Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2025, Vol. 134, pp. 160–173

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2025.134.13

Legal Challenges of Harmonizing Smart Contract Regulations within the European Union

Vytautas Vičius

PhD student of Vilnius University Law Faculty
https://ror.org/03nadee84
Department of Private Law
Saulėtekio 9 – I block, LT-10222 Vilnius, Lithuania
Phone. (+370) 5 236 6170
E-mail: vytautas.vicius@gmail.com

Legal Challenges of Harmonizing Smart Contract Regulations within the European Union

Vytautas Vičius

(Vilnius University (Lithuania))

This article evaluates the regulatory legal landscape of smart contracts within the EU and examines a few essential legal challenges related to the need to harmonize smart contract regulations across the EU. It starts with analysis of some legal and technical aspects of the smart contract term form and arrives at the conclusion that there is no universal and unified term that contains technical aspects of the smart contract. This creates legal uncertainty, as the currently existing legal frameworks in many EU member states are not equipped to address these characteristics of smart contracts.

Another issue of importance is the varied approaches to smart contract regulation across the EU member states. The paper reveals that, currently, there is a spectrum of regulatory strategies from pioneering to conservative, and identifies the main obstacles to regulatory harmonization within the EU. Without a common legal framework, a smart contract deemed valid and enforceable in one state may not be recognized in another member state.

Finally, the current EU legislation is not specifically designed for smart contracts. However, it impacts their regulation by addressing critical aspects of digital operations like data ownership, access and control. Thus, successful integration of smart contracts into the EU's regulatory environment will require a concerted effort to address these complex challenges.
Keywords: blockchain technology, smart contracts, contract law, regulation of smart contract, European Union Law.

Teisiniai iššūkiai derinant išmaniųjų sutarčių reglamentavimą Europos Sąjungoje

Vytautas Vičius

(Vilniaus universitetas (Lietuva))

Straipsnyje vertinamas išmaniųjų sutarčių teisinis reglamentavimas Europos Sąjungoje (ES) ir nagrinėjama keletas esminių teisinių problemų, susijusių su poreikiu suderinti jų reglamentavimą visoje ES. Straipsnis pradedamas išmaniosios sutarties sąvokos teisinių ir techninių aspektų analize. Straipsnyje prieinama prie išvados, kad nėra universalaus ir bendro išmaniosios sutarties apibrėžimo, kuris galėtų apimti techninius išmaniosios sutarties aspektus. Dėl to kyla teisinis neapibrėžtumas, nes daugelyje ES valstybių narių galiojančios teisinės sistemos nėra pritaikytos šioms išmaniųjų sutarčių savybėms.

Received: 09/01/2025. **Accepted:** 31/03/2025

Kita problema – skirtingas požiūris į išmaniųjų sutarčių reglamentavimą ES valstybėse narėse. Straipsnyje atskleidžiama, kad šiuo metu ES egzistuoja reguliavimo požiūrių spektras nuo novatoriškų iki konservatyvių, ir nurodomos pagrindinės kliūtys suderinti išmaniųjų sutarčių reguliavimą ES. Nesant bendros sistemos vienoje valstybėje narėje galiojančia ir vykdytina laikoma išmanioji sutartis gali būti nepripažįstama kitoje valstybėje narėje.

Be to, galiojantys ES teisės aktai nėra specialiai pritaikyti išmaniosioms sutartims, tačiau jie turi įtakos tokių sutarčių reguliavimui, nes šiuose teisės aktuose nagrinėjami tokie svarbūs skaitmeninių operacijų aspektai, kaip antai duomenų nuosavybė, prieiga ir kontrolė. Dabartiniuose ES teisės aktuose nėra aiškiai nustatyti su išmaniosiomis sutartimis susiję aspektai. Taigi, norint sėkmingai integruoti išmaniąsias sutartis į ES teisinę ir reguliavimo aplinką, reikės bendrų pastangų sprendžiant šiuos sudėtingus uždavinius.

Pagrindiniai žodžiai: blokų grandinės technologija, išmaniosios sutartys, sutarčių teisė, išmaniųjų sutarčių reglamentavimas, Europos Sąjungos teisė.

Introduction

Technology enthusiasts are expecting that, in the foreseeable future, new digital instruments will dramatically impact our daily behavior and will significantly facilitate the implementation of currently complex business or legal processes. One of the most promising innovations is smart contracts. There are various opinions that these automatically executed agreements written in the computer code may replace the classical contracts and significantly reduce a need for lawyers' involvement in the contract formation and execution process. Currently, the popularity of smart contracts is highly increasing. Based on various estimations, the value of smart contracts concluded in 2022–2023 reached more than USD 1.5 billion (Smart Contracts Market Size, Share..., 2024). Due to the increasing usage of the digital technologies (e.g., new financial instruments, Internet of Things), it is expected that these volumes will grow more than ten times until 2030 (Smart Contracts Market Size, Share... 2023; Smart Contracts Market Size ... 2023).

However, the practical problems experienced by early users show that the parties of smart contracts still need a possibility to defend their rights by applying the traditional legal measures. As well as the classical contracts, smart contracts may also be a subject of manipulation which could result in the infringement of the party's rights (The Challenges and Risks..., 2021). Usage of the digital technology may impose technical or human related security risks, e.g., hackers may change the smart contract code (How hackers stole $613 million..., 2021), or they may organize attacks with fake contracts (9 Most Common Smart Contract…, 2021). From these cases, it becomes clear that the reasons that gave rise to the traditional contract law have not disappeared, e.g., smart contracts may be subject to fraud, or a smart contract could be coded not completely in line with the parties' intent.

The need for a clear and unified legal framework within the European Union (EU) is also evident. Such a framework would not only provide legal certainty but could also promote innovation by creating a predictable environment for the development and deployment of smart contracts. However, the nature of smart contracts – automated, decentralized, and reliant on the blockchain technology – creates legal uncertainty, as the currently existing legal frameworks in many EU member states are not properly equipped to address these characteristics of smart contracts.

By using the analytical descriptive method, the comparative method, and the method of systematic analysis, this article delves into the dynamic legal landscape shaped by the blockchain technology and smart contracts within the EU and aims to examine a few essential legal challenges related to the need to harmonize smart contract regulations across the EU. This paper is divided in three parts. Analysis begins on the topic of the unclear legal status of smart contracts in the EU and the assessment of the smart contract term form in terms of the legal and technical aspects of this concept. Then, the

exploration of the varied approaches towards smart contract regulation across the EU member states is provided to reveal a spectrum of regulatory strategies from pioneering to cautious, and to identify the main obstacles to regulatory harmonization within the EU. The final part provides a review of the interaction between smart contracts and the currently existing EU legislation, such as the EU Data Act. The currently existing EU legislation may be not specifically designed for smart contracts, but it impacts their regulation nevertheless by addressing critical aspects of digital operations like data ownership, access, and control.

In recent years, legal scholars have increasingly turned their attention to various dimensions of smart contracts, including questions of enforceability, formation and consumer protection within the EU and its member states. Notable examples include Schrepel's (2021) study on "*Smart contracts and the digital single market" through a "law + technology" approach*" and Verstappen's (2023) publication examining legal agreements on smart contract platforms across multiple European private law systems. While these works present valuable insights into the broader legal landscape related to smart contracts, they do not specifically address the challenges of harmonizing the smart contract regulation within the EU. This paper seeks to fill the gap by exploring the legislative and regulatory hurdles arising from efforts to unify the smart contract rules across the EU member states, thus contributing to the ongoing scholarly debate in this rapidly evolving field.

1. Unclear Legal Status of Smart Contracts

Currently, there is no universally accepted term of the smart contracts, and thus it is possible to find many different versions of this concept (Murray, 2019, p. 430). In fact, this term is often the subject of debate, both in the academic area and among legal practitioners. This definitional ambiguity raises essential questions about the legal status of smart contracts, particularly whether they should be classified as classical contracts under the existing legal frameworks, or if they represent a new distinct category of contracts.

Szabo defined smart contracts as a set of promises, specified in the digital form, including protocols within which the parties perform on these promises (Szabo, 1996). However, this definition is a merely technical one, and it does not indicate conditions helping to determine whether a smart contract can be qualified as a legally binding agreement. Indeed, it is widely agreed that smart contracts have technical (e.g., the blockchain technology) and legal (e.g., legislation, case law, soft law, etc.) dimensions (Schrepel, 2021, p. 13). Therefore, in order to develop a deeper understanding of the potential specific smart contract regulation aspects, it is necessary to look at the nature of these instruments.

It is believed that the smart contract offers its parties several important advantages over the traditional contracts. Unlike the traditional contracts that require manual execution or intervention by third parties, such as courts or arbitrators in the event of a breach, smart contracts aim to minimize or eliminate such interventions by automating performance. The use of Boolean algebra and conditional formalized clauses shall also increase the clarity between the parties and reduces the need for subsequent interpretation of contract provisions. The use of the blockchain technology and the automatic enforcement of contract terms increases trust between the parties and avoids potential disputes over the contract enforcement. Moreover, since the content of the contract is expressed in a programming language, such contracts can also be concluded by machines or computer programs, including *IoT* (Internet of Things).

The smart contract is technically understood as a piece of software code in a blockchain which ensures the self-enforcing and autonomous implementation of the terms and conditions stipulated by

the parties to the pre-agreement, applicable to the assets associated with the blockchain (Savelyev, 2016, p. 15). It is possible to identify several main technical features of a smart contract, which we shall discuss below.

Smart contracts are concluded and exist only in the electronic form (Catchlove, 2017, p. 7). All or part of the contract and its implementation conditions shall be drafted and implemented by using a software code. The contract terms and conditions shall be defined by incorporating them into the software code and using the principle "*if ..., then ...*" (Catchlove, 2017, p. 8; McKinney, 2018, p. 324). As specific programming language is used, transactions in a blockchain can technically be made by machines endowed with the capacity to understand such language (Werbach, 2017, p. 115). Smart contracts are executed automatically. Automatic execution is by far the most important feature of a smart contract. From the moment a smart contract has been entered into, its final execution no longer depends on the actions, approvals or the will of the parties (Savelyev, 2016, p. 15). When the conditions specified in the smart contract code are fulfilled, the application automatically performs a pre-programmed action (Werbach, 2017, p. 109).

Smart contracts are also immutable. A smart contract can only be revoked or modified under conditions that are specified/implied in the code itself. Smart contracts are performance-oriented. From the moment of conclusion, the conditions captured in the blockchain's programming code become binding on the parties, i.e., when the conditions specified in the smart contract code occur, the program executes a pre-programmed action (Werbach, 2017, p. 109).

The legal definition and qualification of smart contracts raises many questions for legal researchers and practitioners. Enthusiasts of new technology contracts argue that the blockchain on which smart contracts are based can operate independently, and that it cannot be affected by the traditional legal instruments; therefore, the partisans of smart contracts state that 'code is law', or even that the code is above law. It is also argued that there is no conceptual difference, except perhaps in the level of precision, between an agreement that establishes procedures to manage performance and an algorithm. In other words, since an algorithm is simply a set of rules made up of a set of outputs and inputs, an agreement can be understood as an algorithm specifying the rights and obligations of different parties. Therefore, even a computer algorithm (including a smart contract) can be used as a contract, since algorithms and contracts can be functionally equivalent.

However, basically, a binding agreement between the parties may exist only if there is a legal system that may enforce it. Based on the Hobbesian principles, a contract would be not void if there is a common power set over both parties, with the right and force sufficient to compel performance (Verstappen, 2023, p. 83). Whilst the point that smart contracts exist in a parallel universe, disconnected from the law, stays true to the ideological foundations of the 'cypherpunk' movement, legally speaking, this statement is incomplete. Even if one were to program human relationships, the legal framework remains relevant for the enforcement of the rights and obligations of the parties.

Some legal scholars argue that smart contracts are not contracts in the legal sense of the word. Guggenberger states that the contract is a legal construct that is based on offer and acceptance, the content of which is decided by considering all relevant facts and circumstances of a particular case whereas a smart contract indicates a simple computer programme (Guggenberger, 2020, p. 4). It is indicated that a smart contract may not be the agreement itself even though it is possible for a computer programme to represent an agreement or a part of it.

Indeed, smart contracts test the classical approaches to the formation, performance, and enforcement of contracts. Traditionally, the laws of the EU member states required an offer, an acceptance, a consideration, and an intention to create legal relations between parties (Verstappen, 2023, p. 195), see,

for example, Article 6:213 (1) BW: "*A contract <...> is a multilateral legal act, whereby one or more parties undertake an obligation as against one or more others*." In smart contracts, these elements may well be represented in the code, but it is the absence of any human readable language along with the automated nature that complicates the determination of the parties' intentions and the interpretation of the contractual terms. As De Filippi argued, the code itself becomes the law governing the parties' relations, thus potentially bypassing the traditional legal frameworks (De Filippi, 2018, p. 12).

It is essential to understand that smart contracts are not uniform due to their nature. Therefore, regulators (ELI Principles…, 2023) and legal scholars identify four types of smart contracts (Filatova, 2020, p. 225). Smart contracts may be a simple software code which does not imply any legally binding agreement. In this case, it can be considered as a technical transaction, e.g., transfer of data. Furthermore, a smart contract can be a means of enforcing a legal agreement. In this case, the legal agreement is indicated and exists in the traditional contract and is used as an ancillary means of the execution of the legal contract.

A smart contract may also be a legally binding contract. In this case, the legally binding expression of the parties' will, e.g., an offer or acceptance, or the legal agreement itself, is embedded in the software code of the smart contract. Finally, a smart contract may be linked to the legal agreement, and therefore it exists simultaneously on and off-chain. In this case, the agreement of the parties should determine how such a contract should be treated, i.e., as on or off-chain.

Considering the technical aspects of smart contracts and the variety of their types, their users may be unsure whether the concluded contract is valid even though the parties clearly intend to have legally binding consequences. For example, smart contracts often operate without the need for human interpretation or discretion that could challenge their compatibility with the traditional legal doctrines such as fairness, unconscionability, or good faith. Additionally, the self-executing nature of smart contracts raises concerns about the enforceability of such agreements in situations where unforeseen circumstances arise, or where one party claims that they were coerced, misled, or lacked the capacity to enter into the agreement. The lack of a standardized term in this case leads to varied interpretations of whatever constitutes a smart contract. This inconsistency presents barriers for the development of uniform legal principles and can result in uneven legal protections and obligations for the parties across different jurisdictions.

Therefore, for smart contracts to be properly recognized in the EU legal system, there ought to be a way in which immutability can be addressed. The issue of not having the option to reverse a transaction renders some solutions useless and may lead to infringement of the rights of at least one party of the agreement. Additionally, smart contracts ought to allow for some form of adjudication, whether through a system of courts, or else through arbitration that needs to be programmed into the smart contract in advance (Verstappen, 2023, p. 83). However, the EU and national member states legislators may lack technical expertise that is needed to predict how these measures would be implemented in practice. The technical features of smart contracts, such as immutability and lack of the unified smart contract term, may also cause issues related to the enforcement of the rights and the obligations of the parties. The EU and its national courts may struggle with interpreting and enforcing smart contracts due to their technical nature and the absence of clear legal guidelines. This can lead to unpredictable outcomes in disputes and undermine confidence in the use of smart contracts.

The lack of uniformed smart contract term may also result to inconsistent legal recognition across the EU member states. Without a common definition, member states may establish different approaches in recognizing smart contracts as legally binding. Some jurisdictions might fully accept smart contracts as enforceable agreements, while others may ignore all or a part of their legal consequences, thus causing

a fragmentation in legal recognition within the EU (see Section 3 of this Article). Due to these differences, it could be problematic for the member states to agree on the respective harmonized EU rules.

It is also evident that the legal uncertainty surrounding smart contracts poses a significant challenge to their harmonization within the EU. The lack of a standardized legal definition and the absence of a comprehensive regulatory framework across the EU contributes to an environment of unpredictability and risk for businesses and individuals engaging in smart contracts. This uncertainty is not merely academic. It has practical implications for the harmonization of laws across the member states, potentially undermining the uniformity of the internal market and the enforceability of smart contracts across borders. Ultimately, the key challenge for legal scholars and policymakers is to determine how to balance the potential benefits of smart contracts, such as an increased efficiency and reduced transaction costs, with the need to ensure fairness, accountability, and enforceability in an increasingly automated world.

2. Divergent National Approaches

The contract regulation in the EU is influenced by various legal traditions of different EU member states. The EU is composed of countries that have both *civil law* and *common law* systems. Each of these systems has its own approach towards the treatment of the contracts and their legal interpretation. Civil law countries, such as Germany and France, rely on codified statutes and legal codes. Whereas, common law countries, such as Ireland or Malta, operate based on judicial precedents and case law (Hesselink, 2006, p. 75). There are also some countries in the EU such as Malta or Estonia that seek to attract businesses and therefore intend to be the technological and regulatory hubs within the EU for smart contract developers and users. These fundamental differences in the legal philosophy and technological approach create obstacles to the harmonization of the smart contracts regulation due to the mere fact that whatever may be acceptable in one system may not be easily transposed to another.

Germany's legal tradition is rooted in civil law with a focus on detailed legal codes that govern contractual obligations. Currently, there is no targeted German legislation specifically regulating smart contracts. Instead, it views smart contracts against the backdrop of its existing contract law, primarily the German Civil Code (*Bürgerliches Gesetzbuch*). The German legal doctrine generally holds the view that it could incorporate smart contracts into its already existing legal concepts as long as they meet the required foundation for a contract forming act, including offer and acceptance or mutual will. This kind of agreement should have evidential value before German courts (Woebbeking, 2019, p. 111). This reliance on the existing law underlines the flexibility of the German contract law. However, it may provide uncertainties in applying traditional concepts to technology-related and complex agreements such as the conclusion, interpretation and enforcement of smart contracts. Novel technologies also became a subject of German national institutions, for example, Germany's financial regulator (BaFin) has published guidance on cryptocurrencies and the blockchain technology. Even though these guidelines do not indicate any specific aspects regarding the regulation of smart contracts, it shows that Germany has intentions to develop a framework for new technologies.

The legal system of France also follows a civil law tradition which emphasizes formalities in contract law. The French Code Civil requires contracts to be clearly expressed, which can pose challenges for smart contracts written in code. While the French Law permits the use of electronic contracts under Article 1366 of the French Code Civil, it is less clear how smart contracts that are self-executing pieces of code meet the requirements for the contractual consent of both parties and clarity. As a result, smart contracts face potential legal uncertainty, particularly in consumer contracts where protection regulation is more stringent.

However, the regulation of the innovative technologies related to smart contracts is developing in France. The PACTE Law has introduced measures aimed at facilitating the use of the blockchain technology in the financial sector. This law recognizes the blockchain technology. However, it does not provide comprehensive regulations for the execution and treatment of smart contracts. Although there is no specific legislation on smart contracts in France, these steps of new regulation are indicative of the direction of their legal recognition and integration into the existing legal system.

Meanwhile, Italy has been more proactive from a legislative perspective related to smart contracts. In 2019, the Italian government converted Decree-Law No. 135 of 14 December 2018 into law. This decree legally defined DLTs and adopted a legal definition to smart contracts[1]. It provides that smart contracts meet the form in writing requirement when the identity of the parties is certified by electronic means according to the standards set by the Agency for Digital Italy. Smart contracts shall satisfy the requirement of the written form upon the digital identification of the contracting parties. Although the Italian legal system embraces the principle of freedom of contract forms, many transactions require the written form for their validity or probation. The exact conditions for smart contracts qualifying the requirement of the written form give legal validity to the dynamic aspect of blockchain-related transactions.

Malta has positioned itself as one of the leading countries in the world in regulating blockchain and smart contracts. To this end, Malta has enacted three key laws, i.e., 1) Malta Digital Innovation Authority Act; 2) Innovative Technology Arrangements and Services Act; and 3) Virtual Financial Assets Act. These laws provide a regulatory regime for blockchain technologies and smart contracts. For example, the Innovative Technology Arrangements and Services Act includes the possibility for the certification of technology arrangements such as smart contracts to ensure that they meet certain standards[2]. Based on the Virtual Financial Assets Act, the smart contract means a form of an innovative technology arrangement consisting of the following aspects: i) a computer protocol; ii) an agreement concluded wholly or partly in an electronic form; iii) it is automatable and enforceable by execution of a computer code (although some parts may require human input and control); iv) it is enforceable by ordinary legal methods or by a mixture of both. Malta's regulatory framework stems from its common law tradition, which allows for a more flexible interpretation of contractual agreements. With the pursuit of balance between innovation and protection, Malta is trying to position itself as one of the most blockchain-friendly jurisdictions. However, this position sets Malta apart from other EU member states that often take a more cautious approach to the smart contract legality.

No special legislation that regulates smart contracts has been adopted in the Netherlands so far. The Research and Documentation Centre of the Dutch Ministry of Justice and Security published a report on DLTs and smart contracts. Therefore, smart contracts could be interpreted based on the general principles of contracts indicated in the Dutch Civil Code. Contrary to the French and German law, the Dutch Civil Code provides little to no guidance on how contracts should be interpreted according to the Dutch law (Verstappen, 2023, p. 121). The report on DLTs and smart contracts considers that the Dutch contract law applies to smart contracts, and, therefore, an adaptation of the regulatory framework seems unnecessary. Smart contracts are, in practice, regarded as agreements, which may be legally

[1] Article 8-ter(2) defines smart contracts as "*computer programs that operate on distributed registers-based technologies and whose execution automatically binds two or more parties according to the effects predefined by said parties*".

[2] In order to ensure the protection of interests of the parties and to avoid illicit activities, Malta Digital Innovation Authority (MDIA) may certify the specific smart contract by evaluating the legality, integrity, transparency and accountability requirements. This shall ensure that a smart contract is legally valid and understandable for its users.

binding provided that they meet the basic contract requirements. However, in the absence of special rules, a lot of uncertainty especially regarding protection and liability, may still arise.

Estonia is known for a wide-ranging modern digital infrastructure and for multiple e-governance initiatives (e.g., the e-residency programme). Despite the progressive approach and the interest in the blockchain technology, no specific legislation related to smart contracts has been adopted yet. Estonia's contract law, similar to other civil law countries, may be flexible enough to recognize digital contracts, including smart contracts. The Estonian law already applies many basic contract principles, and smart contracts may be legally binding if they can meet the provisions of the Law of Obligations Act. While Estonia's digital-friendly environment might allow easy adoption of smart contracts under the national contract law, a lack of specific legal provisions may result in some uncertainties for smart contract developers, users and businesses.

The aforementioned variations in different EU member states create a fragmented regulatory landscape which complicates efforts to develop a harmonized EU framework for smart contracts. Without a common legal framework, a smart contract deemed valid and enforceable in one member state may not be recognized in another member state. This lack of uniformity could undermine the EU's internal market, where the free movement of goods, services, capital and people relies on a consistent legal environment across the EU member states.

This makes a harmonized approach to regulating smart contracts within the EU difficult. First, non-uniformity creates legal uncertainty regarding cross-border transactions. For the parties, difficulty may arise in determining which national laws apply, how to deal with disputes, and whether their smart contracts will be considered valid and enforceable in another EU member state jurisdiction. This aspect is important taking into consideration that, in the majority of smart contracts, the applicable law in not included in the code. The second consequence is that inconsistent regulatory provisions impede the advancement of standardized practices and technological interoperability. This may affect the developers and companies in their attempt to draft universal smart contracts that can comply with numerous legal systems. As a result, it may inhibit innovation and hamper market development. Thirdly, regulatory arbitrage is involved when businesses will opt to operate in jurisdictions where the respective regulations are the most lenient. This could also undermine the cohesion of the internal market of the EU. Therefore, harmonization of the EU laws regulating the smart contracts would be beneficial, and potentially would help to avoid these disadvantages.

The discussed different national approaches disclose some complexities in regulating smart contracts within the EU. Such divergences may be noticed from the degree to which legislation has been adopted, the interpretation of the current legal framework and the policy priorities in the EU member states. From the analysis of regulations of different member states, it is clear that different legal traditions, contracting rules and technological priorities of specific member states shape the different national models of smart contract regulation throughout the EU. Some countries, such as Italy and Malta, have legislated smart contracts specifically with the aim of creating legal certainty so that to increase legal and technical innovation. Whereas, other EU member states are trying to view smart contracts through the lens of the traditional existing national contract law principles (e.g., Germany, the Netherlands, Estonia). This may raise some smart contract application issues as they technically require automation, shall be immune to changes and shall be executed in a distributed manner. These different national views on smart contract regulation raise significant questions that may hinder the adoption of harmonized EU legislation of smart contracts. However, the positive aspect is that all the presently analyzed EU member states in principle recognize that smart contracts may give rise to rights and obligations on their parties, and that smart contracts could be, at least theoretically, executed in the EU member states.

3. Specificities of Regulation in EU

The specifics of the EU legislation mechanism are another major problem in attempting to homogeneously regulate smart contracts in the EU. The EU has limited competencies to fully regulate specific matters and establish a unified legislation (e.g., regarding competition, personal data protection, consumer protection). There is no direct power, either, to coordinate the legislation regulating classical contracts or smart contracts within the EU. Thus, the regulation of smart contracts currently remains outside the scope of the EU legislation (Benson, 2024, p. 55). This means that each member state may have its own legal framework governing contract-related matters, including their formation, enforceability, and interpretation. Furthermore, a part of legal challenges also lies in the existing the EU legislation that may also partly regulate smart contract-related aspects, and the currently applicable rules may be contrary to the essence of smart contracts. This may cause uncertainty regarding the application of smart contracts and their possible enforcement by the state.

Currently, there is no EU legislation which would particularly address smart contracts, and only general EU rules may apply indirectly to smart contracts. There are EU directives and regulations that deal with electronic commerce, digital signatures, data protection and data governance that may affect the treatment of smart contracts in terms of legal validity and legal enforceability in the EU member states.

One of the most important aspects in the conclusion of a smart contract is the identification of the parties of the agreement. As smart contracts are concluded by using an electronic code, it is essential for the parties to be sure that the obligations are assumed by the competent person. This shall also be done via the approved electronic process or means. The eIDAS Regulation[3] establishes a regulatory framework for electronic signatures. This regulation sets legal equivalence to electronic signatures and handwritten ones. However, the application of the eIDAS Regulation for smart contracts is less clear. Smart contracts that are self-executing and concluded on blockchain platforms raise uncertainty over how electronic identification and the associated trust services apply when the parties do not apply the traditional authentication processes ensured by trusted service providers. This may cause problems to the smart contract users who intend to prove the validity of that contract as, based on the general contracts principle, the parties of the contract shall be identified. This aspect is extremely important if the distributed ledger enables anonymous or pseudonymous transactions. However, the current provisions of eIDAS do not provide the clear guidance position regarding this issue.

Another relevant legislation is GDPR[4] which enforces obligations on processing personal data[5]. Smart contracts are due to the technological specifics of the public blockchain smart contracts immutable. This may contradict the provision set in GDPR which require the removal or alteration of personal data, e.g., right to be forgotten, the right to rectification or the principle of data minimization. The data (including personal data) is written in respective blocks of the chain, and, basically, this data of the certain block cannot be changed. The next block may only amend the basic information of the previous block. Furthermore, as smart contracts are decentralized, this means that the personal data that is recorded in the blocks of a blockchain may be processed in the network from anywhere in the

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[5] Personal data is any information that relates to an identified or identifiable living individual. This term is understood systematically, i.e., different pieces of information, which, collected together, may lead to the identification of a particular person, also constitute personal data.

world. However, GDPR stipulates that personal data may be transferred from the EU only if specific conditions apply and if the security of the personal data processing is ensured. This may cause discrepancies with cross-border personal data transfer requirements. In addition, some other personal data protection principles (security, purpose limitation) that are worthy of study may also raise the regulatory non-compliance of smart contracts. Therefore, in order to ensure legal certainty from the personal date perspective, the provisions of GDPR shall also be reviewed and amended. The EU has recently adopted the Data Act[6] which serves the objective of ensuring a harmonized framework within the EU for data access and use. The Data Act entered into force on 11 January 2024. The primary goal of the Data Act is to ensure fairness in the allocation of the value of data amongst the actors in the data economy. It clarifies who can use what data and under which conditions.

The Data Act sets that a smart contract is a "*computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering*"[7]. This means that the performance of the agreement shall occur fully or partly automatically once the parties have agreed on the use of the smart contract. This notion is technologically neutral, and it does not need to be based on blockchain solutions. Therefore, any technology that complies with the requirements of the Data Act and that could be used for the automatic execution of a data-sharing agreement could be recognized as a smart contract. Furthermore, among the rules which are laid down in relation to smart contracts used for data-sharing agreements, Article 30 of the Data Act requires that smart contracts used for data sharing would be robust, providing appropriate access control and allowing security termination and interruption.

However, the provisions on smart contracts in the Data Act have been criticized as being insufficient and not extensive enough to solve the broader legal application problems that arise with smart contracts.

The regulation narrowly addresses only smart contracts used for data sharing (making data available), without mentioning any other applications of smart contracts (e.g., the smart contract as an agreement). This means that many different agreements that are in use in the industry with a purpose different from "*making data available*" may not be in-scope of the Data Act. That is a narrow scope which does not give sense of legal certainty and assurance to users of smart contracts within the EU and places the EU at a competitive disadvantage *vis-à-vis* others, especially large markets with comprehensive regulations. One of the key issues of this regulation in the Data Act is the need for consensus among the member states on what these standards should entail. Different countries have different legal traditions and regulatory approaches, which can make it difficult to agree on a single set of standards. For example, while some member states may prioritize consumer protection and data privacy in their approach to smart contracts, others may focus more on promoting innovation and reducing regulatory burdens (Raskin, 2017, p. 319).

The further complexity of the requirements of the Data Act is that they might contradict with the established functionality of smart contracts. For example, it can be difficult to expect smart contracts that are designed to be immutable and self-executing, to provide for mechanisms of safe termination and interruption. These features are hard to combine within one entity or person that is responsible for the proper performance of a smart contract. Therefore, it is not fully clear how the compliance with the Data Act regulation can be combined without compromising technological advantages. Unsurprisingly, the market participants have strong concerns that these provisions of the Data Act may limit the key features of a smart contracts, and, therefore, they will not be widely used in the EU.

[6] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[7] Article 2(39) of the Data Act.

In addition to the Data Act, the EU has also adopted a Regulation on Markets in Crypto-assets (MiCA)[8] that came into force on 9 June 2023. The MiCA regulation intends to create a harmonized regime for crypto-assets that extends to some issues involving smart contracts. MiCA does not contain any provisions that directly regulate smart contracts. For example, the MiCA regulation does not set forth that smart contracts providing for the automated exchange of one crypto-asset for another would be specifically regulated under this regulation. However, the adoption of the MiCA regulation shows the general position and a clear intention to establish a legal framework for a smart contract regulatory framework within the EU.

Considering the provided analysis of the current provisions of the EU law, the EU legislation regarding smart contracts is fragmentary, including the narrow provisions of the Data Act dealing with some aspects of smart contracts. Therefore, there is a significant legal barrier to harmonization in this respect stemming from the issue that EU directives and regulations may be interpreted differently at the national level. Due to the narrow scope of the Data Act, it does little to address the wider legal application issues with smart contracts. This undoubtedly does not constitute sufficient user assurance in the EU or a competitive advantage *vis-à-vis* other major markets.

The absence of extensive EU legislation on smart contracts leads to legal fragmentation whereby the different EU member states can interpret and apply their national and currently existing EU legislation variously. That is the main reason influencing the fact that treatment of smart contracts under different jurisdictions within the EU could be inconsistent. While the respective smart contract could be regarded as legally valid based on the national contracts law in some EU member states, the lack of a legislative background could lead to non-recognition of the same smart contract in other jurisdictions.

The main issue manifested through this fragmentation is that it introduces several legal challenges to harmonization. First, the differing manifestations of national laws create a level of uncertainty for the parties entering a cross-border transaction using smart contracts. It is problematic to legally define issues such as which law governs a respective contract, how their disputes would be resolved, and whether the contract would be enforceable or not. These aspects are fundamentally important when we have smart contracts that are concluded only in the code, i.e., when no additional provisions are indicated in supporting or supplementing documents. Second, the lack of harmonized regulation is a real obstacle to achieving standardized practices and technical interoperability. Without unified standards in the legal framework, development of smart contracts to cater to diverse jurisdictions within the EU is very challenging for developers and businesses. The consequence may be the damping of innovation and limitation of the scalability of applications that are made from and for smart contracts. Third, the different interpretation of the existing EU legislation undoubtedly tends to create regulatory arbitrage. For example, companies, developers or users may leverage a smart contract's and a blockchain's decentralized and cross-border nature to operate in regulatory environments that are more favorable to their objectives. Therefore, the parties involved may select jurisdictions with more lenient regulations, which undermines the integrity of the internal market and creates an uneven playing field amongst the EU member states.

These problems have been the cause of arguments calling for the EU to propose a comprehensive legal framework for smart contracts. The European Parliament in its resolution on *Distributed Ledger Technologies* (DLTs) and blockchain emphasized that legal certainty needs to be provided, and invited

[8] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA regulation).

the European Commission to consider whether any legislation could be necessary. However, the current fragmented EU legislation which, in some cases, contradicts the nature of smart contracts raises obstacles against the adoption of a uniform regulation of smart contracts. Therefore, it would be required to review and amend some fundamental current EU legislation (e.g., GDPR, consumer protection legislation). Furthermore, the EU and some member states have adopted a conservative approach on the change of legislation, and it is hard to reach an agreement for all member states on some essential changes that need to be implemented so that to introduce the unified legislation within the EU. The common agreement between the member states is essential in order that the unified legislation in the EU should be adopted.

Conclusion

1. Integration and regulation of smart contracts within the EU presents complex legal challenges that demand a comprehensive approach. Firstly, the absence of a universally accepted legal definition of smart contracts across the EU member states complicates efforts to harmonize their regulation. The divergent national approaches create a fragmented legal regulatory landscape, undermining the potential for a cohesive internal market. This also raises significant questions about the recognition and enforceability of smart contracts in different EU member states. Addressing this issue requires the EU to develop a uniform definition of a smart contract that can be integrated into the existing legal framework. This definition shall also reflect the unique characteristics of smart contracts such as automatic execution, immutability, etc. Secondly, the different legal traditions of the EU member states contracting rules and technological priorities set the different national models of smart contract regulation throughout the EU. This raises some significant smart contract application issues as they would technically require automation, shall be immune to changes, and shall be executed in a distributed manner. These different national views on the smart contract regulation raises fundamental questions that may interfere with the adoption of the harmonized EU legislation defining smart contracts. Finally, the EU legislation problems have been the cause of arguments calling for the EU to propose a comprehensive legal framework for smart contracts, e.g. even the European Parliament emphasizes that legal certainty needs to be ensured for the market participants. However, the fragmented current EU legislation which, in some cases, contradicts with the nature of the smart contracts, raises obstacles against the adoption of a uniform regulation of smart contracts. In order to reach the intended regulatory certainty, it would be required to review and amend some currently existing EU legislation (e.g., GDPR). Furthermore, the EU and some member states have adopted a conservative regulatory approach and this and this can be an obstacle to changing existing laws. Due to these aspects, it could be hard to introduce the unified legislation for smart contracts within the EU.
2. The successful integration of smart contracts into the EU's legal and regulatory environment will require a concerted effort to address these complex challenges. By developing clear definitions, creating harmonized legal frameworks, promoting interoperability and standardization and enhancing consumer protection and security, the EU can create a robust legal infrastructure that supports the growth and innovation of smart contracts while safeguarding the rights and interests of all stakeholders. This balanced approach will be essential for realizing the potential of smart contracts in establishing a more efficient, transparent and secure digital economy within the EU.

Bibliography

Legal Acts and European Commission's Communications

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*, L 257, 28 August 2014, pp. 73–114.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA regulation). *Official Journal of the European Union*, L 155, 2 June 2023, pp. 1–102.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union*, L 300, 14 December 2023, pp. 1–49.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *Official Journal of the European Union*, L 119, 4 May 2016, pp. 1–88.

R (eds) *German Civil Code – Volume I: Books 1-3 Article-by-Article Commentary*. C.H. Beck, München.

French Civil Code (Code Civil), Legifrance [online]. Available at: https://www.legifrance.gouv.fr [accessed on 22 August 2024].

Malta Digital Innovation Authority Act 2018, Government of Malta [online]. Available at: https://legislation.mt [accessed on 22 August 2024].

Innovative Technology Arrangements and Services Act 2018, Government of Malta [online]. Available at: https://legislation.mt [accessed on 22 August 2024].

Virtual Financial Assets Act 2018, Government of Malta [online]. Available at: https://legislation.mt [accessed on 22 August 2024].

Conversion Law of February 11, 2019, No. 12, Amending Decree-Law of December 14, 2018, No. 135 (Italy), Gazzetta Ufficiale [online]. Available at: https://www.gazzettaufficiale.it [accessed on 22 August 2024].

Plan d'Action pour la Croissance et la Transformation des Entreprises (PACTE) Law No. 2019-486 of 22 May 2019, Légifrance [online]. Available at: https://www.legifrance.gouv.fr [accessed on 22 August 2024].

Special literature

Benson, V., Adamyk, B., Chinnaswamy, A. *et al.* (2024). Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions. *Eur J Law Econ* 57, p. 37–61, https://doi.org/10.1007/s10657-024-09797-w.

Catchlove, P. (2017). *Smart Contracts: A New Era of Contract Use* [online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090226 [Accessed on 21 August 2024].

DiMatteo, L. A. (2019). Blockchain Technology and Digital Platforms. In: *The Cambridge Handbook of Smart Contracts.* Cambridge: Cambridge University Press.

Guggenberger, N. (2020). Teil 13.7-Smart Contracts, ICOs und Datenschutz. In: Hoeren. T., Sieber, U., Holznagel, B. (eds). *Handbuch Multimedia-recht*. C.H Beck, München.

Hesselink, M. W. (2006). *The Politics of a European Civil Code*. Kluwer Law International.

Micknney S. A., Landy R., Wilka R. (2018). *Smart contracts, blockchain, and the next frontier of transactional law*, 13 Wash. J. L. Tech. & Arts.

Raskin, M. (2017). The Law and Legality of Smart Contracts. 1 *Geo L Tech Rev* 305.

Savelyev, A (2016). *Contract Law 2.0: „Smart" contracts as the Beggining of the End of Classic Contract Law* [online]. Available at: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241* [Accessed on 22 August 2024].

Schrepel, T. (2021). *Smart contracts and the digital single market through the lens of a "law + technology" approach* [online]. Available at: https://digital-strategy.ec.europa.eu/en/library/smart-contracts-and-digital-single-market-through-lens-law-plus-technology-approach; [Accessed on 21 August 2024].

Szabo, N. (1996). *Smart contracts: building blocks for digital free markets*. Extropy 16:50–53 [online]. Available at: https://archive.org/details/extropy-16/page/54/mode/2up. [Accessed on 22 May 2024].

Verstappen, J. (2023). *Legal agreements on smart contract platforms in European systems of private law: Formation, interpretation, vitiation, and consumer protection in English, French, German, Dutch, and European Union contract law*. Doctor of Philosophy, Maastricht University, Maastricht.

Werbach, K., Cornell, N. (2017). Contracts Ex Machina. 67 *Duke Law Journal* 313.

Woebbeking, M. K. (2019). The Impact of Smart Contracts on Traditional Concepts of Contract Law. 10 *JIPITEC* 106, para 1.

Other sources

The Challenges and Risks of Smart Contracts [online]. Available at: https://www.icba.org/newsroom/blogs/main-street-matters/2021/11/12/the-challenges-and-risks-of-smart-contracts [accessed on 9 September 2024].

ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection [online]. Available at: https://www.europeanlawinstitute.eu/projects-publications/publications/eli-principles-on-blockchain-technology-smart-contracts-and-consumer-protection/ [accessed 22 August 2024].

Germany's financial regulator (BaFin) published guidance on cryptocurrencies and blockchain technology [online]. Available at: https://www.bafin.de/EN/Aufsicht/FinTech/Geschaeftsmodelle/DLT_Blockchain_Krypto/DLT_Blockchain_Krypto_node_en.html [accessed on 2 September 2024].

Explainer: How hackers stole and returned $600 mln in tokens from Poly Network [online]. Available at: https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/ [accessed on 23 August 2024].

Smart Contracts Market Size, Share, Growth Analysis, By Blockchain Type (Public, private and hybrid), By Enterprise size (Small and Medium Enterprises (SMEs) and Large Enterprises), By End-use (BFSI, Retail, Healthcare, Real Estate), By Region - Industry Forecast 2025-2032 [online]. Available at: https://www.skyquestt.com/report/smart-contracts-market [accessed on 19 August 2024].

Smart Contracts Market Size, Share, Trends, Growth 2030 [online]. Available at: https://www.zionmarketresearch.com/report/smart-contracts-market [accessed on 8 September 2024].

Smart Contracts Market Size, Share, & Trends Analysis Report By Platform, By Blockchain Type, By Contract Type, By Enterprise Size, By End-use (BFSI, Retail), By Region, And Segment Forecasts, 2023 – 2030 [online]. Available at: https://www.grandviewresearch.com/industry-analysis/smart-contracts-market-report [accessed on 8 September 2024].

9 Most Common Smart Contract Vulnerabilities [online]. Available at: https://blaize.tech/article-type/web3-security/9-most-common-smart-contract-vulnerabilities-found-by-blaize/ [accessed on 8 September 2024].

Vytautas Vičius is a PhD student at the Department of Private Law, Faculty of Law, Vilnius University. His field of research includes Contract Law, Technology Law and regulation of economic activities performed on a basis of blockchain technology. The title of the dissertation in progress: "Smart Contracts in the Context of Lithuanian Law".

Vytautas Vičius yra Vilniaus universiteto Teisės fakulteto Privatinės teisės katedros doktorantas. Pagrindinės jo mokslinių interesų ir tyrimų sritys: sutarčių teisė, technologijų teisė ir blokų grandinės technologijos pagrindu vykdomos ekonominės veiklos reguliavimas. Rengiamos disertacijos pavadinimas: „Išmaniosios sutartys Lietuvos sutarčių teisės kontekste".