INNOVATIVE PUBLICATION

Journal of Effective Learning and Sustainable Innovation

Vol.3 №6 (2025). June

innovativepublication.uz

Distinctive features of obligation fulfillment in civil relations complicated by smart contracts

Isakulova Elmira

Master's student of Business Law in Tashkent

State University of Law, Tashkent, Uzbekistan

Tel: +998 94 245 99 22

Email: elmiraisakulova100@gmail.com

Abstract: the integration of smart contracts into civil law relations introduces a paradigm shift in how obligations are formed, executed, and enforced. This article examines the distinctive legal and practical aspects of fulfilling obligations in civil transactions involving smart contracts, with a particular focus on challenges within the legal framework of Uzbekistan. Drawing on international experience and scholarly sources, the study highlights the gap between the technological logic of smart contracts and the foundational principles of traditional civil law

Keywords: smart contracts, blokchainn, digital contract, automatization, Nick Szabo, Ethereum, DeFi, DApps, legal coding, immutability, trust issues, Web 3.0, digital economy, criptography, contract law

Introduction. In the rapidly evolving digital economy, the integration of blockchain technology and smart contracts into legal frameworks has catalyzed a profound transformation in the nature and execution of civil obligations. Smart contracts—self-executing digital agreements encoded on a blockchain—represent a fundamental departure from traditional legal instruments by automating performance based on predetermined conditions, often without recourse to human interpretation or intervention. This shift raises significant questions regarding the adaptability of existing civil law doctrines, particularly in jurisdictions grounded in Romano-Germanic legal traditions, such as Uzbekistan.

Historically, the fulfillment of obligations in civil law has been predicated upon principles of autonomy of will, contractual freedom, and judicial oversight. These principles allow for the interpretation of parties' intent, equitable adjustment in the face of unforeseen circumstances, and a structured mechanism for dispute resolution. In contrast, smart contracts rely on the logic of code—precise, immutable, and indifferent to nuance—which challenges the normative underpinnings of conventional legal relationships. While the technological efficiency and trustless architecture of smart contracts offer considerable advantages in terms of transparency, cost-reduction, and transaction speed, they also risk engendering rigidity and injustice where real-world complexity exceeds the scope of algorithmic expression.

In the context of Uzbekistan, a nation actively transitioning toward a digital economy and exploring legal-tech innovations, the introduction of smart contracts into the civil sphere presents both opportunity and peril. Although nascent pilot projects signal a governmental willingness to embrace blockchain-based solutions, the existing legal infrastructure lacks the specificity and sophistication necessary to fully integrate and regulate smart contractual mechanisms. Consequently, civil obligations executed through

smart contracts operate in a legal gray zone—technologically enforceable but potentially devoid of legal legitimacy or recourse under current statutes.

This article endeavors to explore the distinctive features of obligation fulfillment in civil relations complicated by the use of smart contracts. By juxtaposing the deterministic nature of smart contracts with the adaptive principles of civil law, and by analyzing relevant legal doctrines, this study aims to identify both the conceptual tensions and the prospective avenues for harmonizing technological innovation with legal certainty. Special attention is devoted to the Uzbek legal context, drawing comparisons with international models to propose a roadmap for future legal reforms that could accommodate the unique challenges posed by smart contracts

Smart contracts in civil law. Traditional contracts have a clear, transparent and enforceable legal basis in every important aspect of the activities under their jurisdiction. However, for smart contracts that are applicable to Blockchain technology, legal supervision is in a blank state. The legal basis of a smart contract should consist of framework legislation and specific legal, regulatory and system-level agreements. In addition to focusing on the system itself, both parties to the transaction need to pay attention to their respective contractual rights and obligations. Regardless of whether it is a transaction party or a third-party organization, because Blockchain technology is used as a data transaction platform, no single entity can change the agreement in the smart contract, so there is no centralized regulator that can force changes and processing of the agreement. In contrast, this is intrinsically different from the fact that in the traditional contract, the supervisory authority has the actual control and can control the contract rules. The agreement in a smart contract does not define any legal rights or obligations of its members. In a decentralized, distributed, intelligent contract system, the protocol replaces the existing legal framework and implementation process of the regulatory body, which is at the bottom

of the payment ecosystem. Since the current regulatory agencies do not provide a legal framework for the use of smart contracts that are supported by Blockchain technology, these frameworks do not effectively address the risks involved in contract performance.

In spite the fact that, smart contracts have high transparency, speed and technical clarity, they have arised many questions in terms of their legal and regulatory issues.

Firstly, enforceability, a legally binding contract usually requires:

- Offer and acceptance;
- Intention to create legal relations;
- Consideration (exchange of value).

Smart contracts may not clearly demonstrate these, especially when written only in **code**, not in natural language. This may result in some misunderstandings. Furthermore, immutability which once blockchain is deployed, smart contracts cannot be easily changed. In contrast, in traditional contracts force majeure (force majeure refers to unforeseeable and uncontrollable event**s**—such as natural disasters, wars, pandemics, or government actions—that prevent a party from fulfilling contractual obligation**s**. In traditional legal systems, force majeure clauses excuse or suspend performance during such events) can be considered while making contracts, but smart contracts cannot understand the context and or exercise discretion like human. For example, if a sales contract is coded to pay upon delivery but a flood halts transport, the smart contract may still try to execute payment unless specifically code is put.

Security. The majority of smart contracts on the first generation of blockchain platforms are balance-based, whereby a defect in one exposes all addresses linked with that contract. That means if hackers discover a bug and are successful in exploiting it, they will be able to drain cash from every single address that has ever transacted with the faulty

system. According to EU Blockchain report, Decentralised finance (DeFi) is a highly volatile market where millions of people become victims of large-scale privacy breaches and theft. If we look at the number, we find that within the first three months of 2022 USD 682 million was lost due to hacks and crypto fund owners and businesses lost USD 3.3+ billion as a result of hacker attacks and security breaches. Deliberate hacks that exploit blockchain-type technologies can include ‘rug-pulls’, ‘flashloan attacks’, and a combination of these attacks with traditional types of irregular behaviour. Opportunistic attacks on smart-contracts can also exploit vulnerabilities, bugs and errors in the contract code.

However, smart contracts can be highly versatile and adaptable, allowing for complex conditions and actions beyond simple value transfers. As such, they can be applied to a wide range of use cases beyond just the exchange of assets, including supply chain management, voting systems, and more. Generally, to have real world use, smart contracts must have three things: 1) an exchange of value; 2) a meeting of the minds between parties; and 3) a representation of an exchange.

The parties must intend to exchange something of actual value, such as digital assets or cryptocurrency. Smart contracts, like traditional contracts, are typically used to facilitate some form of value exchange. This value exchange can take various forms, such as digital assets, cryptocurrencies, or even physical goods and services. Smart contracts are designed to automate and secure these exchanges by executing predefined actions once certain conditions are met.

There must be a meeting of the minds as to the exchange of value, meaning the parties must intend to agree to the terms. In contract law, the meeting of the minds refers to a mutual understanding and agreement between the parties involved. In the context of smart contracts, this means that the parties must clearly understand and consent to the terms and

conditions encoded within the contract. Smart contracts are typically transparent and self-executing, which can help ensure that all parties are on the same page and that there is a shared understanding of the contract's terms.

There must be a physical representation for the value exchange, meaning a record on the ledger digitally signed between and naming the parties.34 Smart contracts often rely on blockchain technology or distributed ledger systems to record and verify the terms and execution of the contract. These digital records serve as a representation of the value exchange, providing a tamper-resistant and transparent ledger of all transactions and contract executions. Each party's digital signature on the blockchain can confirm their agreement and participation in the contract.

Obligation fulfillment of smart contracts. In traditional legal theory, an **obligation** is a legal relationship whereby one party (the obligor) must perform a duty to another party (the obligee). According to civil codes such as Uzbekistan’s, performance of an obligation must:

- Correspond to the agreed-upon terms,
- Be executed in good faith,
- Occur at the appropriate time and place,
- Involve parties with legal capacity.

Smart contracts encode these terms in code, and fulfillment is achieved when the programmed conditions are satisfied.

For instance, a smart contract may automatically transfer payment to a seller once a delivery oracle confirms that goods have been received. This **automated fulfillment** bypasses many of the interpretative and procedural stages found in traditional enforcement

mechanisms. Smart contracts deploy by monitoring real-time conditions and automatically executing the terms coded into them. This provides **certainty**, **speed**, and **trustless interaction**—ideal for digital environments. Once [deliveryConfirmed] becomes [true] (often via an oracle), the obligation is fulfilled from the smart contract's perspective. Smart contracts cannot access real-world data on their own, **oracles** are used to input external data (e.g., confirmation of delivery, weather status, legal events). The accuracy of the oracle thus directly impacts the validity of fulfillment.

Legal considerations and paradigm across the Europe.

The European Union have accepted the Data Act (published in February 2022), herein smart contracts are defined as ""computer programs on electronic ledgers that execute and settle transactions based on predetermined conditions. They have the potential to provide data holders and data recipients with guarantees that conditions for sharing data are respected. As such, they facilitate the automated and interoperable use of data. The use of electronic ledgers implies they use advanced encryption techniques, and can be decentralised and distributed, resulting in immutability."

Smart contracts have the potential to ensure that conditions for sharing data are respected. Thus, smart contracts are of particular relevance for data transfers and data pooling, since they can give data holders and data recipients trust, that data agreements are followed. The proposed regulation aims to promote the interoperability of smart contracts in data sharing applications. Smart contracts are addressed under Chapter VIII of the Data Act legislative proposal, in Article 28 (1) (d) and Article 29.

According to the article 30 (1) of Data Act, there are four requirements for smart contracts:

1. robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;
2. safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;
3. data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and
4. access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers.

REFERENCES:

1. Szabo N. Smart Contracts: Building Blocks for Digital Markets // Extropy–1996 – No. 16
2. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform // Ethereum White Paper. – 2013. – Available at: https://ethereum.org/en/whitepaper/.
3. EU Blockchain Observatory and Forum. The European Union Blockchain Ecosystem Developments. – 2022. – Available at: https://www.eublockchainforum.eu/reports.
4. European Commission. Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) // EUR-Lex. – 2022. – Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068.
5. Civil Code of the Republic of Uzbekistan. – Tashkent: Ministry of Justice, 2023.
6. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. – New York: Portfolio/Penguin, 2016. – 343 p.

7. Werbach K., Cornell N. Contracts Ex Machina // Duke Law Journal. – 2017. – Vol. 67. – P. 313–382.

8. Raskin M. The Law and Legality of Smart Contracts // Georgetown Law Technology Review. – 2017. – Vol. 1. – No. 2. – P. 305–341.

9. Clack C.D., Bakshi V.A., Braine L. Smart Contract Templates: Foundations, Design Landscape and Research Directions. – 2016. – Available at: https://arxiv.org/abs/1608.00771.

10. Wright A., De Filippi P. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. – 2015. – Available at: https://ssrn.com/abstract=2580664.