STUDIA JURIDICA ET POLITICA JAURINENSIA
VOL. 11, NO. 1, 2024, 103–113
DOI: 10.71100/STUDIA.2024.1.9

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

SMART CONTRACTS: A COMPREHENSIVE ANALYSIS OF VULNERABILITIES AND EUROPEAN MEASURES

HIBATALLAH, LOUKIL[1]

ABSTRACT

Smart Contracts form a predominant tool for today's operations, and it is existing in practically all fields like health, banking, investments etc. It is an alternative that matches the rapidity, and the easiness required by the new era. But legal adjustments are needed to preserve the rights and confront the challenges that come with it.

KEYWORDS Smart contracts, blockchain, European Union, regulations

1. Introduction

Accessibility and facility are the requirements for our era. The fast-paced life made our system establish an updated process that can come up with new factors. As many fields changed their way of operation, law also has been changing to reach the necessities of this new world either by creating new sections or switching rules from traditional form to an updated form.

This paper aims to explore the role of legal technology, smart contracts, in the future contract law and their impact on the legal system. The emergence of new technologies is reshaping how contracts are written, signed, and conflicts are settled, bringing up various legal and ethical concerns. By examining these issues closely, we can gain insight into the capabilities and constraints of legal technology, which can inform the evolution of civil law in the future.

2. Smart Contract: a new technology built upon blockchain

Before jumping directly into emphasizing the term "smart contract", it is essential to define the contract, which is an agreement between parties, creating mutual obligations that are enforceable by law (Committee on Payments and Market Infrastructure, 2017, p. 2).[2]

[1] PhD Student at University of Debrecen, Faculty of Law, Department of European Law, Debrecen, Hungary.

[2] DLT refers to the processes and related technologies that enable nodes3 in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes.

The fundamental components needed for a contract to be legally binding include mutual agreement demonstrated through a valid offer and acceptance, fair consideration, capacity of the parties involved, and compliance with legal requirements.

In certain jurisdictions, consideration may be fulfilled through acceptable alternatives. Potential solutions for breaching a contract encompass general damages, consequential damages, reliance damages, and specific performance. The concept of smart contracts was first developed in 1994 by Nick Szabo, an American computer scientist. Szabo defined smart contracts as computerized transaction logs that execute the terms of a contract. It involves recording contracts in the form of computer code that would automatically activate when certain conditions are met. When these triggering elements occur, the encoded contract executes itself. This operation shows it as a software, the smart contract is more of a technology than a legally binding contract in the traditional sense. This innovation enhances remote transactions between completely unrelated parties without any intermediate authority through blockchain.

A blockchain or "distributed ledger technology" (DLT) , is a distributed database that keeps an ever-expanding list of organized records, known as blocks. These blocks are connected through cryptography, with each block containing a cryptographic hash of the preceding one, along with a timestamp and transaction data. Functioning as a decentralized, distributed, and public digital ledger, a blockchain records transactions across numerous computers. Its design ensures that altering any past record necessitates changing all subsequent blocks and gaining consensus from the network (Catalini, 2018). This smart contract can operate without being tied to a central authority. All assets requiring central authority can be exchanged on a blockchain: financial assets, property titles, etc. It's the trust provided by the blockchain that enables it to become a tool for disintermediation. This disintermediation has the power to reduce costs and make exchanges more seamless.

According to Nick Szabo:

> *"A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart-contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs."* (Szabo, 1997)

Trying to seek the differences between traditional contracts and smart contracts, the enforcement is based on a blockchain which needs a consensus mechanism to generate the contracts. The consensus remains a main stone in both traditional and smart contracts but in different shapes. There are two main consensus mechanisms: proof-of-work and proof-of stake. If it is a proof of work "PoW", parties agree through using their computational power.[3] The agreement will be incorporated into and upheld by a blockchain if the majority of the computational power within the blockchain agrees to it. As per Satoshi Nakamoto, the pseudonymous creator of Bitcoin, through a proof-of-work mechanism, individuals express their acceptance of valid blocks by dedicating their CPU power to extending them and reject invalid blocks by abstaining from working on them.

This protocol requires a verification process handled by someone called "the miner" to resolve the cryptographic question quickly to get the tokens as a reward.

The second way is the proof of stake "PoS", it depends on the available amount in the digital wallet of the validator or the "stake". It is like a lottery game where the wealthiest in the system, the higher the probability of becoming the block leader and winning the validation as it is chosen by the system.

The second difference is the language used in preparing the contract is the language. It is switched from a legal composed clause to a computer language that can be stored in the system as a code .

Szabo says that:

> *"The basic idea behind smart contracts is that 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."* (Szabo, 1997)

He installed his theory on the example of a vending machine where the fact of inserting the coin will result in the automatic delivery of the products. This implies that every smart contract includes a collection of rules that initiate

[3] Blockchain computation involves carrying out the instructions contained within transactions or smart contracts on the blockchain. This process demands substantial computational power and energy, particularly for blockchains that handle intricate smart contracts. Block producers, such as miners or validators, typically perform the computation process, enabling state changes by executing transaction.

predefined responses automatically, matching specific conditions within a deterministic computational log.

The smart contract, by guaranteeing the permanence of transactions, will help in foreseeing the different terms of the contract. Essentially, any alteration, deletion, or removal of an entry from the ledger requires consensus from all network members, ensuring the high security of the blockchain. Smart contracts will enable the automated execution of various agreements such as insurance contracts, transportation agreements, loans, shareholder agreements, or preference agreements. Self-executing contracts faced a hurdle in transfer assets without relying on a trusted intermediary (like a bank or notary). However, blockchain-powered smart contracts have changed this situation to having the contract terms, represented as lines of computer code, stored on the blockchain and executed automatically. These terms are immutable once recorded but are available for all stakeholders to review.

3. Legal risks in smart contracts

Cryptography was the tool for the blockchain to ensure the integrity of transaction terms. This aspect is particularly intriguing for the field of law. Through this operation we will be able to prove the existence of agreement and commitments made by the parties involved. As a ledger, the blockchain guarantees traceability of all operations conducted, along with different transaction dates. Therefore, it will be impossible to deceive or lie about the fulfilment of contract conditions which will provide the right information with no need of proof.

Another interesting aspect regarding the "preservation" of the ledger is viewing the blockchain as an archive. Not only is it unchangeable, as mentioned earlier, but the blockchain also retains all its data, stored in storage nodes. Everyone can see it, and everything is retrievable. It's unlike a paper contract, which can be (and sometimes is) lost. Thus, by definition, the blockchain fulfils the publicity conditions inherent to a contract. Logically, if everyone has access and can see what happens on the blockchain, then the obligations of publicity and publication are met.

These elements are surely facilitating but doesn't still make the smart contract legally right?

Usually, a contract implies an offer, an acceptance meeting the conditions of validity like consent, capacity, absence of fraud, absence of error, stated in the national Civil Code but here the informatic code is the law Logically, the question arises: can a smart contract fulfil these conditions of the traditional contract?

Also, the identification of the contracting party is blurry. As mentioned earlier, each blockchain user possesses a private key, which is crucial for certifying their actions on the blockchain. This private key can be stolen or lost, or it can be held by multiple different individuals (similar to multiple people using the same bank card, knowing the PIN). Additionally, since blockchain allows for anonymity, the contracting party in a smart contract may wish to remain anonymous.

4. Interpretation of Terms and Conditions

The first difficulty lies in formalizing the offer and ensuring informed and valid acceptance of the offer by the co-contractor. As it must be of legal age, capable of understanding all the terms of the contract, not making any errors, and not being subject to pressure to sign the contract.

It is already challenging to verify all these conditions in the case of traditional contracts, and they are even more difficult to verify in the case of digital contracts, because it's the code that defines the smart contract in a complex programming language, so the terms are hard to be interpreted and can be confusing for non-technical persons.

Therefore, it must be proven that the co-contractor understood the code integrated into the contract and he approved it without any ambiguities.

Interpreting the terms and conditions of smart contracts (Cannarsa, 2018) may raise the question of whether it should be objective or subjective. In traditional contracts, interpretation is often based on the parties' intention, which can be subject to differing opinions. In the case of smart contracts, interpretation may be based solely on the computer code, providing a more objective interpretation. However, this can lead to unexpected or unfair outcomes in certain situations, but the computers are "non thinking, high performing agents" (Susskind & Susskind, 2015) who follow the rule according to the available information that was inserted in the system as there is no room for interpretation which makes it a rigid instrument especially in problem situations.

At that point the responsibility of the parties take place in a dispute regarding the execution of a smart contract, it can be difficult to determine who is responsible, particularly in cases of programming errors or differing interpretations of the terms. Parties may find themselves in a situation where they must bear unforeseen or unfair consequences due to the interpretation of the terms and conditions placed by the code.

5. Absence of specific regulation

The absence of specific regulation creates an uncertain legal framework for smart contracts. Existing laws may not be suited to address the unique challenges posed by this technology. Traditional legal principles may not directly apply to smart contracts, leading to uncertainty regarding their validity, execution, and interpretation. This situation can make it difficult for involved parties to understand their rights and obligations. The validation and enforceability of smart contracts are major concerns in the absence of specific regulation. In many countries, traditional contracts are generally valid and enforceable if certain conditions are met, such as offer, acceptance, and consideration. However, smart contracts may require different criteria to be considered valid and enforceable. The lack of clear regulation can make it challenging to determine how smart contracts should be legally formed and enforced. It also raises questions regarding the contractual liability of parties involved in smart contracts. In case of disputes or breach of contractual terms, it may be difficult to identify available remedies and determine the parties' liability in the absence of clear legal guidance. This can lead to legal challenges in resolving disputes and protecting parties' rights.

Therefore, it can impact consumer protection in the context of smart contracts. Consumers may face risks such as unfair contract terms, programming errors, or unfair business practices. Without clear regulation, it can be difficult to ensure that consumers are adequately protected when using smart contracts.

6. Confidentiality and personal data

It is insightful that blockchain technology offers complete transparency to smart contracts, allowing all parties involved in a transaction to access necessary information. However, this transparency must be balanced with data protection, so we can ensure that only necessary information is shared while preserving the confidentiality of sensitive data.

The user consent and control can be programmed so that users have total control over their personal data. For example, a user can specify the conditions under which their data can be used and share only necessary information. This approach enables users to give informed consent and maintain control over their data. This is an advanced cryptography technique to protect personal data.

Sensitive information can be encrypted before being stored on the blockchain, ensuring that only authorized parties can access it. Additionally, smart contracts can be designed to automatically delete sensitive data once predefined conditions are met.

But these above-mentioned options sometimes fail to comply with data protection regulations. Mainly smart contracts can be designed to comply with data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) and by integrating privacy and data protection mechanisms into the design of smart contracts, companies can avoid non-compliance risks and ensure the confidentiality of their users' personal data but some characteristics in the contract itself can be debatable with GDPR.

The immutability and the non-changing element in this type of contract can be against data subject rights such as right of rectification and right to erasure (right to be forgotten) in article 17 from the same regulation. While concluding and finalizing the General Data Protection Regulation Jan Philip Albrecht, a Member of the European Parliament who played a prominent role expressed that:

> *"Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subject' s rights] based on their architectural design […] This does not mean that blockchain technology in general has to adapt to the GDPR, it just means that it probably cannot be used for the processing of personal data."* (Meyer, 2018)

7. The regulatory framework for smart contracts

All kinds of innovation need to be organized and legally well-structured to build the trust of users towards the new technology and feel safe as being protected by the government in case of a problem.

While smart contracts offer innovative solutions for executing agreements and transactions, they must still adhere to relevant laws and regulations governing contract formation, consumer protection, data privacy, and financial transactions.

One of the challenges with smart contracts is that they often exist in a legal grey area due to the novelty of the technology and the lack of specific regulations tailored to them. As a result, legal experts and policymakers are working to adapt existing laws or create new ones to accommodate smart contracts and ensure their legal validity and enforceability.

Thus, the European Union introduced through the last decade multiple regulations to be up to date with the advancements in different fields, it has undergone a transforming shift in the personal data and its impact by technologies.

8. Data Protection and Privacy compliance

Smart contracts often involve multifaceted considerations such as the processing and storage of personal data, raising concerns about compliance with data protection regulations such as the European Union's General Data Protection Regulation (GDPR,) where developers must implement privacyenhancing measures to safeguard sensitive information and comply with consumers rights as for the users.

More provisions took place with GDPR to ensure lawful and transparent processing of personal data like Eu Data Act, eIDAS regulation and the European Law Institute's Principles of Blockchain Technology.

The vision started in 2018 with the Communication Towards a common European Data Space in order to cover personal data and public data to reach business-to-business and business-to-government data sharing. with the adoption of the Data Governance Act in 2022 and was the first deliverable under the European strategy for data, the concretisation of a harmonized strategy came to the light as it focused on having a united market data with European sovereignty. The application started with Data Governing Act serves as a comprehensive mechanism for supervising the utilization of public or safeguarded data across diverse industries. Its primary goal is to streamline data exchange by regulating newly established entities called data intermediaries and advocating for altruistic data sharing practices. Both personal and non-personal data fall under the purview of the DGA, with the General Data Protection Regulation (GDPR) being applicable whenever personal data is involved.

To foster trust in data sharing and reuse, the DGA incorporates additional safeguards alongside GDPR. This emphasis on trust-building is pivotal for expanding data availability within the market.

The Data Act is a complementary tool for the above-mentioned provisions, as the Data Governance Act establishes frameworks and procedures aimed at promoting data sharing, particularly within the public sector. The Data Act introduces fresh regulations governing the utilization of data generated by connected products and associated services. It delineates guidelines regarding how users can utilize such data and outlines conditions under which data holders can derive economic benefits from it and insert detailed definitions in Article 2 for data and even for smart contracts as *"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"* and it included a whole section in Article 36 for *"essential requirements regarding smart contracts for executing data sharing agreements"* that regulates the use of smart contracts as a tool between IoT providers who are the data holders and third party recipients who need to enter an agreement for data sharing and flow.

The use of smart contract in the act was "neutral" as mentioned, as it can mean electronically ledger connection or "in- house for internal use" but the key is the

> *"requirement to ensure that smart contracts can be interrupted and terminated implies mutual consent by the parties to the data sharing agreement. The applicability of the relevant rules of civil, contractual and consumer protection law to data sharing agreements remains or should remain unaffected by the use of smart contracts for the automated execution of such agreements"* (Data Act, Preamble 104)

and for that smart contracts are for any vendor sharing data and for data holders of IoT providers where any operations that will provide a third-party data, the application is direct.

In the same matter, European Union introduced since 2014 the eIDAS electronic identification and trust services(eIDAS) the digital identity (eIDAS2) and the self-sovereign identity, which involves the use of a verifiable credential from an issuer in a signature process and simplifies the work of the verifier throughout the European Union.

The legal report on SSI analyses various scenarios regarding the use of the eIDAS Regulation to ensure digital identity and transactions based on DLT technologies, i.e., from a centralized perspective. It contains insightful suggestions regarding the ongoing revision of the eIDAS Regulation (European Commission, 2024).

9. Financial Regulation and Market Integrity

As Smart contracts operate on blockchain technology and promote high levels of efficiency and transparency, it became a required tool in the BFSI "Banking, Financial Services and Insurance Sector" to achieve some strategies in manual processing, minimize fraud rates and lower the expenses. Its compliance with the encoding regulatory requirements in different regulations is essential such as Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) regulations, as well as Know Your Customer (KYC) requirements[4] to ensure accountability, safety and transparency in identity verification to provide a high level of security in processing agreements.

Infinite number of operations are done every second and limiting crimes is getting more challenging with high-speed application, so the extension is needed to cover more than traditional crimes to emerging frameworks tailored for digital assets and blockchain technology. "Markets in Crypto-Assets Regulation" (MiCA), is a revolutionary milestone legal framework that stand up for management of crypto assets in the EU by clarifying and unifying the law in this matter and it is also a complementary document for Central Securities

[4] KYC is a process implemented by companies to confirm their clients' identities in adherence to legal requirements and regulations, including AML, GDPR, and eIDAS (Koczan, 2021).

Depositories Regulation (CSDR), Markets in Financial Instruments Directive (MiFID), and Transaction Reporting Regulation (TFR) regulations.

These sets form a package that fulfil the gap between the old management of financial law and the new digital ecosystem. By establishing these significant elements, the adjusting of new crimes and the operation of future processes will be elevated and harmonized.

The clarity imposed in Mica that places a mechanism for crypto across Europe allows to facilitate the cross-border activity and implement standard practises to ensure the market integrity and stabilize risks.

The integration of other regulations works on aligning interoperability between institutions and create a smooth cooperation to develop a strategic service for the innovative financial market.

10. Conclusion

Smart contracts are a double-edged weapon, where it presents risks and high problem probabilities but the fast changing world is implementing easier and faster processes to get up to the results enchanted by the market.

For that the European Union has strategic steps implemented through the years to get approximately a completed vision that works on the major loopholes that were declined by the traditional texts.

References

[1] Cannarsa, M. (2018). Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts? *European Review of Private Law*, 26(6), pp. 773-785. https://doi.org/10.54648/erpl2018054

[2] Catalini, C. (2018). Blockchain Technology and Cryptocurrencies: Implications for the Digital Economy, Cybersecurity, and Government. *Georgetown Journal of International Affairs*, *19*(Fall 2018), pp. 36–42. http://www.jstor.org/stable/26567525

[3] Committee on Payments and Market Infrastructure. (February 2017). *Distributed ledger technology in payment, clearing and settlement: An analytical framework*. Bank for International Settlements. http://www.bis.org/cpmi/publ/d157.pdf

[4] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID)

[5] European Commission. (October 10, 2024). *Shaping Europe's digital future: A European strategy for data*. https://digital-strategy.ec.europa.eu/

[6] Koczan, G. (January 19, 2021). *Harmonisation KYC procedures: Summary of DIMCG separate session* [Conference presentation]. 4th Debt Issuance Market Contact Group Meeting. https://www.ecb.europa.eu/paym/groups/pdf/dimcg/ecb.dimcg210127_item3.1b.en.pdf

[7] Meyer, D. (February 27, 2018). *Blockchain Technology is on a Collision Course with EU Privacy Law*. IAPP. https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/

[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML/CFT Regulation).

[9] 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).

[10] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[11] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (TFR).

[12] 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).

[13] Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 Text with EEA relevance (CSDR).

[14] 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).

[15] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS2).

[16] 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 (eIDAS).

[17] Susskind, R. & Susskind, D. (2015). *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. Oxford University Press. https://doi.org/10.1093/oso/9780198713395.001.0001

[18] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548