Chantal Bomprezzi*

From Trust in the Contracting Party to Trust in the Code in Contract Performance

A Critical Analysis of the Relationship between Blockchain-Based Smart Contracts and Consumer Protection

Smart contracts take advantage of the decentralised and immutable nature of blockchain technology. When blockchain-based smart contracts are used to automate the performance of contracts, it is affirmed that the obliged party cannot influence the execution of the contract. There is a shift from trust in the other party to trust in the code. Therefore, it is wondered whether blockchain technology may foster consumers' trust in the right performance of B2C contracts and enhance consumers' protection towards businesses. The work tries to answer this research question. It aims to verify if blockchain-based smart contracts exclude non-performance and prevent businesses from exercising a kind of control over the performance of the contract. To this end, it takes into consideration some hypothetical scenarios of use of smart contracts and the blockchain for the automatic performance of B2C contracts.

I. Introduction

The present study tries to verify whether blockchain-based smart contracts can help to remedy a lack of trust in the obliged party, thus enhancing consumers' protection.

Blockchain is considered a very secure database. Because of its characteristics, it is believed that it cannot be either modified or centrally controlled. Smart contracts are computer programs able to self-execute according to pre-programmed functions. Execution of smart contracts can also be blockchain-based. In the latter case, smart contracts take advantage of blockchain properties. Thus, when blockchain-based smart contracts are used for the automatic performance of contracts, it is said that after the conclusion of the contract the obliged party is no more able to breach it.

In view of the above, blockchain technology could have the potential of fostering consumers' trust in the right performance of B2C contracts and granting consumers' protection. It is well known that the latter are much weaker than traders. Traders get in contact with consumers for professional purposes. So, they have much more information and awareness of the content of the contract than consumers, which act for personal interests. For this reason, consumers are often subject to abuse. Consumers are not able to protect themselves because they are usually not conscious of their rights, or do not have sufficient power to enforce them. Contract enforcement becomes even more problematic when they trade with businesses online, provided that they communicate at a distance and behind a computer screen.

Instead, blockchain technology could be of support for the enforcement of B2C contracts in favour of consumers. Smart contracts would perform traders' contractual duties without any possibility of *ex-post* intervention. Consumers would not have to worry about exercising enforcement remedies because the blockchain could ensure *ex-ante* that the contract will be rightly performed. In particular, such kinds of applications are emerging in travel insurance, especially for transport cancellations or delays. Indeed, the latter can be easily automated and verified by machines. Moreover, they could be very useful for consumers considering that consumers' compensations are not of a high value in this field, and in most cases they renounce to start a claim. Smart contracts, on the contrary, would automatically indemnify consumers without any need to activate. However, it can be imagined that blockchain-based smart contracts will spread in all trade sectors where technological advancements allow the embedding of contractual conditions into software.

This research wonders whether blockchain technology really prevents businesses from exercising control over the performance of the contract. To this end, it firstly gives an overview of the technical functioning of blockchain and smart contracts and the current European legal instruments for consumers' protection, especially online, when consumers face the major risks (respectively Section II. and III.). Section IV. explains why it is asserted that blockchain technical features could be a tool to enhance consumers' trust and protection against the dangers they encounter in e-commerce.

The following sections provide the author's critical analysis. Namely, Section V. attempts to demonstrate that blockchain technology cannot give rise to breach-less contracts by enlist-

* Research fellow at Alma Mater Research Institute for Human-Centered Artificial Intelligence, University of Bologna; fellow of the Italian Academy of the Internet Code (IAIC); E-mail: chantal.bomprezzi@unibo.it.

ing some potential cases of breach of the contract when contract performance occurs through blockchain-based smart contracts. The fact that non-performance remains practicable implies that consumers cannot solely rely on the code, and they have to find further ways to enforce their rights. Moreover, Section VI. criticises the idea that the obliged party cannot exercise any control on the execution of the smart contract because of blockchain decentralisation. It clarifies that adopting a decentralised technology like the blockchain does not necessarily mean that the trader cannot influence the execution of the smart contract. One thing is the technology as such, while another thing is how the technology is used. In this regard, the section describes the typologies of blockchain and identifies some hypothetical scenarios of use of smart contracts and the blockchain for the automatic performance of B2C contracts.

Starting from the analysis of the scenarios, it is observed that the trader can still control contract performance. More specifically, the trader can exercise a direct or indirect control on contract execution. Direct control depends on the characteristics of the application and the subject matter of the obligation, and is deepened in Section VI. Indirect control derives from the fact that in B2C contracts the business dictates the contractual conditions, as better illustrated in Section VII. In sum, the article shows that blockchain-based smart contract does not help to solve the problem of lack of trust in the business, as traditional legal instruments for consumers' protection do. That said, consumers still need to resort to some legal instruments for the *ex-post* enforcement of contracts. Hence, Section VIII. verifies the suitability of current remedies for non-performance of the contract even for the blockchain context.

The last section makes a summary of the results of the analysis and some concluding remarks.

II. Functioning of Blockchain and Smart Contracts

Smart contracts are deterministic computer programs that can automatically execute on a blockchain according to prespecified functions.[1] They represent the most advanced blockchain applications.[2] They are deterministic because they follow the instructions (the functions) of the code and always return the same output.[3] Through this mechanism, the smart contract can fix that 'if X, then Y' (where X is the input and Y the output). So, automatic execution means that the code can verify by itself, without human intervention, the inputs it receives and decides whether a specific condition is met.[4]

Smart contracts, despite the referral to 'contracts', are not contracts. They do not always have a legal meaning. They can automate every action or operation. Of course, they can get legal relevance. They can also be applied in the contractual domain. Here, the smart contract is a tool for performing contractual obligations. In this case, somebody suggested talking about 'smart legal contracts', as opposed to 'smart contract code'.[5]

The use of electronic means to automatically perform contracts is not a novelty.[6] These kinds of programs have been operating for several years, and they can also exist without the blockchain.[7]

The blockchain is a distributed database. Distributed means that a copy of the same data set is stored and replicated across a network of nodes, or electronic devices.[8] Distributed systems developed to overcome two main problems.[9] Firstly, they are more secure in case of shutdowns. Centralised systems have one server, while distributed systems can rely on several servers that continue to operate through data replication. Secondly, traditional client-server systems become overwhelmed when the traffic of data is very high. To face more requests, the hardware has to be upgraded, which can be very expensive. Distributed systems are more efficient and less costly because more computers hold the same information.

In distributed ledgers, to ensure that all nodes return the same latest version of data, consensus algorithms are developed. They set the rules to update the system.[10] The blockchain is a distributed ledger. The difference is in the way the nodes reach the consensus on the updating.[11] While in distributed databases coordination between nodes is centralised (i. e. there is a master node that coordinates the others), in distributed ledgers nodes update by following some shared rules, on a peer-to-peer basis. Therefore, the system is distributed and decentralised.

The peculiarity of blockchain is its tamper-resistance.[12] Records in the blockchain are grouped together in blocks. A hash identifies every block. A hash is a string of random letters and numbers that cannot be modified without chan-

1 P. Cuccuru, 'Beyond Bitcoin: an early overview on smart contracts' (2017) 25 International Journal of Law and Information Technology 179, 185.

2 Perugini and Dal Checco call blockchain platforms that support smart contracts 'Platforms 3.0'. See M. L. Perugini, P. Dal Checco, 'Smart Contracts: A Preliminary Evaluation' (*SSRN*, 8 December 2015) 18 <https://ssrn.com/abstract=2729548> accessed 5/7/2021.

3 A. Anand *et al.*, 'The Legal Aspects of Blockchain' (*UNOPS* 2018) 21 <https://www.unops.org/> accessed 5/7/2021.

4 C. Syllaber, B. Walti, 'Life Cycle of Smart Contracts in Blockchain Ecosystems' (2017) 8 Datenschutz und Datensicherheit 497, 498.

5 J. Stark, 'Making Sense of Blockchain Smart Contracts' (*CoinDesk*, 7 June 2016) <https://www.coindesk.com/making-sense-smart-contracts> accessed 5/7/2021. 'Smart contracts' is a misleading expression because it recalls contracts. The computer scientist Nick Szabo coined the term 'smart contract' in the 1990 s. He envisioned the possibility to embed contractual clauses in hardware and software that should have substituted humans in contracting. He desired to overcome the problem of lack of trust between parties, which causes delays, obstacles and supplementary costs. At that time, technological advancements did not allow Nick Szabo to move from theory to practice, as it is nowadays with blockchain and smart contracts. See N. Szabo, 'Smart Contracts' (1994) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.-contracts.html> accessed 5/7/2021; N. Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2 First Monday <https://ojphi.org/ojs/index.php/fm/article/view/548/469> accessed 5/7/2021.

6 A. Davola, R. Pardolesi, 'What is wrong in the debate about Smart Contracts' (2020) 5 Journal of European Consumer and Market Law 201, 204.

7 S. A. McKinney, R. Landy, R. Wilka, 'Smart contracts, blockchain, and the next frontier of transnational law' (2018) 13 Washington Journal of Law, Technology & Arts 313, 315.

8 J. Bacon, J. D. Michels, C. Millard, J. Singh, 'Blockchain Demystified', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 268/2017, 4 <https://ssrn.com/abstract=3091218> accessed 5/7/2021.

9 P. De Filippi, A. Wright (eds), *Blockchain and the law – the rule of code* (Harvard University Press 2018) 17.

10 M. Finck (ed), *Blockchain regulation and governance in Europe* (Cambridge University Press 2018) 7.

11 Distributed ledgers operate in an adversarial environment (i. e. assuming not every participant is honest), and are designed to be Byzantine fault-tolerant (which means that they can run even if a certain number of nodes are acting maliciously). G. Hileman, M. Rauchs, '2017 Global Blockchain Benchmarking Study' (*SSRN*, 22 September 2017) 23-24 <https://ssrn.com/abstract=3040224> accessed 5/7/2021.

12 On blockchain technology, see Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' (proceedings of the 2017 IEEE 6th International Congress on Big Data, Honolulu, 25-30 June 2017) <https://ieeexplore.ieee.org/document/8028379> accessed 5/7/2021; I. Bashir (ed), *Mastering Blockchain* (2nd edn, Packt 2018).

ging the underlying data. It is practically impossible that different data return the same hash value. So, hashes safeguard data integrity. Hashes of the blocks are linked together to form a chain. Consequently, any unauthorised change will be immediately visible, because it would cause a modification of the hash and the linked ones. Any attempt of re-hashing could be successful only if the attacker re-hashes all the subsequent blocks, and if the majority of nodes collude to change the current state of the ledger. For this reason, the blockchain is considered unilaterally immutable.[13]

Blockchain-based smart contracts take advantage of blockchain properties.[14] Once added on the blockchain, they cannot be unilaterally changed or modified. As a result, they cannot avoid execution and or execute themselves incorrectly. Moving to smart legal contracts, some studies state that the decentralisation and tamper-resistance of blockchain technology determine that no single contracting party is in the absolute control of the blockchain and can interrupt or modify the execution of the smart contract code.[15] Therefore, it is assumed that it removes the need to trust that the other party rightly performs the contract because trust is in the code.[16] There is a shift from trust in the counterparty to trust in code.[17] For this reason, maybe blockchain technology can be of support for fostering trust in commerce. In particular, electronic commerce entails the greatest dangers, especially for unaware consumers.[18]

III. European Legal Instruments for Consumers' Protection in B2C Online Contracting

When two or more parties conclude a contract, there is the risk that the obliged one does not fulfil her obligations. For this reason, contract law provides some remedies in case of breach of the contract.[19] The latter induce parties to engage in trade.[20] Indeed, trade is based on trust. People are less likely to enter into agreements if they do not have sufficient guarantees that the ones they trade with will perform contracts. In other terms, the function of these remedies is to compensate for the absence of trust in the (correct) performance of the contracting party.[21]

Contract enforcement becomes problematic when parties trade on the Internet. The Internet is an open network that permits communication at long distances.[22] If it has favoured international trade on the one hand, and opened electronic commerce to consumers all around the world, on the other hand it has rendered commerce very risky.[23]

Of course, consumers face the major risks, in the light of their weaker position compared to businesses. At the EU level, much has been done since the 1970 s to protect and enforce consumers' rights against abuses and unfair business practices.[24] Nevertheless, the capacity of these legal interventions

13 O. Meyer, 'Stopping the Unstoppable. Termination and Unwinding of Smart Contracts' (2020) 1 Journal of European Consumer and Market Law 17.

14 The European Union Blockchain Observatory and Forum, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (thematic Report, 27 September 2019) 22 <https://www.eublockchainforum.eu/reports> accessed 5/7/2021, gives the following definition of a smart contract: 'In the blockchain context, it generally means computer code that is stored on a blockchain and one or more parties can access that. These programs are often self-executing and make use of blockchain properties like tamper-resistance, decentralised processing, and the like'.

15 De Filippi, Wright (n 9) 74-75; R.H. Weber, 'Smart Contracts: Do we need New Legal Rules?' in A. De Franceschi, R. Schulze (eds), *Digital Revolution – New Challenges for Law* (Beck Nomos 2019) 299, 308; A. Stazi (ed), *Automazione contrattuale e "contratti intelligenti" – Gli smart contracts nel diritto comparato* (Giappichelli 2019) 100.

16 A. Savelyev, 'Contract law 2.0: 'smart' contracts as the beginning of the end of classic contract law' (2016) Higher School of Economics Research Paper no. WP BRP 71/LAW/2016, 11 <https://ssrn.com/abstract=2885241> accessed 5/7/2021.

17 T. J. De Graaf, 'From old to new: from internet to smart contracts and from people to smart contracts' (2019) 35 (5) Computer Law & Security Review 105322, 2.

18 Below, Section III.

19 The European legislature lacks a general competence for private law. Thus, contract law remedies in case of non-performance are conceived on a national basis.However, for the purpose of this work, some commonalities between the Member States can be considered. Two main projects have attempted to identify these commonalities and elaborate a set of rules to guide contract law interpretation and harmonisation in the EU: the Principles of European Contract Law (PECL), drafted between 1982 and 1996 by a group of academics guided by Professor Ole Lando; the Draft Common Frame of Reference of European Private Law by the Study Group on a European Civil Code (DFCR). The latter includes other fields of private law other than contract law. See, for the PECL, European Union, *The Principles of European Contract Law 2002 (Parts I, II and III)* (SiSU 2002) <http://lexmercatoria.org> accessed 5/7/2021; for the DFCR, Study Group on a European Civil Code, Research Group on EC Private Law, *Principles, Definitions and Model Rules of European Private Law – Draft Common Frame of Reference (DFCR), Outline Edition* (sellier.european law publishers 2009). There is a third similar initiative by the International Institute for the Unification of Private Law (UNIDROIT), called the UNIDROIT Principles of International Commercial Contracts (PICC). However, it explicitly deals with international B2B commercial transactions (not with contract law in general), and is intended to restate the contract laws of the entire world (not only European). See International Institute for the Unification of Private Law, *Unidroit Principles of International Commercial Contracts* 2016 <https://www.unidroit.org> accessed 5/7/2021.

20 In general, parties can claim for the performance of the contract through litigation or arbitration or damages for non-performance. So, the debtor can be forced to perform or economically compensate the creditor for non-performance. Another remedy is the possibility of asking for the termination of the contract. The latter is applicable in case of mutual performances, in the event the debtor does not perform the contract. All these remedies intend to lead the other party to perform the contract and protect creditors from unreliable debtors. For further details, see J. Kleinschmidt, 'Particular remedies for non-performance' in N. Jansen, R. Zimmermann (eds) *Commentaries on European contract laws* (Oxford 2018) 1185-1556.

21 C. Poncibò, L.A. Di Matteo, 'Smart contracts, Contractual and Noncontractual Remedies' in L.A. Di Matteo, M. Cannarsa, C. Poncibò (eds), *The Cambridge Handbook of smart contracts, blockchain technology and digital platforms* (Cambridge University Press 2020) 122.

22 C. Reed, 'Electronic commerce' in C. Reed (ed), *Computer Law* (7th edn Oxford University Press 2011) 268.

23 The Internet favours the conclusion of cross-border contracts. In this regard, the United Nations Commission on International Trade Law (UNCITRAL) works for the harmonisation of e-commerce laws all around the world. See G. Finocchiaro, 'Il ruolo dell'UNCITRAL nello sviluppo della disciplina sul commercio eletronico' in G. Finocchiaro and F. Delfini (eds), *Diritto dell'informatica* (Utet 2014) 63. One important outcome is the United Nations Convention on the Use of Electronic Communications in International Contracts of 23 November 2005 <https://treaties.un.org> accessed 5/7/2021. For more information, see A.H. Boss and W. Kilian (eds), *The United Nations Convention on the Use of Electronic Communications in International Contracts: An In-depth Guide and Sourcebook* (Wolters Kluwer 2008); M. Ratti, 'La Convenzione sull'uso delle comunicazioni elettroniche: le principali disposizioni' in Finocchiaro and Delfini (*ibid*) 71. The Convention is inspired by the principles elaborated in the 1996 Model Law on Electronic Commerce <https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf> accessed 5/7/2021. Another considerable achievement of the UNCITRAL, that was not explicitly born for electronic commerce but for commercial cross-border sales contracts, is the Convention on Contracts for the International Sale of Goods (CISG) of 1980 <https://www.uncitral.org/pdf/english/texts/sales/cisg/V1056997-CISG-e-book.pdf> accessed 5/7/2021. About the Convention, see S. Kröll, L. Mistelis, M. del Pilar Perales Viscasillas (eds), *UN Convention on Contracts for the International Sale of Goods, A Commentary* (2nd edn Beck Hart Nomos 2018). The Convention contains some rules concerning applicable remedies for non-performance.

24 For a summary of the EU legal framework regarding consumer protection, see European Parliament, ' Protecting European consumers' (2019) 3-4 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/633141/EPRS_BRI(2019)633141_EN.pdf> accessed 5/7/2021.

to enforce consumers' contracts is still insufficient. Many times consumers do not know their rights. Furthermore, they are often discouraged to enforce them because of the low value of their complaints with respect to the complexity, length and costs of the procedures.[25]

With the rise of electronic commerce on the Internet, risks for consumers have even increased. Business-to-consumers (B2C) electronic commerce usually occurs by accessing some websites and clicking some virtual buttons.[26] The process of contract conclusion is very fast.[27] Moreover, they do not have the possibility to directly test products and services before the conclusion of the contract. As a consequence, traders may abuse of consumers' weaker position and behave in an unreliable way.

On the Internet, consumers communicate with suppliers from behind a computer screen. They do not know traders' identities.[28] Thus, in case of breach of contracts, it may be unlikely that consumers are able to prosecute them. Lastly, the Internet favours the conclusion of cross-border contracts, so any controversial has to face significant costs and the problem of the choice of applicable law and jurisdiction.[29] In particular, the criteria set by the Bruxelles I-*bis* Regulation[30] and the Rome I Regulation[31] have revealed quite problematic in electronic commerce because they are based on territoriality, while the Internet cannot be constrained into physical borders.[32]

Of course, these assumptions are also valid in B2B contracts. However, as said before, consumers are inherently more disadvantaged than traders. So, apart from traditional consumer law, in Europe the legislator has made an attempt to protect consumers even in the online market and to guarantee the enforcement of B2C contracts. In electronic commerce, businesses have mandatory information duties towards consumers, both under Directive 2000/31/CE on electronic commerce[33] and Directive 2011/83/EU[34] on consumer rights.[35] Such information mainly concerns the suppliers, the products and services offered, the process of contract conclusion, and some additional suppliers' duties and recipients' rights. For example, the supplier has to acknowledge the receipt of the recipient's order without undue delay and by electronic means.[36] Consumers can also withdraw from distance contracts at no costs and without any reason by the following 14 days.[37] Such information has to be given in a clear and comprehensible manner to ensure consumers' real understanding.[38] The recent Proposal of the European Commission

25 See European Commission, 'Consumer Conditions Scoreboard' (2019 edn) <https://ec.europa.eu/info/sites/info/files/consumers-conditions-scoreboard 2019_pdf_en.pdf>.

26 On the Internet, businesses usually conclude adhesion contracts with consumers in the form of wrap agreements, instead of by exchanging e-mails. The most common wrap contracts are click-wrap and browse-wrap agreements. In a click-wrap agreement, the terms are presented in a scrollable box or at a hyperlink, and the other party has to click on an 'I agree' button to accept. In a browse-wrap agreement, the terms are accessible through hyperlinks ('Terms of use' or 'Legal terms') and the user accepts using a website or downloading the digital content, without having to click on the 'I agree' box or take any other positive action. Existence of consent has been discussed about click-wrap and browse-wrap agreements. In both cases, courts have expressed the need to provide the other party with sufficient notice of the existence of the terms before or at the time of contract conclusion. In this regard, it is not sufficient to give notice of the existence of the terms, but the terms have to be conspicuously and clearly presented to the non-drafting party. Therefore, the supplier has to take care that the other party is (or should be reasonably) aware of being entering into a contract. Without these arrangements, it has been argued that in browse-wrap contracts it is unlikely that the non-drafting party is aware of the existence of a contract because she is not required to take any positive assenting action. Similarly, in click-wrap contracts, online users do not give importance to the action of clicking on a box as they do with the physical act of placing a signature. In the latter case, however, a higher level of awareness is presumed because the offeree is asked to do something to enter the agreement. On this topic, see R. Momberg, 'Standard terms and transparency in online contracts' in A. De Franceschi (ed), *European Contract Law and the Digital Single Market* (Intersentia 2016), 189-207.

27 Businesses make 'take it or leave it' offers, standard contracts that the consumer cannot but adhere or not adhere. This particular kind of contract conclusion favours efficient and fast transactions at the detriment of negotiations and dialogue between the parties. See M. Granieri, 'Technological contracts' in P. G. Monateri (ed), *Comparative Contract Law* (Edward Elgar, Cheltenham-Northampton 2017).

28 In 1993, the New Yorker published a cartoon showing a dog sitting behind a computer screen with the sentence 'On the Internet, nobody knows you are a dog'.

29 Reed (n 22) 269.

30 Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1.

31 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6.

32 In particular, both the Bruxelles I-*bis* Regulation (Art.17(1)(c)) and the Rome I Regulation (Art.6(1)) provide peculiar protection for consumers when the business has directed its activities to the consumer's country. The former favours the place of residence or domicile of the weaker party and prevents that the trader can choose a less favourable jurisdiction for the consumer. The latter states that consumers are subject to the law of the country in which they have their habitual residence and, in case of a different choice between the parties, this choice may not deprive consumers of the protection that would be afforded by the law which would have been applicable if the parties had not made any choice. In these cases, the question is under which circumstances can one say that the business' activities are directed to the consumer when contracts are concluded via a website. On this point, the European Court of Justice has given a non-exhaustive list of factors to take into account. For more information, see P. Kindler, 'The law applicable to consumer contracts in the Digital Single Market' in De Franceschi (n 26), 173-186; D. Svantesson, 'Digital Contracts in Global Surroundings' in S. Grundmann (ed), *European Contract Law in the Digital Age* (Intersentia 2018) 49-86.

33 Directive (EC) 31/2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1, Artt. 5 and 10. See G. Pearce, N. Platten, 'Promoting the Information Society: The EU Directive on Electronic Commerce' (2000) 6 European Law Journal 363; C. Hultmark Ramberg, ' The E-Commerce Directive and Formation of Contract in a Comparative Perspective' (2001) 26 European Law Review 429.

34 Directive (EU) 83/2011 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance [2011] OJ L 304/64. See H. Hall, G. Howells, J. Watson, ' The Consumer Rights Directive – An Assessment of its Contribution to the Development of European Consumer Contract Law' (2012) 8 European Review of Contract Law 139; S. Grundmann, 'The EU Consumer Rights Directive – Optimizing, Creating Alternatives or a Dead-End' (2013) 18 Uniform Law Review, 98.

35 The recent Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7 (or 'Omnibus Directive') has amended Directive 2011/83/EU. The Directive has been approved to strengthen enforcement of EU consumer law and modernising EU consumer protection rules in view of market development, like the norms on information requirements for distance contracts (e. g. the trader has to inform the consumer whether the price was personalised on the basis of automated decision making; there are additional information requirements for contracts concluded on online marketplaces; etc.). By 28 November 2021, Member States shall implement the Directive. Implementation rules shall apply from 28 May 2022. For a summary of the novelties brought by the Directive, see the European Commission Factsheet 'New Deal: What benefits will I get as a consumer?' available at the following link <https://ec.europa.eu/info/sites/info/files/factsheet_new_deal_consumer_benefits_2019.pdf> accessed 5/7/2021.

36 Art. 11 of the Directive (EC) 31/2000.

37 Art. 9 of the Directive (EU) 83/2011. Norms related to the right of withdrawal are more favourable for the consumer if compared to general provisions.

38 These provisions stress the importance of quality – more than quantity – of information.

for a Digital Services Act,[39] which is supposed to amend Directive 2000/31/EC, contains an obligation for certain online platforms to receive, store and partially verify and publish information on traders using their services to conclude distance contracts with European consumers.[40] The latter provision aims to ensure an even safer environment for consumers.

Then, to improve the rights of consumers with regard to the conformity of supplied goods, digital contents and services to the contract and remedies in case of defects, the European Parliament and the Council have adopted the Directive (EU) 2019/770[41] and Directive (EU) 2019/771[42] on contracts for the sale of goods and contracts for the supply of digital content and digital services.[43] In particular, by introducing harmonised rules for all Member States and objective requirements for conformity, both Directives are intended to provide better protection for consumers.[44]

Lastly, to overcome the problems related to cross-border disputes, the European Union has created and Online Dispute Resolution (ODR) platform for consumers that seek to resolve online disputes stemming from online sales or services contracts.[45] Indeed, ODRs are alternative dispute resolution means that take place entirely online, so they can put in communication parties located in different countries.

IV. Blockchain as a Tool for Enhancing Consumers' Trust in B2C Contracts?

Some studies state that decentralisation and tamper-resistance of blockchain technology determine that no single contracting party is in the absolute control of the blockchain and can interrupt or modify the execution of the smart contract code.[46] Therefore, it is assumed that it removes the need to trust that the other party rightly performs the contract because trust is in the code.[47] There is a shift from trust in the counterparty to trust in code.[48] The following example can clarify the above statement.[49]

A seller of a car has installed an immobiliser that allows the starting of the car after payment by the buyer. The immobiliser connects with the vendor's bank to verify whether the buyer has effectively paid. If yes, the car starts. If no, the car does not start. This is a traditional smart contract. The immobiliser receives information by the bank about the payment and acts accordingly. The immobiliser is under the control of the seller that can instruct the immobiliser not to start the car even though payment has been made. Instead, with the blockchain, decentralised execution and tamper resistance prevent the seller from altering the functioning of the immobiliser. By uploading the smart contract on the blockchain, the party cannot refuse to perform. It is asserted that there is no more need to trust in the other party – that cannot avoid execution – but in the code.

From this follows that blockchain technology might be of support for consumers to remedy a lack of trust in the obliged party. Because smart contracts automate performance, consumers are not required to activate claim procedures, with significant time and cost savings. Secondly, as blockchain prevents the breach of contracts, blockchain-based smart legal contracts might be suitable when consumers negotiate with unknown offerors at a distance and by electronic means. As a matter of fact, if blockchain guarantees performance there would be no need to identify the counterparty and prosecute her.

Fewer disputes would also imply less costs of litigation and avoid the obstacles related to applicable law and jurisdiction in cross-border contracts especially when they have been concluded through the Internet.

For instance, the insurance sector is developing applications that automate the performance of insurance contracts for consumers thanks to blockchain-based smart contracts. More specifically, some initiatives are focusing on the enforcement of passengers' right to be indemnified in case of delays or cancellation of air flights.[50]

---

39 Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final <https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=-COM%3A2020%3A825%3AFIN> accessed 5/7/2021. The Proposal builds on the key principles set out in the e-Commerce Directive while seeking to ensure the best conditions for the provision of innovative digital services in the internal market. Along with the Digital Markets Act, the Digital Services Act constitutes the Digital Services Act package, which encompasses a single set of new rules applicable across the whole EU that will create a safer and more open digital space, with European values at its centre. For more information, see <https://ec.europa.eu/digital-single-market/en/digital-services-act-package> accessed 5/7/2021.

40 See Art. 22 of the Proposal.

41 Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1.

42 Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods amending Regulation (EU) 2017/2394 and Directive 2009/22/EC and repealing Directive 1999/44/EC [2019] OJ L 136/28.

43 The Member States shall adopt the necessary measures to comply with the Directives by 1 July 2021, and apply them from 1 January 2022. See: R. Brownsword, 'The E-Commerce Directive, consumer transactions, and the Digital Single Market – Questions of regulatory fitness, regulatory disconnection and rule redirection' in Grundmann (n 32) 198-202; R. Shulze, D. Staudenmayer, S. Lohsse (eds), *Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps* (Hart Nomos 2017); R. Schulze, 'Supply of Digital Content. A New Challenge for European Contract Law' in De Franceschi (n 26), 127; G. Howells, 'Reflections on Remedies for Lack of Conformity in Light of the Proposal of the EU Commission on Supply of Digital Content and Online and Other Distance Sales of Goods', *ibid*, 145.

44 The consumer has to expressly and separately accept eventual deviations from such objective requirements when concluding the contract.

45 By adopting Regulation (EU) 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes (Regulation on Consumer ODR) <http://ec.europa.eu/consumers/odr/> accessed 5/7/2021. See J. Morais Carvalho, J. Campos Carvalho, 'Online Dispute Resolution Platform – Making European Contract Law More Effective' in De Franceschi (n 26) 245-266. See also I. Amro (ed), *Online Arbitration in Theory and in Practice – A Comparative Study of Cross-Border Commercial Transactions in Common Law and Civil Law Countries* (Cambridge Scholars Publishing 2019).

46 De Filippi, Wright (n 9) 74-75; R. H. Weber, 'Smart Contracts: Do we need New Legal Rules?' in A. De Franceschi, R. Schulze (eds), *Digital Revolution – New Challenges for Law* (Beck Nomos 2019) 299, 308; Stazi (n 15) 100.

47 Savelyev (n 16) 11.

48 De Graaf (n 17) 2.

49 The example is taken from De Graaf (n 17) 4.

50 Some examples of smart insurance contracts for automating claims and refunds for flight delays or cancellations are the products built by the Etherisc community (https://fdd.etherisc.com), InsurETH by the start-up Oraclize, and Fizzy by AXA insurance company. Smart contracts receive data from the websites of airports regarding flight status through oracles. About InsurETH, see M. L. Perugini, P. Dal Checco (n 2) 22-23; more information about Fizzy can be found at the following link: <https://fizzy.axa/en-gb/> accessed 5/7/2021. In 2018, The Italian National Association of Insurance Companies (ANIA), the Italian Institute for Insurance Supervision (IVASS), the Research Centre on Technology, Innovation and Financial Services of Università Cattolica del Sacro Cuore in Milan and the company Reply started a collaboration and created the Insurance Blockchain Sandbox (<https:/7www.insuranceblockchainsandbox.com>) to experiment real use cases of smart insurance contracts in a limited and protected environment. As can be seen in the official IBS website, three use cases were developed on travel insurance: one is about risks of bad weather; the second is for flight delays or cancellation; the third is for lost luggage <https://www.reply.com/en/content/insurance-companies-start-experimenting-with-blockchaintechnology> accessed 5/7/2021.

The insurance sector is one of the most promising in terms of number of blockchain-related initiatives.[51] Indeed, insurance claims processing and settling are usually complex, not always fair, and lengthy. This lowers insured people's trust in their insurance companies. On the other hand, insurance still involves many manual and paper-based processes. Moreover, it is a heavily intermediated industry (e. g. brokers, reinsurance companies). Insurers have to make many controls to verify that the payment is effectively due. There is a high risk of claim fraud. For these reasons, the costs are very high. With smart contracts, on the contrary, the code verifies if there are the conditions to perform insurer's obligations. The policyholder does not have to start the claim procedure, and the insurance company has not to appoint any employee. Everything is automated. Blockchain technology ensures that the insurance company cannot but pay if the contractual conditions are met.[52] In line with what affirmed above, such experimentations might have the potential to lower disputes between the insurance companies and their customers and pursue passengers' rights.[53]

The following sections criticise the above statements. First of all, Section V. attempts to demonstrate that blockchain technology cannot give rise to breach-less contracts by enlisting some potential cases of breach of the contract when contract performance occurs through blockchain-based smart contracts. The aim of this article is to show that blockchain-based smart contract do not help to solve the problem of lack of trust in the business, as traditional legal instruments for consumer protection do.

V. Blockchain-Based Smart Contracts and the Myth of Breach-Less Contracts

As reported in the preceding section, it is affirmed that blockchain technology guarantees contract performance. In reality, it has been pointed out that blockchain technology cannot give rise to breach-less contracts.[54] There can be several situations in which the self-execution of a smart contract leads to the breach of that contract. It has been made an attempt to catalogue these hypotheses into three groups: a) the content of the code does not match with the will of the parties, thus determining that the execution of the contract does not satisfy the consumer; b) technological problems that impact on the performance of the contract; c) other problems due to the closed nature of the blockchain, when there is the need to link the smart contract with the off-chain world to perform the contract.

The first hypothesis is immediately understandable: when the code does not perform as intended by the consumer and agreed in the contract, the contract is breached.

Turning to the second, blockchain-based applications are made up of multiple components. Technological problems can negatively affect such components and cause the violation of the contract.

First of all, the code of the smart contract can be subject to bugs, like any computer program.[55] Problems may also derive from the underlying blockchain.[56] These bugs can give room for manipulation of the execution of a smart contract that exploits the security flaw and makes smart contracts susceptible to abuse.[57] Moreover, oracles can be compromised.[58]

51 M. Rauchs et al ., '2nd Global Enterprise Blockchain Benchmarking Study' (SSRN, 18 September 2019) 32-33 <https://ssrn.com/abstract=3461765> accessed 5/7/2021. The insurance sector is developing numerous projects, from smart insurance contracts with customers, prevention of insurance fraud, to applications that automate manual processes involving many actors, e. g. the reinsurance business. See M. Abramowicz, 'Blockchain-Based Insurance' (2019) GWU Law School Public Law Research Paper No. 2019-12 <https://ssrn.com/abstract=3366603> accessed 5/7/2021. Also insurance institutions and companies are realising the potential of blockchains and smart contracts, e. g. see: Organisation for Economic Cooperation and Development (OECD), 'Financial Markets, Insurance and Pensions: Digitalisation and Finance' (2018) 62-63 <https://www.oecd.org/finance/privatepensions/Financial-markets-insurance-pensionsdigitalisation-and-finance.pdf> accessed 5/7/2021; European Insurance and Occupational Pensions Authority (EIOPA), 'EIOPA InsurTech Roundtable – How Technology and data are reshaping the insurance landscape. Summary from the roundtable organised by EIOPA on 28 April 2017' <https://eiopa.europa.eu/Publications/Reports/08.0_EIOPA-BoS17-165_EIOPA_InsurTech_Roundtable_summary.pdf#search=-EIOPA%20InsurTech%20Roundtable%20How%20technology%20and%20data%20are%20reshaping%20the%20insurance%20landscape> accessed 5/7/2021. For further analysis of current challenges faced by the insurance industry and expected benefits of blockchain technology see: M. Mainelli, C. von Gunten, 'Chain of a lifetime: how blockchain technology might transform personal insurance' (Long Finance Report, December 2014) <http://archive.longfinance.net/images/Chain_Of_A_Lifetime_December2014.pdf> accessed 5/7/2021.

52 About insurance contracts and blockchain-based smart contracts: J. Evans, 'Curb your enthusiasm: the real implications of blockchain in the legal industry' (2018) 11(2) Journal of Business, Entrepreneurship and the Law 273, 294-296; A. Borselli, 'Smart Contracts in Insurance. A Law and Futurology Perspective' (*SSRN*, 19 January 2019) 9-10 <https://ssrn.com(abstract=3318883> accessed 5/7/2021.

53 About blockchain-based smart contracts and passengers' reimbursement in case of delay or cancellation, see O. Borgogno, 'Usefulness and Dangers of Smart Contracts in Consumer Transactions' in Di Matteo, Cannarsa, Poncibò (n 21) 297-299. The paragraph also recalls the EU legal framework for the protection of passengers (by rail, bus/coach, ferry or airplane) within the Internal Market.

54 Poncibò, Di Matteo (n 21) 124; McKinney, Landy, Wilka (n 7) 329.

55 Savelyev (n 16) 14; for example, in 2016, Peter Vessenes (co-founder of the Bitcoin Foundation) estimated that Ethereum smart contracts contained 100 errors every 1000 lines of software code. See P. Vessenes, 'Ethereum Contracts are Going to be Candy for Hackers' (*Vessenes*, 18 May 2016) <http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/> accessed 5/7/2021.

56 E. Mik, 'Blockchains. A Technology for Decentralized Marketplaces' in Di Matteo, Cannarsa, Poncibò (n 21) 175. They predominantly have regard to the selection and order of transactions. On this point, see L. Luu *et al*., 'Making Smart Contracts Smarter' in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, October 2016, 254-269 <https://doi.org/10.1145/2976749.2978309> accessed 5/7/2021. For example, transaction-ordering dependency occurs when two transactions that invoke the same contract are included in one block. Users have uncertain knowledge of which state the contract is at when their individual invocation is executed. Thus, there is a discrepancy between the state of the contract that users may intend to invoke and the actual state when their corresponding execution happens. Decisions about the order of transactions are up to the miner, so the final state of the contract depends on how the miner orders the transactions. This can give unexpected results to a user invoking a smart contract when there are concurring transactions. For instance, in a sale agreement, the seller updates the price of the item. It may happen that the buyer has to pay a higher price than the one she agreed to pay when she sent the buy request.

57 To take the example of transaction-ordering dependency, Luu (n 56) 257 describes a Puzzle contract in Ethereum that rewards users who solve a computational puzzle. A malicious owner of the contract could exploit transaction-ordering. Namely, the owner could wait until a user sends a correct solution of the puzzle and immediately send a transaction that reduces the reward of the contract to zero. If the miner executes the latter transaction before the user's transaction, the user does not get any reward. Another example is the notorious Dao hack, where an attacker was able to steal over three million ethers by utilising so-called reentrancy vulnerability. See Luu (n 56) 259.

58 E. Mik, 'Smart contracts: terminology, technical limitations and real world complexity' (2017) 9 Journal of Law, Innovation and Technology 269, 297. To avoid oracle failures, someone suggests making use of multiple oracles and data sources. However, V. Gatteschi, F. Lamberti, C. Demartini, 'Technology of Smart Contracts' in Di Matteo, Cannarsa, Poncibò (n 21) 56 observe that 'this approach is still prone to errors, as an ill-intentioned person could still perform a coordinated attack on multiple platforms inspected by the oracles'.

Oracles are interfaces that connect the blockchain with the outside world. They transmit information from external data sources to smart contracts, and vice versa. So, untrustworthy oracles can negatively influence the performance of the contract.[59] Lastly, because oracles do not create the information to send to smart contracts themselves but obtain it from external data sources, it is necessary to select a trustworthy data source. Indeed, the external data source may malfunction or become inactive.[60]

Finally, group c) encompasses the situations when contract execution is only possible by linking the smart contract to the off-chain world. Indeed, blockchain technology is 'deaf and blind', which means that it cannot directly retrieve information except dictated by the protocol (e.g. the transfer of crypto-tokens).[61] In this regard, oracles and data sources were mentioned. Therefore, if such information is not given at all or is incorrect, the contract is not executed or not executed properly. This cannot only happen for technical malfunctions (group b)) but also for human errors or actions. Think, for example, to the courier that signals to have delivered the package to the specified address, while the package has not been sent, or the content of the package differs from what the parties agreed in the contract. The inclusion of input data in the blockchain is under the direct control of someone and does not benefit from the decentralised character of the blockchain.

Furthermore, when the execution of the contract has to produce its effects off the chain, the execution of the smart contract code does not guarantee the performance of the contract. Due to the closed character of the blockchain, further operations outside the database have to follow the outputs of the smart contract code. For example, a smart insurance contract for flight delays detects the policyholder's right to payment. The output of the smart contract code is not sufficient to make the payment, because the insurance company has to activate the payment.[62]

The fact that non-performance remains practicable prevents consumers from solely relying on the code, and they have to find further ways to enforce their rights in case of contractual non-performance.

VI. The Mismatch between Decentralised Technology and Absence of Control on Contract Performance

Even with the blockchain, breaching the contract is possible. Consequently, consumers have to activate claim procedures, with related expenditure of costs and time, and problems of identification of the applicable law and jurisdiction in case of cross-border contracts.[63] Otherwise, they cannot enforce their rights. There is still the need of some *ex-post* remedies to enforce the contract.

There is also another aspect to consider, which concerns the decentralised character of the blockchain.

As already underlined, the peculiarity of blockchain-based contracts is that the obliged party cannot exercise any control on the execution of the smart contract, so she cannot but perform. Instead, it is believed that this is not always true.

The blockchain is a decentralised technology. There is much confusion on the meaning of the term 'decentralisation'. The latter might refer both to the technology as such and the governance of the application that runs on a blockchain.

First of all, blockchain is a kind of technology. It is decentralised because of the consensus protocol shared among nodes, and through which nodes update. A decentralised computer system is more efficient and safer than a centralised one, as already described.[64] Decentralised governance is a separate issue, and has regard to the capacity of controlling and managing the technology (both at the hardware and software level). So, decentralised technology can have centralised governance. This misinterpretation is probably due to the use of the same terms in different fields (not only in the technical one) that have different meanings.[65] Moreover, the political ideas that surrounded blockchain invention may have contributed to creating much confusion on the right meaning of 'decentralisation'.[66]

Blockchain originated from a group of crypto-anarchists[67] that wanted to free people from traditional institutions, like banks.[68] To reach this goal, they primarily needed a system of money transfer that lacked centralised control, but that was safe at the same time.[69] As a matter of fact, the first blockchain applications are the so-called crypto-currencies (the most famous is Bitcoin)[70]. They are a form of digital

59 Oracles might send wrong data to the smart contract (inbound) or to the external source (outbound).

60 M. Giancaspro, 'Is a 'smart contract' really a smart idea? Insights from a legal perspective' (2017) 33(6) Computer Law & Security Review 825, 833. For instance, a smart insurance contract has been programmed to pay the policyholder in the event of a flight delay of two hours. One could imagine that the software of the airport timetable does not operate for a few hours that correspond to the time when a flight delay should be recorded. The example is taken from M. Clément, 'Smart Contracts and the Courts' in Di Matteo, Cannarsa, Poncibò (n 21) 280.

61 O. Rikken *et al*., 'Smart contracts as a specific application of blockchain technology' (2017) 17 <https://dutchblockchaincoalition.org/> accessed 5/7/2021.

62 The alternative is that the insurance company makes the payment in cryptocurrencies. Indeed, smart contracts can directly transfer cryptocurrencies because they are native tokens of the blockchain.

63 It is very likely to have cross-border contracts because nodes of the blockchain can be located everywhere and accessed from everywhere as is for electronic commerce, especially if blockchain are open networks (permissionless) such as the Internet.

64 See Section II.

65 Mik (n 58) 270 states that 'the legal analysis of smart contracts is rendered difficult by the fact that the phenomenon originated in technical writings which are characterised by inconsistent and incorrect use of legal terms'.

66 *Ibid* 270:'To complicate matters, the smart contract narrative is often laden with ideologically charged arguments that associate certain technological features of blockchains (e.g. decentralised consensus) with broader social and economic issues, such as the disenchantment with financial institutions or the (perceived) lack of trust in the legal system'.

67 Called 'The Cypherpunk Movement', whose manifesto suggested the use of information technology to defend everybody's privacy, safe from government institutions, relying on cryptography and anonymous systems for sending e-mails, digital signatures, and electronic money. For the Manifesto, see E. Hughes, 'A Cypherpunk's Manifesto' (1993) <https://www.activism.net/cypherpunk/manifesto.html> accessed 5/7/2021.

68 D. Chaum, 'Security without Identification: Transaction Systems to Make Big Brother Obsolete' (1985) 28(10) Communications of the ACM 1030.

69 They had to overcome the 'double spending' problem. Indeed, digital cash can be easily copied. So, in the absence of a trusted third party like a bank, a subject may send the same amount to more recipients. See U.W. Chohan, 'The Double Spending Problem and Cryptocurrencies' (*SSRN*, 19 December 2017) <https://ssrn.com/abstract=3090174> accessed 5/7/2021.

70 The Bitcoin platform was first described in an article by Satoshi Nakamoto (a pseudonym). See S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 5/7/2021. On the legal issues related to crypto-currencies, see F. Barrière, 'Blockchain-Based Financial Services and Virtual Currencies in France' (2020) 1 European Consumer and Market Law 40; G. Gitti, M. Maugeri, 'Blockchain-Based Financial Services and Virtual Currencies in Italy' (2020) 1 European Consumer and Market Law 43; A.M. Gambino, C. Bomprezzi, 'Blockchain e criptovalute' in G. Finocchiaro, V. Falce (eds), *Fintech: diritti, concorrenza, regole – Le operazioni di finanziamento tecnologico* (Zanichelli 2019) 267.

'money' that people can exchange anonymously and without asking banks to guarantee that money is not double-spent, thanks to tamper-resistance of the blockchain.[71] Then, blockchain technology is commonly associated with disintermediation or a lack of central authorities.

Having said this, blockchain can be centralised at both the hardware and the software. Usually, blockchains can be permissionless or permissioned. Differences have regard to the different types of permission granted to network participants. Namely, there is the permission to write (i. e. to generate new transactions) and commit (i. e. to update the state of the ledger and add new blocks).[72] In permissionless blockchains, anyone can become a user and write transactions without pre-identification. Any computer can be a node in the network.[73] Furthermore, everyone can add new blocks and update the ledger. In permissioned blockchains, only pre-selected participants can transact in the network, only authorized devices can take part as nodes and add blocks.

Permissionless and permissioned blockchains also differ for permission to access the ledger and read transactions. Indeed, permissionless blockchains are usually public, so they have a high degree of openness and anyone can read the transactions. Instead, permissioned blockchains are generally private, because transactions are only visible to authorised users. The reason is that permissionless blockchains are general purpose and do not belong to anyone. In contrast, permissioned blockchains are specifically built to fit a specific purpose of someone (e. g. a single entity or a consortium) that decided to invest in setting up the entire system (hardware and software).

Permissionless and permissioned blockchain can guarantee a different level of immutability. As mentioned before,[74] modifications can only occur if the majority of nodes collude to change the current state of the ledger. In permissionless blockchains, this is more difficult. Firstly, because permissionless blockchains are open to the participation of new users, so the copies in which the blockchain is stored continuously grow and are not easily controllable. Secondly, collusion is complicated by the fact that underlying identities are unknown.[75] In this respect, it is objected that because adding new blocks is usually expensive[76] mining pools[77] have emerged over time that increase the risk of a 51 % attack.[78] However, it is also argued that these consolidations of miners are not interested to alter the system because they are the ones who most financially benefit from it.[79] In permissioned blockchains, instead, the number of nodes is smaller and validators are known. All this facilitates changes.[80]

In light of the above, centralisation is typical of permissioned blockchains, because they are closed and proprietary systems. Centralised governance implies the possibility to control the execution of the smart contract, to stop or modify it. So, in permissioned blockchains it might be possible to influence the performance of the contract.

To clarify this concept, one has to focus on the possible concrete use of blockchain and smart contracts in the contractual domain. Before doing that, the distinction between nodes and users also has to be highlighted. Nodes are electronic devices that store copies of the blockchain. They are the units of the blockchain network. Users are the individuals or entities that make use of a blockchain-based application. Nodes and users are not synonyms. There can be some nodes that are not users. For example, miners can be interested in running a node to compete for adding new blocks and be rewarded. But they are not obliged to write new transactions.[81] Similarly, not all users run a node. They can interact with the distributed ledger both directly, by running a node, or indirectly, through the interface of a blockchain-based application.[82] The user might be not even aware that she is using a service built on top of a blockchain. By cross-referencing permissionless/permissioned blockchains and nodes/users, the following four concrete scenarios may be envisaged:

(i) Permissionless blockchain/nodes

Users get access to a permissionless blockchain (that supports smart contracts) by running a node. They use the platform for the conclusion/execution of contracts. Users may be both businesses and consumers.[83] It can be imagined that businesses enter such a blockchain to encounter potential customers.

(ii) Permissionless blockchain/application users

This is mainly a B2C scenario, where the business develops services for its customers and uses a permissionless blockchain as back-end. The front-end is a blockchain-based application for users that do not run a node of the permissionless blockchain.Here, the contract is concluded online, and the smart contract is the tool for performing the agreed contract.[84]

(iii) Permissioned blockchain/nodes

In this scenario, each user also runs a node of a permissioned blockchains. It is considered suitable for B2B contractual relationships, for two main reasons. Firstly, because they have the economic power to create their blockchain, as op-

71 To avoid the double-spending problem, the protocol searches thorough all previous transactions to verify that a user has enough bitcoins to send. If it is the case, the transaction is valid and is added to a block. Otherwise, the network rejects the transaction.
72 Hileman, Rauchs (n 11) 20.
73 Permissionless ledgers usually rely on open-source software that anyone can download.
74 Section II.
75 H. Eenmaa-Dimitrieva, M. J. Schmidt-Kessen, 'Regulation through code as a safeguard for implementing smart contracts in no-trust environments', EUI Working Paper LAW 2017/13, 11 <http://hdl.handle.net/1814/47545> accessed 5/7/2021.
76 In terms of computing power and electricity.
77 A mining pool is the pooling of resources by miners, who share their processing power and split the rewards accordingly.
78 D. Conte de Leon. *et al.*, 'Blockchain: Properties and Misconceptions' (2017) 11(3) Asia Pacific Journal of Innovation and Entrepreneurship, 286, 294-295.
79 Indeed, participants of mining pools increase their probability of winning the competition and get rewards. See Finck (n 10) 21.
80 Eenmaa-Dimitrieva, Schmidt-Kessen (n 75) 13.
81 Given that the system does not belong to anyone, there is a need to incentivise people to maintain and update it.
82 Hileman, Rauchs (n 11) 27-29.
83 For instance, OpenBazaar (<https://openbazaar.org>) is a blockchain-based decentralised marketplace for peer-to-peer e-commerce, both for private users and businesses. Anyone can use the platform anonymously and there are no restrictions on the object of the trade. Participants can transact only by running a node where to install the application.
84 As an example, Fizzy (n 50) is an initiative by the insurance firm AXA that makes use of the Ethereum platform for registration of smart contracts that keep track of flight status and provide automatic compensation in case of delays or cancellation. The users conclude the insurance contract by getting access to a dedicated website. Users do not run a node, but they can see the address of the smart contracts and the transactions using a blockchain browser like Etherscan.

posed to consumers. Secondly, because permissioned blockchains are closed ecosystems, thus considered safer by businesses when dealing with their affairs.[85]

iv. Permissioned blockchain/application users

This scenario can be typical of B2C relations. A business may create a permissioned blockchain to offer smart contracting services to end-users that do not run any node. This case differs from scenario 2 because of the presence of a permissioned (instead of permissionless) blockchain as the back-end of the business.[86]

Scenario 3 does not involve consumers, so it is not of any interest in this study. As regards the remaining scenarios, it appears evident that scenario 4 is an example of centralised governance of the blockchain at the hardware and software level. The blockchain application belongs to the business that uses it as back-end for its services. Hence, contract performance is under its control, with no further advantages for consumers.

Nonetheless, even in scenario 1 and 2 there can be a centralised control over the performance of the contract by the business. The latter does not depend on the centralised governance of the application, but rather from the subject matter of the contractual obligation.

As explained in section V., blockchain is a closed system. So, when contract execution is only possible by linking the smart contract to the off-chain world, both in input and in output, one might argue that the performance of the contract comes back under the control of the obliged party (the business) in which the aggrieved party has to trust (the consumer). Therefore, the consumer has to trust that the business feeds the smart contract with correct inputs and puts in place the necessary operations that have to follow the outputs of the smart contract.

VII. Another Case of (Indirect) Control on the Performance of Blockchain-Based Smart Legal Contracts

Until now, the present analysis has produced two main results. The first is that blockchain-based smart contracts are not breach-less contracts. The second is that, despite the blockchain, the business can still influence the performance of the contract. In both cases, blockchain technology is not of further support for consumers to remedy a lack of trust in the counterparty.

Even admitting that the business cannot govern the performance of the contract, the consumer might suffer another kind of indirect control by the trader on the performance of the contract.

As affirmed in Section V., when the code of the smart contract does not behave according to the will of the parties, the contract is not rightly performed. But the point is how the parties determined their will. In this respect, one should refer to the modalities of contract conclusion. The abovementioned scenarios might be useful.

In scenario 1, the business enters a permissionless blockchain platform to encounter potential customers (such as OpenBazaar). The situation is similar to online marketplaces like Amazon or e-Bay. In scenario 2, the business uses a permissionless blockchain as back-end by holding a node and downloading the protocol software. The consumer does not take part to the blockchain and does not hold a node. In front of the consumer, it is like when a business offers its products or services online through a website or mobile application. In both situations, it is very likely that the business not only provides the code but also drafts the contract in the form of general terms and conditions to which the consumer can only adhere or not.[87] The different bargaining power between businesses and consumers can give rise to abuses at the expense of the consumer.

In this way, the business can *de facto* manage the performance of the contract, although indirectly, because the smart contract behaves according to the contractual conditions provided by the business. In this respect, the fact that the blockchain can prevent any kind of ex-post intervention on the smart contract becomes irrelevant. Blockchain technology is not of any support for consumers.

Instead, only traditional legal instruments can protect consumers. For example, Annex I(1)(i) of the Unfair Contract Terms Directive (Directive 1993/13/EC)[88] states that the consumer should have a 'real opportunity of becoming acquainted' with the terms 'before the conclusion of the contract', otherwise the term is considered unfair and does not bind the consumer. Moreover, the information requirements laid down in the Directive 2000/31/CE[89] on electronic commerce and the Directive 2011/83/EU on consumer rights[90] aim to ensure the awareness and comprehensibility of contract terms for the weakest party in online contracts. Both Directives stress the importance of transparency of such information.[91] In particular, Recital 39 of the Consumer Rights Directive states that 'it is important to ensure for distance contracts concluded through websites that the consumer is able to fully read and understand the main elements of the contract before placing the order'.

---

85 As rightly pointed out by Gatteschi, Lamberti, Demartini (n 58) 42, these kinds of blockchains 'have the advantage of lowering validation time and costs, as network nodes are known and trusted. Furthermore, as read rights can be controlled, they provide greater privacy. Finally, it must be underlined that in cases of emergency (e. g. hacker attacks, bugs) these two latter types of blockchains could be easily modified or reverted to a previous state by making all network nodes agree on a previous version of the blockchain'.
An example can be the Spunta project, promoted and coordinated by the Italian Banking Association (ABI), which aims to implement the blockchain in interbank reconciliation. Every node corresponds to one of the involved banks, the network participants. The interbank reconciliation procedure in Italy aims to reconcile the transaction flows that generate accounting entries in the mutual accounts of Italian banks, and at managing pending transactions. The process follows the rules of an interbank agreement created in 1978, revised in 1987 and further amended in the '90 s. This agreement was recently updated allowing the adoption of DLT for the entire sector from 1 March 2020. For more details, see I. Ferraro, 'La pazienza della blockchain' (2019) Press release English version 88 ff <https://bancaforte.it/articolo/un-e-book-sulla-pazienza-della-blockchain-RB97945k> accessed 5/7/2021.

86 To facilitate this parallel, it can be cited the Insurance Blockchain Sandbox (n 50), which is similar to Fizzy by Axa (the use of blockchain for smart travel insurance contracts) except for the type of blockchain adopted as back-end.

87 According to Davola and Pardolesi (n 6) 205, 'it is reasonable to expect that smart contracts might diffuse primarily in "take it or leave it" scenarios where costs are lower, such as in the case of standard forms'.

88 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29.

89 Information requirements are mandatory in B2C contracts.

90 Above, Section III.

91 Art. 10 of the Directive 2000/31/CE dictates that the information is given by the service provider 'clearly, comprehensibly and unambiguously'. Art. 6 of the Directive 2011/83/EU establishes that the provider shall provide the consumer with the information 'in a clear and comprehensible manner'.

VIII. Persisting Need of Ex-Post Remedies for Contract Enforcement and Suitability for the Blockchain Context

As shown from the above analysis, the mere adoption of blockchain-based smart contracts does not solve the problem of consumers' lack of trust in the counterparty in the performance of B2C contracts. It has been demonstrated that the blockchain does not lead to increase consumers' confidence in the right performance of the contract by the business. Attention must not be paid to the decentralised character of the technology, but on how the technology is built and used, on the subject matter of the obligation, and on the modality of contract conclusion.

Having ascertained this, consumers have no choice but to seek the *ex-post* enforcement of contracts. The section examines the applicability of present remedies for non-performance of the contract.

The task is easy when the cause of the non-performance of the contract can be found outside the blockchain. As noticed above,[92] when contract execution is only possible by linking the smart contract to the off-chain world, both in input and in output, the performance of the contract is not under the control of the blockchain but of the obliged party (the business), in which the aggrieved party (the consumer) has to trust. The consumer has to trust that the business feeds the smart contract with correct inputs and puts in place the necessary operations that have to follow the outputs of the smart contract. Therefore, the business could be deemed responsible in front of the consumer, which could take advantage of traditional remedies for non-performance.[93]

Instead, when the cause of the non-performance is inside the blockchain (for instance, the content of the code does not match with the will of the parties, or there are some malfunctions), further distinctions are necessary. Before that, however, it should be reminded that blockchain applications are multi-layered and combine various components.

To simplify, at the basis there is the protocol layer, which is the core software infrastructure of the blockchain. On top of it, one can build various applications (the application layer).[94] The smart contract is the code recorded on a blockchain infrastructure. The smart contract code plus other components (such as oracles and data sources) form the application. For instance, Fizzy by Axa represented the application layer, while Ethereum was the protocol upon which Fizzy resided. Fizzy consisted in a smart contract connected with the company FlighStats (that gave information on flight arrivals and departures) through an oracle.[95] As seen in Section V., each part can have some malfunctions and determine the breach of the contract.

Behind every layer or component there is a creator. So, saying that trust is in the code is a misleading expression. The code is not something to trust in, because it has not a legal personality.[96] It is argued that it should be more correct to say that 'trust is in the creators of the code' (i. e. of the various elements of the blockchain application).[97]

This considered, in order to find the liable party, a focus on the scenarios can help.

In scenario 4, the blockchain application belongs to the business that invested to set up the entire infrastructure (both hardware and software) and uses it as back-end for its services. As affirmed in Section VI., scenario 4 is an example of centralised governance of the blockchain at the hardware and software level. The creator of the various elements of the blockchain application could be the business itself, its internal staff or a third party previously engaged by the business.[98] In all cases, the performance of the contract is under the control of the business, so it is assumed that the business is responsible towards the consumer. Classical rules are applicable.

Scenarios 1 and 2 have decentralised governance. Thus, it is wondered who should be held responsible. Indeed, existing rules governing contractual liability have been conceived to induce the other party (as far as it is of interest here, the business) to perform. They would have no sense in presence of other liable subjects, and they should be replaced by new liability rules.

Scenario 2 is similar to scenario 4, except for the kind of blockchain (permissionless). The business did not invest to set up its own blockchain infrastructure (the protocol layer). To use the blockchain protocol, the business has downloaded and installed a software in its node.[99] Then, it has developed (internally or through third parties) the blockchain application (the application layer) that sits on top of the protocol layer. The consumer is extraneous to the blockchain. She has simply concluded a contract with the business. The blockchain-based smart contract is the mean that the business uses to automatically perform the contract. The consumer trusts that the business performs the contract. Every malfunction

92 Section VI.

93 The debtor could also be liable towards the consumer for her auxiliaries' acts (according to the rules on performance entrusted to another), and of third parties. In the latter case, if the debtor engaged the third party through a contract, she could exercise her right to regress against the third party.

94 See Hileman, Rauchs (n 11) 26.

95 The use of the past tense is because Axa terminated Fizzy at the end of 2019, after almost two years of experimentation. The project head Laurent Benichou declared that there is not sufficient market appetite for the product, despite its innovative nature. Axa also reported that the right distribution channels do not yet exist for Fizzy. It added, however, that it is going to continue to test parametric insurance products, taking advantage of the experience gained with this project (<https://coinrivet.com/axa-drops-ethereum-based-flight-insurance-platform/>). Nevertheless, it is one of the most cited examples of smart contract applications, and one of the first that was put into production.

96 An international juridical debate developed on the right qualification of the so called 'software agents' as agents or as mere tools that make actions in place of humans. The view that considered them as agents has been subjected to criticisms, primarily because they lack legal personality. See E. M. Weitzenboeck, 'Electronic Agents and the Formation of Contracts' (2001) 9(3) International Journal of Law and Information Technology 204; T. Allen, R. Widdison, 'Can Computers Make Contracts?' (1996) 9(1) Harvard Journal of Law & Technology 25; G. Finocchiaro, 'La conclusione del contratto telematico mediante I 'software agents': un falso problema giuridico?' (2002) 18(2) Contratto e impresa 500. The UNCITRAL has also clarified that 'while the expression "electronic agent" had been used for purposes of convenience, the analogy between an automated system and a sales agent was not entirely appropriate and that general principles of agency law (for example, principles involving limitation of liability as a result of the faulty behaviour of the agent) could not be used in connection with the operation of such systems. The Working Group reiterated its earlier understanding that, as a general principle, the person (whether a natural or legal one) on whose behalf a computer was programmed should ultimately be responsible for any message generated by the machine'. See United Nations Commission on International Trade Law, *Yearbook Volume XXXII: 2001* (United Nations 2003) 240.

97 According to Mik (n 56) 165 'the ability to trust the code implies the need to trust the person(s) who created the code'.

98 Singh and Michels talk about 'Blockchain-as-a-Service' (BaaS) offerings, i. e. service providers that offer and manage various components of a DLT infrastructure. See J. Singh, J. D. Michels, 'Blockchain as a Service', Queen Mary University of London, School of Law, Legal Studies Research Paper No. 269/2017, 4, available at <https://ssrn.com/abstract=3091223> accessed 5/7/2021.

99 The software is usually given under an open-source license and after having accepted its terms of use. So, the business concludes a software license agreement.

that can prejudice the performance of the contract is at the own risk of the business that chose to perform the contract through a blockchain-based smart contract.[100]

In scenario 1, the underlying blockchain is permissionless. Both businesses and consumers contributed to build the blockchain by running a node, on which they installed the blockchain protocol. As evidenced in Section VII., the business enters such a permissionless blockchain platform to encounter potential customers, like Amazon or e-Bay. The business might adopt a pre-existing blockchain-based smart contract application, including both the protocol and the application layer (such as OpenBazaar). Alternatively, the business might develop its own application on the protocol layer (such as Ethereum). In the first hypotheses, it concludes a software license agreement with a third party to use the application. In the second, it concludes a software license agreement to obtain the protocol layer; as concerns the application layer, it might develop it with its internal staff or by concluding a software development agreement with a third party. However, it is believed that even in such scenario the business can be considered responsible in case of non-performance of the contract because it decided to perform the contract through a blockchain-based smart contract. Then, if the non-performance of the contract has been caused by problems in the blockchain protocol or application, the business may turn to the third party that provided the protocol and/or the application.

On the latter point, it is usually asserted that nobody is responsible for malfunctions of the blockchain protocol because the blockchain is permissionless. In permissionless blockchains, the software of the platform is usually open source,[101] meaning that anyone can see the source code and propose improvements.[102] For this reason, terms of use usually declare that the system is decentralised, and that nobody is responsible in case of malfunctions.[103]

In reality, as Mik rightly notices, blockchain participants cannot change the code already in operation. Each node in the system has to follow the rules dictated by the protocol. Decisions on the algorithms are not up to network participants. Once they enter the system, their nodes download the software and execute that software. Instead, behind permissionless blockchains there are usually companies, foundations, or other similar entities that identify as the founders of blockchain projects and that are entitled to make software upgrades.[104] Other is to create an alternative blockchain and make it available to others to download, given that the software is open source. However, the fact remains that the business can be considered responsible towards the consumer. Consequently, it is believed that the consumer could resort to traditional remedies for non-performance.

IX. Conclusions

In summary, the analysis gave the following results.

First of all, as explained in Section V., breaching contracts is still possible even with the blockchain. Consumers are not relieved from starting disputes.

Moreover, the affirmation that the decentralised and immutable characters of the blockchain determine that the system is not under the party's control is not accurate. There is confusion about the meaning of the term 'decentralisation'. The fact that blockchain technology is decentralised does not imply that the governance of the technology is also decentralised. When the governance of the technology is centralised, it cannot be said that trust is in the code because there is still someone able to influence the performance of the contract. Furthermore, given that blockchains are closed systems, smart contracts themselves are insufficient to guarantee the performance of the contract. A correct execution depends on the inputs the smart contract receives and on the interactions in output with the off-chain world. Again, the performance of the contract may still depend on the business that can govern such 'in input' and 'in output' activities.

Finally, the smart contract executes according to the contractual provisions. Thus, to protect consumers it is of vital importance to ensure that they are conscious of the content of the contract, that the contract is not too much unbalanced in favour of the business, and does not include unfair clauses. If contractual conclusion is in the hands of the business, no matter that smart contracts are able to self-execute. The business can indirectly influence the performance of the contract.

It is believed that blockchain technology does not determine a shift from trust in the other party to trust in the code. The code is a human creation. Hence, such creators, or who engaged them, should be held liable for those malfunctions of the code that caused the breach of the contract. As shown in this work, consumers have still to trust in the business and traditional legal remedies for non-performance are applicable.

In the end, it results that blockchain technology cannot increase consumers' trust in e-commerce or enhance consumers' protection. It cannot be given regard to the technology itself, but how the technology is used. For this reason, the study has taken into consideration some hypothetical scenarios of use of blockchain-based smart contracts for the performance of B2C contracts.

---

100 For instance, the general conditions of the insurance contract Fizzy (<https://fizzy.axa/fr/static/media/conditionsgenerales.38af84e2.pdf>) state that the smart contract performs automatically, so the consumer has not to activate to receive the payment by the insurance company (Art. 6.1.1). However, Art. 6.2.1 allows the consumer to activate in case the automatic payment does not occur, and Art. 8.5.2 provides that if the insurance company disagrees with making the payment, the consumer can address her claim to a Mediator or start litigation against the company. Therefore, the general conditions admit the contractual liability of the insurance company.

101 Bacon *et al* (n 8) 21-22.

102 According to Mik (n 56) 177 n 61, this does not mean that everyone can change the code already in operation, but that can create an alternative protocol and make it available for others to download. Then, it is not sufficient to provide a new version of the software to create a new blockchain. Instead, miners, users, and nodes must adopt the resulting software and maintain the blockchain infrastructure.

103 E.g. OpenBazaar's terms of use (n 83) state that it is a network 'without any central organisation controlling the platform. This means you are responsible for your own activity on the network'.

104 Bacon *et al* (n 8) 21-22; For example, in Ethereum there is the Ethereum Foundation, whose Ethereum's founder Vitalik Buterin is one of the members (<https://docs.ethhub.io/ethereum-basics/ethereum-foundation/>); in OpenBazaar, there is the OB1 company (<https://ob1.io/about.html>). Software upgrades occur through so-called 'forks' that split the blockchain into two. It is usually distinguished between 'soft forks' and 'hard forks'. While in case of a soft fork clients can choose not to upgrade to the latest version and continue using the oldest, hard forks invalidate previously valid blocks and require all users to update. See Bashir (n 12) 274. Developers of permissionless blockchains usually do not work *pro-bono*. Indeed, they can profit from the fact that their tool is used by an increasing number of people. As observed by the European Union Blockchain Observatory and Forum (n 14) 18 'their profits often do not result from dividends or fees charged on transactions, but from an increase in the value of tokens financing the total or partial development of a business or from advisory services to a foundation which supports the development of the project. Core developers, as co-founders, often retain some tokens for themselves, so part of their profit depends on the success of the venture'.

If contracts are not breach-less, and the business can still govern their execution, both directly and indirectly, the aggrieved party has to resort to traditional remedies for non-performance. Solely relying on the code is not enough, both if the counterparty is another business or a consumer, with the same problems of waste of time and money, identification of the liable party and the applicable law and jurisdiction.

As happens without the blockchain, consumers might be unconscious of their rights or consider their enforcement too much expensive. *A fortiori*, present European rules for consumers' protection, which have been seen in Section III., can be applied.

Namely, the information requirements laid down in the Directive on electronic commerce and in the Consumer Rights Directive (plus that information that online platforms have to provide to European consumers on traders according to the Proposal for a Digital Services Act) can assist the consumer in effectively understanding the content of the contract. So, they could impede the execution of blockchain-based smart contracts that act too much in favour of the trader, thus allowing an indirect control of the trader over the performance of the contract even in presence of a blockchain. The Directive on Unfair Contract Terms goes in the same direction. Information requirements also facilitate the identification of the trader in case the consumer has to start a claim.

There are other special rules for consumers, such as the right of withdrawal of the Consumer Rights Directive, the rights of consumers with regard to the conformity of the goods, digital content or services to the contract, and remedies in case of defects dictated by the European Directives 770 and 771 of 2019, or the criteria of identification of the applicable law and jurisdiction set by the Bruxelles I-*bis* Regulation and the Rome I Regulation, which have been enlisted above (Section III.). These rules, combined with other instruments (for instance, the ODR platform created by the European Union) can boost consumers to enforce their contractual rights even when contract performance occurs through blockchain-based smart contracts.

In conclusion, it appears unlikely that blockchain technology can play the same role as existing rules for consumers' protection, or even replace them. However, it is not intended to underestimate the potential of blockchain-based smart contracts. Indeed, smart contracts and blockchain technology might help to cut costs and processing time of exchanged data by sharing a common, secure, and transparent ledger. As a matter of fact, they are being especially tested in those sectors that process huge amounts of data on a daily basis between various intermediaries that exchange such data. These activities are usually characterised by a high degree of inefficiency. Each intermediary's activities reside on their separate platforms, so they are prone to data duplication errors and determine limited transparency of the data processing workflow.

Instead, blockchain technology provides all the intermediaries with a common data layer. The latter bypasses the need for data reconciliation, reducing related times and costs, and potential mistakes. For example, the insurance industry has caught the opportunity of investing in blockchain-based solutions, as indicated in Section IV. There are other promising fields, such as financial agreements[105] and trade finance.[106] The final aim is to improve competitiveness and customer experience. For these reasons, blockchain-based smart contracts might allow more efficient and less expensive services for consumers. Hence, the application of consumer-oriented legal instruments reveals itself as fundamental to foster the development of blockchain-based smart contracts for the execution of B2C contracts. ■

105 In particular, smart financial instruments (e. g. stocks, bonds, options, etc.) are attracting the most attention. One representative initiative is R3 (<https://www.r3.com>), a bank consortium now transformed into an enterprise software firm to develop blockchain applications for financial services on Corda, an open-source blockchain platform, and Corda Enterprise, a commercial version of Corda for enterprise usage. Stock markets are also experimenting. For example, in 2015 NASDAQ launched the project 'Nasdaq Linq' to grant private companies the ability to manage and trade their stocks through blockchain technology (<http://ir.nasdaq.com/news-releases/news-release-details/nasdaq-launches-enterprise-wide-blockchain-technology-initiative>). The Swiss Exchange is building a fully integrated issuance, trading, settlement, and custody infrastructure for digital assets, named SIX Digital Exchange (<https://www.sdx.com/en/home.html>). Blockchain-based smart contracts might enhance the settlement and clearance of securities and derivatives. Some limitations affect post-trading activities: the presence of many intermediaries that increase costs and time needed for executing their tasks; limited transparency of the processing workflow because transaction data and logs of each intermediary's activities reside on their separate platforms that hinder the traceability of the life cycle of the security; limited interoperability of intermediaries' systems. Smart contracts incorporate the instructions to carry out the operations that concern securities (e. g. the purchase, the transfer of the security, or the execution of payment obligations). The execution of the operations is allowed for authorised external agents (such as the security's buyer, seller, or broker) according to the provisions of the smart contract code. Blockchain technology records the state changes of the smart contract securely and transparently. See De Filippi, Wright (n 9) 89-96; S. McJohn, I. McJohn, 'The Commercial Law of Bitcoin and Blockchain Transactions', Suffolk University Law School Legal Studies Research Paper 16-13, 22 November 2016, 10 <http://ssrn.com/abstract=2874463> accessed 5/7/2021; European Commission, Joint Research Centre, 'Blockchain now and tomorrow – assessing multidimensional impacts of distributed ledger technologies' (2019) 62-64 <https://ec.europa.eu/jrc/en/facts4eufuture/blockchain-now-and-tomorrow> accessed 5/7/2021.

106 The inefficiencies of trade finance are similar to those enlisted above: mainly, high level of intermediation and manual activity. Furthermore, buyers and sellers (often coming from different countries) do not trust each other: buyers want to be sure that their purchases arrive in good condition before making the payment; sellers want to be sure to receive the payment. For this reason, in long-distance sale contracts, banks issue letters of credit and parties conclude escrow agreements. With a letter of credit, the buyer's bank (which issues the letter) guarantees the payment to the seller upon the delivery of the goods. Escrow agreements are concluded between buyers and sellers that involve an escrow agent to hold the money until the specified conditions of the contract are met. Although these services reduce the counterparty's risk, the exchange of paper documents and the presence of different actors lengthen the entire process and enhance the risk of fraud. It is believed that blockchain and smart contracts can alleviate these pain points. In both cases, a smart contract can be programmed to automatically transfer the funds. Blockchain reduces time and costs and increases transparency because all parties have access to the transaction records by sharing a common ledger. The fact that letters of credit and escrow agreements are highly standardised contracts, whose conditions can be easily translated into code, enables the development of smart contracting platforms. As a matter of fact, there are plenty of projects. See European Union Blockchain Observatory and Forum, 'Blockchain in trade finance and supply chain' (thematic Report, 9 December 2019) <https://www.eublockchainforum.eu/sites/default/files/report_supply_chain_v1.pdf> accessed 5/7/2021.