programmers. Several legally relevant steps take place within these lines of code.

First, the smart contract operates with a similar logic to "traditional" contracts: the will of both parties to enter the agreement is needed in order for it to be valid. In a smart contract, the declaration of intent is given through a transaction to the contract itself. In the example, Adeline created the contract but Bob also made a transaction from his account to the contract. The declaration of intent is not separate from the formation of the contract or from the execution of it. This raises questions of how contractual law applies to smart contracts both *in casu* and in general. Also, the self-execution embedded in the code affects the parties' needs to regulate on dispute resolution of possible future disputes, e.g. inclusion of arbitral clauses.

Second, there is an external reference point for establishing "real world" facts within the smart contract. In our example, Adeline and Bob trust that this external source of information provides trustworthy data. The smart contract itself has no way to verify whether the external data is correct or not, it simply applies it. Still, the data is retrieved by the smart contract when the function to pay the winner is called. Adeline and Bob trust the execution of the contract to the decentralised Ethereum platform instead of using intermediaries like escrows or turning to the courts in case of disagreement.

Although this example of fact-finding is a simple one, its implications are more far-reaching. In this example the fact-finding is a part of the smart contract itself and the external fact-finding functions as a method for executing the contract as conflict prevention. The question remains whether such a structure could be employed to the needs of dispute resolution as well. Much of the fact-finding conducted by the courts in simple civil cases deals with examining written documents. As ODR has shown, simple e-commerce cases can already be resolved through automated online procedures. Hence the question is whether smart contracts could provide a new chapter for the automation of low intensity disputes both in public courts and in ODR procedures.

Third, there is no separate execution of contractual obligations, nor is there the need to force the compliance of the other party. As the smart contract comes into being only by the transactions made by the parties, the means for self-execution are already embedded within the contract. The implications of this irreversible self-enforcement could be tremendous. On one hand, self-enforcement is also conflict prevention. On the other hand, it is probable that some disputes will arise regardless of irreversible self-enforcement. The question is how these follow-up disputes can be resolved.

Fourth, writing the code for a smart contract is not just a simple translation of legal expectations to a programming language. As the example illustrates, there are several

alternative ways to affect the implications of a smart contract. We may limit the participants of the bet or not, we may require that only a third party is allowed to call the function `payWinner`. We may allow the parties to change their minds before the bet ends or may not. All of these choices are done at the code level but have legal relevance as well.

The blockchain exemplified here in simplified form might be employed to other uses than simple contracts between two fixed parties. However, it should be noted that the implications of this example to the overall automation of complex legal issues are not straightforward. The objective here has been to demonstrate that smart contracts can be used to solve legally simple, yet multifaceted disagreements. As the weather bet demonstrates, two parties can program their disagreement about the weather into a smart contract that verifies the data and allocates funds to the winner.

The practical utility of smart contracts beyond their use to bet on publicly available and objectively verifiable information emanates from such simple origins. A significant portion of low intensity online disputes takes place in relatively simple factual circumstances. For example, a typical e-commerce dispute regarding whether the paid goods have been delivered or not can easily be verified through delivery notices. This is to say that the resolution of such simple cases is most likely to benefit from automation through smart contracts. Low intensity disputes could be the first dispute category to be automated. However, it remains to be tested whether and how more complex cases, e.g. the quality of delivered goods, can be automated. In other words, the question is not whether all forms of dispute resolution can be solved by technological means: instead, the question is which dispute categories can be automated first.

Still, as this example confirms, the use of a blockchain for the purposes of dispute resolution or escrows is no longer a question of the distant future and neither is the emergence of legal programming.

3.2. Challenges of Smart Contracts

It is clear that both the private enforcement of e-commerce sites as well as the self-execution of smart contracts change our understanding of enforcement. Use of coercion to force compliance is no longer limited to the nation state's monopoly on violence. The danger is that as coercion detaches from the nation state, it also detaches from the state's due process control, which up until now has been the requirement for accessing the state's enforcement mechanism.

It is possible that use of blockchain technologies will also emerge within the domain of dispute resolution; such a development could both benefit and impede access to justice. On one hand, low value cases, which form the majority of e-commerce disputes, seldom

exceed the litigation threshold in public courts, but simultaneously there is concern for whether they can be resolved by ODR procedures. Private ODR does not necessarily follow the same level of due process as public courts do and it produces no binding precedents. Blockchain-based dispute resolution could solve the latter issue, as all transactions within the blockchain are public.

On the other hand, a blockchain infrastructure – including all its applications – is a neoliberal's dream: there are no external authorities, public or private ones, which can dictate the transactions that are added to the public ledger. Transactions in the blockchain are irreversible, and it is unclear what this would mean for the rule of law and the protection of weaker parties. In other words, we have no idea whether removing the state from all phases of the equation of a contract, from formation to execution and possible dispute resolution, is really a good idea. In the end, nation states are often bound by constitutional obligations to provide the rule of law and protection of basic rights, which is not the case with other actors in the field.

As blockchain-based applications like smart contracts are gaining ground, reactions from the legal system are required. These reactions are not limited to questions about how we regulate cryptocurrencies, or user communities advocating for them. There are subtler questions: for example, what does the irreversibility of blockchain transactions mean from the legal perspective? How do we provide such an infrastructure with effective redress mechanisms, or can we at all? What assumptions are we making within smart contracts, e.g. if we assume the parties to be equal, rational actors, is there room for taking imbalances in their power relations into consideration?

Another issue relates to the possibilities provided by anonymity. For example, Howden draws attention to the challenges of cryptocurrencies, especially Bitcoin's vulnerability to abuse of dominant position in mining and transaction malleability.[58] On the other hand, De Filippi observes that although regulation of cryptocurrencies is needed, at the current stage self-regulation would probably provide better results, as it would not hinder future innovation.[59]

4. Conclusions

The emergence of smart contracts suggests a new chapter of law and technology, where blockchain technology is used as a cryptocurrency, as means of entering contractual

[58] See note 34 above at 796.

[59] P De Filippi, "Bitcoin: a regulatory nightmare to a libertarian dream" (2014) 3 *Internet Policy Review* available at http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream (accessed 5 Nov 2015).

relations and as means of self-enforcement. The technology has the potential to change our understanding of contractual law, of dispute resolution and enforcement and the divide between public and private use of power.[60] An urgent issue is whether smart contracts should be interpreted as belonging to law or not.[61] Furthermore, the hybrid nature of smart contracts as both contractual arrangements and conflict prevention obscures the already ambiguous boundaries between contractual law and procedural law. Further research is certainly needed, if we are to address the legal implications arising from the increasing use of smart contracts.

The case study of the weather bet demonstrated that smart contracts can be employed to resolve a difference of opinion between two parties regarding the weather. The fact that smart contracts can include the verification of external data also entails promising prospects for the automation of simple, low intensity cases. As there are no plausible solutions to enforce ODR decisions, the potential of smart contracts must be evaluated from this perspective. Nonetheless, the ground-breaking novelty of Ethereum-based smart contracts lies in the benefits of decentralisation. Decentralised smart contracts remove trust as the focal concept of interaction: as external influence is excluded from the blockchain and all transactions take place in the public ledger, there is no need place trust in the other party, the market place, the escrow service or the ODR provider.

At the moment, use of smart contracts requires programming skills, but there is no doubt that web-based applications of the technology can bring the technology within everyone's grasp. However, the question of digital literacy remains, as this new model of contractual relations relies on a distinct technological functionality that differs significantly from our traditional understanding of contract law and dispute resolution.

Another question is whether the blockchain can adopt the role of enforcement. The tentative first steps suggesting a "yes" are taken here in this introductory analysis. In addition to self-execution of smart contracts, the blockchain could transform our understanding of ODR. Right now there are more questions than answers. One question is whether and how dispute resolution could be organised through a blockchain infrastructure. Another question is what redress mechanisms exist or should exist for smart contracts that are irreversible by default.

---

[60] Calliess and Zumbansen discuss essentially the same phenomenon: "The transnational challenge to legal theory presents itself to the fields and distinct doctrinal frameworks in both public and private international law at a time when both disciplines are already under extreme pressure to adapt their toolkits and even their conceptual frameworks in responding to the challenges arising from increasingly de-centralised and relativised law-making forums." G-P Calliess and P Zumbansen, *Rough Consensus and Running Code* (Oxford: Hart Publishing, 2010) at 7.

[61] As Schultz notes, recognition of private regimes as belonging to the legal system is important, as "calling something law grants it the authority that law usually has and thus creates a moral reason to comply with it". See note 23 above at 29.

The technological methods for decentralised ODR based on the blockchain are quickly becoming something more than just reveries of a technology enthusiast. There is the potential for further automation of dispute resolution and enforcement, but there is also the fundamental question of how we can safeguard fairness and due process within such decentralised networks irrespective of state control. Still, there is no reason, why blockchain-based solutions could not be adopted within public dispute resolution as well. As the technology develops, these issues of access to justice are becoming increasingly urgent.