UNIVERZITA MATEJA BELA
V BANSKEJ BYSTRICI

ZBORNÍK PRÍSPEVKOV
Z MEDZINÁRODNEJ ŠTUDENTSKEJ
VEDECKEJ KONFERENCIE

PRO-LEGAL Deň študentov práva a doktorandov 2026

2026

BELIANUM

Univerzita Mateja Bela v Banskej Bystrici
Právnická fakulta

Zborník príspevkov
z medzinárodnej študentskej vedeckej konferencie
PRO-LEGAL Deň študentov práva a doktorandov
2026

Recenzovaný zborník vedeckých príspevkov

Ľubica Saktorová
(eds.)

BELIANUM
Banská Bystrica
2026

Zostavovateľ (Editor) : JUDr. Ľubica Saktorová, PhD., LL.M., M.A.

Recenzenti (Reviewers) : doc. JUDr. Ivana Šošková, PhD., MBA
Mgr. Miroslava Dolíhalová, PhD.
JUDr. Peter Trajlinek, PhD.

Príspevky neprešli jazykovou korektúrou.
Za obsahovú a jazykovú stránku textu sú zodpovední autori publikovaných príspevkov.

ISBN 978-80-557-2337-2
EAN 9788055723372
https://doi.org/10.24040/2026.9788055723372

SMART CONTRACTS AS AN EMERGING FORM OF AGREEMENT: LEGAL NATURE AND REGULATORY PERSPECTIVES

VLASIUK YEVHEN*

Abstract

This research investigates the legal nature and regulatory prospects of smart contracts as a transformative form of agreement in the digital age. By analyzing the tension between autonomous blockchain protocols and traditional contract law doctrines, the paper explores whether the "code is law" principle can be harmonized with established judicial standards. The study identifies critical challenges such as jurisdictional ambiguity, the rigidity of immutable code, and the "oracle problem" in automated enforcement. Ultimately, the author advocates for a hybrid regulatory framework that balances technological efficiency with essential legal safeguards, ensuring that algorithmic execution remains subject to human-centered justice and accountability.

Keywords : *Smart contracts, Oracle, Blockchain technology.*

Introduction

The rapid evolution of the digital economy and the Fourth Industrial Revolution have necessitated a fundamental re-evaluation of traditional legal concepts. As global commerce increasingly shifts toward decentralized platforms, blockchain technology has emerged as a transformative force, introducing the concept of smart contracts. First proposed by Nick Szabo in the mid-1990s, smart contracts have evolved from theoretical constructs into practical tools that automate complex transactions without the need for traditional intermediaries.

The relevance of this research stems from the growing gap between rapid technological advancement and the relatively static nature of contract law. While software developers often operate under the radical doctrine of "Code is Law," legal scholars and practitioners face significant challenges in reconciling autonomous, self-executing algorithms with established civil law principles. The primary tension lies in the "immutability" of blockchain protocols, which provides unprecedented security but lacks the inherent flexibility of human-centered legal systems, such as the ability to modify or terminate agreements based on equity or unforeseen circumstances.

The purpose of this paper is to analyze the legal nature of smart contracts as an emerging form of agreement. It seeks to determine whether a smart contract should be classified as a standalone type of contract, a digital form of a traditional agreement, or merely a sophisticated

* Євген Павлович Власюкvlasiuk.yevhen@chnu.edu.ua 1st-year Master`s Student of the Faculty of Law, Yuriy Fedkovych Chernivtsi National University Scientific Advisor: Oksana Kiriiak PhD in Law, Associate Professor of the Department of Privat Law, Yuriy Fedkovych Chernivtsi National University Ukraine

mechanism for contractual performance. Furthermore, this research explores the regulatory perspectives within the international legal landscape, focusing on how jurisdictions can integrate these decentralized tools while ensuring consumer protection, accountability, and the rule of law.

Chapter I

In 1996, Nick Szabo was one of the first to propose the concept of smart contracts, describing them as follows: «Whether enforced by a government, or otherwise, the contract is the basic building block of a free market economy. Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it, encoded into common law. Algorithmic information theory suggests that such evolved structures are often prohibitively costly to recompute. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like property rights that make the modern free market work.

The success of the common law of contracts, combined with the high cost of replacing it, makes it worthwhile to both preserve and to make use of these principles where appropriate. Yet, the digital revolution is radically changing the kinds of relationships we can have. What parts of our hard-won legal tradition will still be valuable in the cyberspace era? What is the best way to apply these common law principles to the design of our on-line relationships? Computers make possible the running of algorithms heretofore prohibitively costly, and networks the quicker transmission of larger and more sophsiticated messages. Furthermore, computer scientists and cryptographers have recently discovered many new and quite interesting algorithms. Combining these messages and algorithms makes possible a wide variety of new protocols. New institutions, and new ways to formalize the relationships that make up these institutions, are now made possible by the digital revolution. I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied. A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises» (Szabo, 1996).

Apparently, today everything related to the word «smart» is perceived as something made by artificial intelligence, but in the case of smart contracts, this word is used because this type of contract is executed automatically, under certain conditions, and does not require intermediaries.

«Many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.

Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.»- Nick Szabo (Szabo, 1997). "*The most fundamental shift that smart contracts introduce is the movement of legal enforcement from ex post to ex ante. In a traditional legal system, a party who believes the contract has been breached must seek a remedy after the fact, usually through a court. A smart contract, by contrast, is designed to ensure that the promised performance occurs automatically. The enforcement is built into the initiation of the relationship. This effectively removes the possibility of a breach in the traditional sense, as the code executes according to its terms regardless of the subsequent will of the parties*." (Werbach & Cornell, 2017).

Smart contracts make any breach of contract impossible, and although on the one hand this is a purely positive feature, on the other hand it sets too strict a framework for the parties, because the parties are people and people are subject to various force majeure events, which cannot be incorporated into the smart contract code.

"*Legal standards are often intentionally vague. Terms like 'best efforts,' 'reasonableness,' or 'good faith' allow the law to be flexible and to account for circumstances that the parties could not have anticipated at the time of formation. Programming code, however, cannot easily accommodate such ambiguity. A smart contract requires a degree of precision that traditional legal drafting often avoids. By forcing parties to translate complex human intentions into binary 'if-then' statements, smart contracts may inadvertently strip away*

the equitable protections that the legal system has developed over centuries to prevent injustice." (Werbach & Cornell, 2017).

In addition, the issue of smart contracts includes the question of whether they should be considered contracts at all, because in fact they are only a way of executing a contract, not creating a new agreement. "*It is a mistake to think of a smart contract as a digital version of a legal contract. Rather, a smart contract is a mechanism for performance. It is a piece of software that can be used to satisfy the requirements of a legal agreement, but it does not necessarily contain the agreement itself. While a smart contract may be evidence of an underlying agreement, the legal contract exists in the shared intent of the parties, whereas the smart contract exists only in the code. Therefore, the code is not the contract; it is the execution of the contract*." (Werbach & Cornell, 2017).

However, there are cases where there is nothing at all besides the code. For example, buying an NFT on a marketplace, in which case a smart contract should be considered a contract.

Chapter II

Smart contracts were widely popularized thanks to the Ethereum ecosystem and its creator Vitalik Buterin.

However, along with the popularization came new challenges and the first failures. Already in the first years of the ecosystem's operation, a precedent was set that still gives critics of smart contracts grounds for critical judgments.

A classic example of exploiting a smart contract vulnerability was the attack on The DAO (Decentralized Autonomous Organization) in June 2016. The attacker used what is known as “reentrancy”: the contract allowed the withdrawal function to be called multiple times before the internal balance was updated. As a result, about 3.6 million ETH were withdrawn to a child contract. The funds could not be withdrawn immediately due to a built-in delay, which gave the community time to react. Later, the Ethereum network hardforked to return funds to investors; this led to the chain being split into Ethereum and Ethereum Classic.

"The 'Code is Law' doctrine assumes that the code is perfect. However, humans write code, and humans make mistakes. Legal intervention is necessary when the code does not reflect the parties' intent."- Vitalik spoke later.

The issue of state regulation and its prospects is also quite complex and ambiguous. If for a programmer the mere fact of working code is success, then for a lawyer this is not enough.

The code must comply with the law and be accurate and transparent, and in the context of smart contracts, this is almost impossible to do, due to the specifics of the blockchain.

"The legal system does not exist merely to enforce agreements that go well; it exists to resolve disputes when things go wrong. Because human foresight is limited and programming is fallible, there will always be situations where the outcome of a smart contract is perceived as unjust, fraudulent, or mistaken. In these cases, the state—through its judicial branch—retains the ultimate authority to look behind the code. The court's role is to ensure that the technological execution aligns with the legal intentions of the parties and the overarching mandates of public policy. To suggest that a smart contract could entirely bypass judicial review is to misunderstand the fundamental protective function of the law in a civilized society." (Werbach & Cornell, 2017).

A smart contract is a "technical fact" and a court decision is a "legal truth." If they conflict, the state will always give priority to the legal truth.

"We must resist the temptation to anthropomorphize smart contracts as autonomous actors. They are tools created by humans to serve human ends. As such, they remain subject to the law of agency and the law of contracts. If a smart contract produces an outcome that no rational person would have agreed to, the law provides doctrines such as unconscionability or mutual mistake to rectify the situation. The role of the state is to provide a 'safety net' that prevents the mechanical rigidity of code from producing outcomes that are socially or economically destructive. In this sense, the law is not an obstacle to smart contracts, but a necessary condition for their widespread adoption and legitimacy." (Werbach & Cornell, 2017).

Chapter III

The problem of regulating smart contracts lies in the nature of smart contracts. This type of contractual relationship was created in order to avoid any intermediaries between the parties, and the state, by interfering in them and trying to regulate, becomes such an intermediary. It doesn't matter if the state will force to add «Kill Switch» to the code as proposed by the European Union, for example or create backdoors for law enforcement, in any case the nature and architecture of smart contracts will be changed.

However, it is still worth considering that smart contracts create a dangerous space for fraud, because in conditions where the state cannot intervene in public relations, the advantage is on the side of the fraudster. Of course, anything the state touches stops working as originally intended, but in the case of smart contracts, this is likely to be less negative than if the state did

not intervene at all. If the state cannot guarantee the safety and protection of the parties to the contract, then such social relations put the foundations of law and the state in general in an unstable position.

The European Union is generally one of the first to regulate smart contracts at such a high level, and it is worth mentioning here EU Data Act (Regulation (EU) 2023/2854). Applies from 12 September 2025, it sets new, harmonized rules on who can access and use data generated by connected devices (IoT) and related services. It aims to foster a fair data economy by empowering users—both consumers and businesses—to access, use, and share their generated data, specifically enabling aftermarkets and reducing reliance on manufacturers.

The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall ensure that those smart contracts comply with the following essential requirements of:

(a) robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

(b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;

(c) data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);

(d) access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers; and

(e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes (European Parliament and Council of the European Union, 2023).

Conclusion

However, smart contract regulation is still in its infancy and requires future refinements and improvements. The introduction of smart contracts can indeed facilitate many aspects of contractual relations, but due to certain disadvantages of this type of contract execution, it can

also entail difficulties and unforeseen force majeure. In addition, the use of smart contracts eliminates the flexibility of contractual relations, which also negatively affects the terms of the contract. Human error, unforeseen circumstances, and general misunderstanding of the contract are not taken into account by the automatic process when using smart contracts, so in such cases the parties are more vulnerable.

Bibliography

1. European Parliament and Council of the European Union. (2023). 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 (Data Act). https://eur-lex.europa.eu/eli/reg/2023/2854/oj
2. Szabo, N. (1996). Smart contracts: Building blocks for digital markets.
3. Szabo, N. (1997). The idea of smart contracts.
4. Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke Law Journal, 67(2), 313–382.