CHALLENGES OF *SMART CONTRACTS* IN THE AGE OF QUANTUM COMPUTING: AN ANALYSIS OF BLOCKCHAIN SECURITY

https://doi.org/10.56238/sevened2024.037-019

Luani Maria de Albuquerque Macário[1] and Marielli Melo Soares de Morais[2]

ABSTRACT

This study explores the interaction between smart contracts and quantum computing, mapping the main advantages, risks and vulnerabilities involved, in addition to analyzing the benefits of *blockchain* technology and its insertion in the Brazilian legal world. Smart contracts are contracts programmed in a *blockchain* structure, which do not depend on human actions to be fulfilled. The use of *blockchain* in Law makes it possible to store encrypted data, making it difficult to violate and alter information. However, Brazilian legislation has not yet regulated the use of these techniques. The article addresses the main advantages of *smart contracts*, such as business autonomy, private data security, elimination of data manipulation, reliability, and agility. It proposes measures to ensure the robustness of smart contracts and *blockchain* in the face of the imminent advancement of quantum computing. The methodology used was a critical analysis, in which it is aimed at proposing measures that ensure the robustness of smart contracts and *blockchain in the face of the imminent reality of quantum computing, through a literature review. The relevance of this work lies in the need to anticipate and mitigate potential threats, ensuring that these technological innovations deliver on their promise of security and reliability in an increasingly digitized society.* It is understood that *smart contracts* represent an evolution in the automation of contracts, with the potential to change the way contractual relationships occur in the legal system, bringing new parameters to the law.

Keywords: Smart Contracts. Blockchain. Technology. Quantum Computing. Legal System.

[1] Dr. in Social and Legal Sciences from the Universidad del Museo Argentino, 2019; Postgraduate degree in distance learning from the Faculty of Jacarepaguá/RJ; TEACHING: Raimundo Marinho College, Mauricio de Nassau College, Fama College, Period: 2007 to 2017; Alagoas Military Police, Alagoas Firefighters, Period from 2007 to 2022; Ministry of Science and Technology. Coordination of Sensitive Assets; Work with UN Anti-Terrorism Security. chemical, biological, nuclear weapons; International Law, an arm of the Civil House. Work considered paramilitary, period: 2001 to 2006.

[2] Editor-in-Chief of the Journal of Legal Design & Visual Law; Privacy and Data Protection Compliance Consultant; Member of the National Compliance Association (ANACO) and the Privacy and Data Protection Committee; Prompt Engineer for Cybersecurity by IBSEC; Member of the Laboratories: LGPD Study Community (Facilitator) and Researcher in Legal Design at the Digital Rights Laboratory of the Federal University of Bahia (Labid²-UFBA); Researcher at the Technology and Research Group on Artificial Intelligence and Law of the Technology, Innovation and Data Protection Commission (CITPD) and OAB/AL in partnership with the Escola Superior de Advocacia de Alagoas (ESA/AL); Professional Master's student in Law, Justice and Development at the Brazilian Institute of Teaching, Development and Research (IDP-BSB); Postgraduate in International Law (CEDIN/ Milton Campos/BH-MG); Postgraduate in Constitutional Law (IDP/UNISUL/LFG);
Email: mariellimelo@infodireitodigital.com.br
LATTES: http://lattes.cnpq.br/0389416055398926
ORCID: https://orcid.org/0000-0002-4894-6642

INTRODUCTION

Contemporaneity is characterized by a deep technological immersion, where digital advances permeate and redefine multiple spheres of our existence. Among these advances, smart contracts and *blockchain* technology stand out, promising significant transformations in several sectors, given their ability to provide unparalleled efficiency, transparency, and security (BARON, Guilherme; HOPPE, Aurélio, 2018). However, the evolution of quantum computing presents a potential challenge to the integrity of these technologies.

Recent literature has highlighted the promising synergy between smart contracts and blockchain, highlighting their ability to automate and validate agreements in a decentralized manner. However, the emerging quantum computing, with its superior computational power, calls into question the security of these innovations (MACÁRIO, L. M. A., MORAIS, M. M. S. de, SILVA, M. A. X. da., 2022). Given this scenario, the present research emerges as an attempt to understand and anticipate the challenges inherent to this intersection.

The central purpose of this study is to explore the interaction between smart contracts and quantum computing, mapping the inherent risks and vulnerabilities, in addition to analyzing *Blockchain* technology and how it is and can be inserted in the legal world in Brazil. Initially, the technology is conceptualized and explained in a way that facilitates the understanding of the entire study around it. Blockchain is a powerful tool that has been gaining more and more visibility, it consists of a practically unalterable chain of blocks, where various information is recorded, stored in each of these blocks and by all the computers that access it.

Smart contracts are contracts with clauses previously programmed in a blockchain structure that, once agreed, are characterized by not being independent of human actions to be fulfilled, generating practicality, transparency, and trust in the execution and execution of agreements. The work seeks to analyze the form of reception of *smart contracts* by Brazilian law, through the discussion held in the doctrine and jurisprudence about the legal nature, the applicable legislation and the casuistry, in order to present and defend potential benefits in addition to describing risks in the adoption of this model.

The topic is important and deserves to be investigated, as *blockchain* makes it possible to store encrypted data in order to hinder the possibilities of data violation and alteration. In this sense, the possibility of using the tool in Law was noted, which boosted the development of several initiatives in the area, such as *smart contracts*.

The concept of *smart contracts* was originally thought up by Nick Szabo in 1996 who devised an internet protocol that would help parties perform contracts more efficiently in

order to prevent non-compliance and make potential contractual breaches self-executing.

At the disadvantage of technology is the Brazilian legislation, which has failed to keep up with such progress and, to date, has not regulated the use of these new techniques. This, however, did not prevent them from being used. In this context, there is a need for legal operators to adapt to such technologies, as well as the regulation of smart contracts in Brazil.

Therefore, the article intends to address the main advantages of smart contract technology, using *Blockchain* technologies and, including, but not limited to, business autonomy without third-party intervention, and, consequently, security of private data and the elimination of possible data manipulation; reliability, because the documents are under a computational language that provides certainty and security; agility, due to the self-execution of *smart contracts*; economy, allowing and facilitating greater business freedom, since it minimizes legal uncertainty due to self-execution through quantum computing.

Through a critical analysis, the objective is to propose measures that ensure the robustness of smart contracts and blockchain in the face of the imminent reality of quantum computing, through a literature review. The relevance of this work lies in the imperative need to anticipate and mitigate potential threats, ensuring that such technological innovations maintain their promise of security and reliability in an increasingly digitized society (FEDOROV, A. K.; KIKTENKO, E. O.; LVOVSKY, A. I., 2018).

BLOCKCHAIN E *SMART CONTRACTS*

It is understood that *blockchain* and *Smart Contracts* have a great importance in the field of law. These technologies aim to offer a series of benefits, such as transparency, security, and process automation, which can be applied in various areas of law.

In the field of law, the use of blockchain-based smart contracts allows for the automatic and immutable execution of agreements, eliminating the need for intermediaries and reducing the risk of fraud or disputes. This brings greater legal certainty and efficiency to transactions.

It is understood that *blockchain* can also be used to record and authenticate documents, ensuring their integrity and authenticity. This is especially noticeable in areas such as intellectual property, public records, and commercial contracts.

In the field of governance and *compliance*, *blockchain* can be used to create immutable records of transactions, ensuring transparency and traceability of activities. This is particularly useful in regulated industries, such as finance and healthcare, where you need to prove compliance with rules and regulations.

Blockchain and smart contracts play a precise role in law, providing greater security, efficiency, and transparency for transactions and legal processes. Its adoption is increasingly present and promises to transform the way we deal with legal issues.

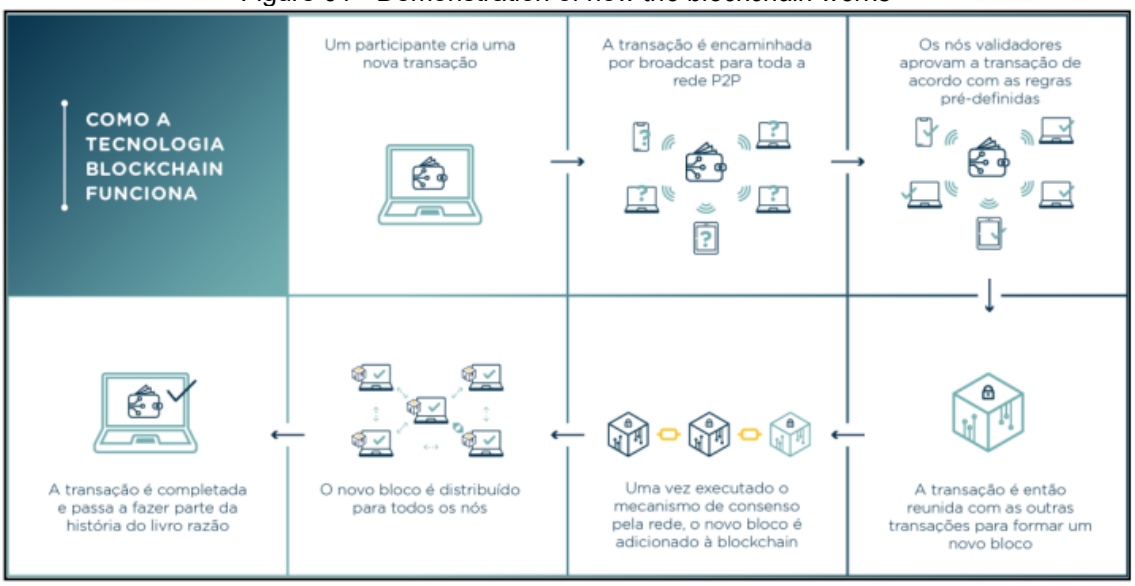
2.1 *BLOCKCHAIN*

The origin of blockchain lies in the Bitcoin protocol, described in an article published by Satoshi Nakamoto (Nakamoto, 2008), which went into operation in 2009. As Bashir (2017) mentions, this paper proposed a new peer-to-peer (P2P) network innovation in which a server, known as a miner, receives transactions with the digital currency bitcoin and, through a Byzantine consensus protocol based on cryptographic challenges, determines the order of transactions.

Blockchain is an emerging and revolutionary information technology that offers distributed, reliable, decentralized and secure support for transactions between participants in a network, based on consensus among them and ensured by a proof-of-work algorithm, whose main objective is to prevent attacks on the network (CHICARINO, JESUS, ALBUQUERQUE and ROCHA, 2017). It is understood that the chain of nodes can be updated by any participant in the peer-to-peer (P2P) network.

Blockchain's ability to create reliable and immutable records makes it notorious and suitable for areas that require high data security and integrity. This is possible thanks to the use of cryptography, allowing each participant to securely process the ledger or digital record of information, known as a *ledger*. Once a block of data is added to the *blockchain*, it is virtually impossible to change or delete it. With this, each transaction is recorded in interconnected blocks, forming a chain of blocks (*blockchain*) that can be viewed by all network participants. Through this system, transactions are visible and accessible to any authorized person, promoting a high level of transparency and accountability (ABIJAUDE, GREVE and SOBEIRA, 2021).

Figure 01 - Demonstration of how *the blockchain works*



Source: Brazil (2020).

As shown in figure 01, all participants in the network can agree on the set and order of execution of transactions through Byzantine consensus, which allows action against malicious nodes that could damage the system. Consensus is an essential element for the development of a reliable and secure system, as it allows participants to agree on the operations to be carried out to maintain the consistency of the system and make it continuous (ALCHIERI, TOMALIN, BESSANI and FRAGA, 2011).

In addition, data security and privacy are important issues that need to be addressed to ensure user trust and regulatory compliance (ALECRIM, 2019). The evolution of the blockchain project can be divided into three phases, as highlighted by Swan (2015, cited by BASHIR, 2017):

> *Blockchain* 1.0, which involved the launch of Bitcoin in 2008, with the first implementations of cryptocurrencies and an ecosystem of applications and payments with digital assets; *Blockchain* 2.0, which began with the innovative proposal of smart contracts in 2013, after the creation of the Ethereum project, conceived by Vitalik Buterin, and the various possible financial applications; and Blockchain 3.0, which characterizes the adoption of *blockchain technology* for the benefit of applications in various areas besides finance, such as government, commerce, arts, health, digital cities (BASHIR, 2017).

Encryption is used to ensure the authorization, authenticity, transaction integrity, and security requirements of the entire system. It is possible to carry out financial transactions without the need for intermediaries, such as banks, quickly, securely, and without borders. The decentralization of *blockchain* allows users to have full control over their financial transactions and data, promoting financial inclusion and individual autonomy. These

transactions are executed and stored permanently on a blockchain and replicated on each server (CHICARINO, JESUS, ALBUQUERQUE and ROCHA, 2017).

SMART CONTRACTS

According to Savelyev (2017), the term "*Smart Contracts*" or smart contracts was first mentioned in 1995 by Nick Szabo, who is a researcher and legal in the field of cryptography, as a principle the central idea was to contribute to the implementation of legal contract and trade practices on the internet. According to the author, although the term was defined in theory, there was no computational infrastructure that could be used to carry out its development (SAVELYEV, 2017).

According to Alecrim (2019), smart contracts are autonomous computer programs that automatically control and execute actions when certain predefined conditions are met. In this way, smart contracts were designed to conceive the facilitation, verification and satisfactorily comply with the negotiation or negotiation of agreements between parties without the need for traditional intermediaries, in this scenario they are considered an innovation of traditional contracts, incorporating computational logic and automation so that there is reliable execution and impartiality of the agreed clauses (ALECRIM, 2019).

It is understood that *Smart Contracts* are systems that move digital assets automatically with pre-specified rules, so these contracts are developed and written in high-level language, the contract will be executed only when a transaction is triggered, in which one contract can trigger another and so on, to a certain extent according to what was pre-defined, where the first contract in this execution chain will be called by a user's transaction (Ølnes et al., 2017).

Another aspect that should be highlighted is the security and transparency of smart contracts is that in addition to immutability and automation, security is a fundamental feature of smart contracts, as they are protected by advanced cryptography and incorporate mechanisms to ensure the authenticity and integrity of transactions. Programming languages such as the previously mentioned, Solidity, are one of those used in the creation of smart contracts

Abijaude, Greve, and Sobeira (2021) highlighted another important aspect of smart contracts, in which security and transparency are precise characteristics. In addition to immutability and automation, security is a fundamental feature of smart contracts, protected by advanced cryptography and incorporating mechanisms to ensure the authenticity and integrity of transactions, programming languages such as *Solidity* are widely used in the creation of smart contracts.

THE INTERSECTION BETWEEN *SMART CONTRACTS* AND *BLOCKCHAIN*

It is understood that the intersection between *Smart Contracts* and *Blockchain* brings with it important implications for the legal field. *Smart Contracts,* which are self-executing, code-based digital contracts, offer the opportunity to automate and streamline legal processes, eliminating intermediaries and reducing costs. In turn, *Blockchain* technology ensures the security, transparency, and immutability of transactions, which can be especially relevant in contractual matters.

Blockchain technology and smart contracts are two revolutionary innovations that are transforming the way transactions are conducted. *Blockchain* and smart contracts form the basis of many cryptocurrency projects, as well as several other applications in industries such as finance, real estate, healthcare and governance, and legal. It is important to note that smart contracts are not limited to legal documents only, but encompass the concept of contract holistically, as taught by Tartuce (2020):

Contracts are, in short, all types of agreements or stipulations that can be created through the agreement of wills and other ancillary factors. In a classical or modern view, the contract can be defined as a bilateral or plurilateral legal transaction that aims to create, modify or extinguish rights and duties of a patrimonial nature (TARTUCE, 2020).

According to Soares (2022), this technology has been widely used in the creation of the aforementioned smart contracts, which are self-executing digital contracts that use pre-defined programming to automate the execution of terms and conditions agreed upon between the parties involved in a transaction. Blockchain provides a secure, transparent, and decentralized environment for the creation and execution of these smart contracts.

One of the biggest advantages of smart contracts is the automation of the execution of an agreement without human intervention. This brings benefits such as cost reduction, increased security and trust for the parties involved and the market, in addition to reducing the chances of fraud resulting from human behavior (SOARES, 2022).

Fachini (2023) mentions that in addition to being self-executing and allowing the self-management of their clauses automatically, without the need for third parties, these contracts can be used to automate the execution of terms and conditions agreed between the parties involved in a transaction.

In practice, when correctly coded, the program that serves as the basis for the smart contract has the ability to take actions and execute the clauses of the contract. This is called programming intelligence. It should be noted that the execution of these clauses may not be immediate. In many cases, the smart contract is reactive, that is, the human being needs to request the execution of a specific clause. However, this does not diminish the

"intelligence" of the smart contract, since automated execution respects the conditions set out in the contract. In view of this, the program only executes the action if all the conditions provided for are completely met (FACHINI, 2023).

Because it is a contract stored in a block of code on the *blockchain*, as mentioned earlier, the codes stored in the blocks of this technology, which function as a ledger, are practically impossible to change. Therefore, the smart contract cannot be changed without the mutual consent of the parties involved.

An example of a smart contract, reported by the TD Team (2023), is when a company places an order for material from a supplier and formalizes the relationship with a smart contract. When the products are delivered, the contract receives this information and automatically releases the payment, without the need to send an invoice or involve professionals in the financial sector. Smart contracts allow parties to have complete freedom to negotiate and agree on their own terms, creating clauses that protect their interests (TD TEAM, 2023).

Smart contracts can be used in a wide variety of applications, such as in the legal field, identity management, property management, allowing the parties involved in a transaction to establish agreements in a reliable and transparent way, without the need for intermediaries or additional costs. Although they are not yet widely used, smart contracts are considered major drivers in the advancement of *blockchain* technology, which is gaining more and more space in several countries. Therefore, a significant increase in the use of this tool is expected, especially in Brazil.

The use of smart contracts brings significant benefits to the parties involved in a transaction. In addition to automation and cost reduction, they provide greater security and reliability, since all clauses and conditions are programmed and executed in an impartial and transparent manner. This eliminates the need for intermediaries and reduces the risks of fraud or manipulation.

Another advantage of smart contracts is the flexibility they offer. The parties have complete freedom to negotiate and establish their own terms, creating custom clauses that meet their specific interests. This allows for greater agility and efficiency in transactions, eliminating the need for lengthy bureaucratic processes and complex negotiations.

However, it is important to note that despite all the advantages, smart contracts also present challenges and limitations. Correct programming and coding are key to ensuring the effectiveness and security of these contracts. In addition, large-scale adoption still faces regulatory and acceptance obstacles by institutions and the market.

In this way, smart contracts are a promising innovation that is transforming the way transactions are carried out. With the combination of blockchain technology and programmed automation, they offer security, transparency, and efficiency for the parties involved. While there are still challenges to overcome, the use of smart contracts is expected to become increasingly common, driving the advancement of *blockchain* and bringing significant benefits to various industries such as the legal field.

However, the application of *Smart Contracts* and *Blockchain* in the legal field also presents challenges, such as the need to adapt existing legislation, ensure the legal validity of digital contracts, and deal with issues related to privacy and data protection. Given this context, it is essential that legal professionals understand the implications of this convergence and are prepared to face the changes and take advantage of the opportunities that arise with this emerging technology.

THE AGE OF QUANTUM COMPUTING

OVERVIEW OF QUANTUM COMPUTING

It is understood that the first ideas for a computer based on principles of quantum mechanics emerged in the 80s, and since then research in the area of quantum computing has intensified, attracting more and more attention from the technological and industrial sector. Quantum computers differ from conventional computing by applying concepts from Mathematics, Physics and computing in practice (NICOLAU, 2010).

According to Mattielo, Silva, Amorim and Silva (2012, p.1), the field of quantum computing and information has been revolutionary when considering that advances in quantum mechanics and Computer Science have modified the modern lifestyle in several aspects. Classical computing has evolved enough to show how significant its influence has been in today's society. It is to be expected that the large-scale commercialization of quantum computers will bring even more revolutions, along with the discoveries that will emerge from the new research using this technology that deals with problems on the atomic scale.

Mello (2018) mentions that the improvement of quantum systems may transform other areas of research, as it enables the resolution of highly complex operations, such as molecular and chemical interactions, resulting in the discovery of new structures to assist in the creation of new materials and medicines. In addition, it would allow for extremely efficient logistics and supply chains, helping to find new ways to model financial data and isolate key risk factors to make better investments.

According to Jack D. Hidary (2021), recent advances in quantum technologies have made it possible to use quantum computers, quantum sensors, and specific networks, such as Quantum Key Distribution (QKD). According to Hidary (2021, p.15), quantum computing began to stand out as a field of study of its own around 1979.

THE TECHNOLOGICAL REVOLUTION OF QUANTUM COMPUTING

In an article published by Mozelli (2023), it is presented that physicists took the first step towards building quantum computers from individual molecules attached to laser devices called optical tweezers.

According to Mozelli (2023), according to *Nature*, two groups of scientists reported their results in Science on December 7, 2023, in both cases making pairs of calcium monofluoride molecules interact in such a way that they are intertwined, a fundamental effect for quantum computing. Given these factors, these findings are considered an important milestone, as they pave the way to harness entangled states and improve the potential applications of molecular tweezer arrays. This approach utilizes molecules such as qubits, fundamental units of quantum information, rather than atoms or ions as in other quantum computing platforms.

As mentioned by Mozelli (2023), the experiments involved the use of optical tweezers to attach calcium monofluoride molecules individually to each tweezers unit. The molecules were cooled to temperatures close to absolute zero, causing them to remain virtually motionless. This technique allowed scientists to manipulate the spin state of these molecules to represent the "0" and "1" states of the qubits.

These advances could also contribute to the use of trapped molecules for high-precision measurements that could reveal the existence of new elementary particles. The researchers highlight the speed with which the field of quantum computing has advanced and say that the molecules will be the basis of a competitive platform capable of performing quantum simulations. These findings represent a significant advance in the construction of quantum computers using individual molecules attached to optical tweezers (MOZELLI, 2023).

In addition to paving the way for a new approach in quantum computing, these studies make it possible to manipulate quantum information using "qutrits" and offer the opportunity to simulate complex materials and fundamental forces of physics more accurately. With new possibilities for measuring elementary particles, this technology is expected to revolutionize science and computing in the near future (MOZELLI, 2023).

By uniting computer science and quantum physics, this field seeks to develop extremely sophisticated computational systems that go beyond the currently established and widely used models. These systems, which are considerably more efficient than classical computers that use "0" and "1" bits, mark a revolution in information processing and management, ushering in a new era in computing (HIDARY, 2021).

QUANTUM COMPUTING VS. DIGITAL SECURITY

Quantum computers are present in research universities, government agencies, and leading scientific companies, and are often out of reach of malicious individuals. However, this is not always the reality (HATTAR, 2023).

As research into quantum computing continues to advance, there is a growing concern that these computers could soon break modern cryptography. This would render all current methods of data encryption obsolete and require the development of new encryption methods to protect against these powerful machines (HATTAR, 2023).

While the concept of quantum computers is not new, the debate around them has increased in recent months, thanks to continued government actions. In May 2022, President Biden released a national security memorandum that outlined the administration's efforts to preempt security concerns related to quantum computing (HATTAR, 2023). In June, the U.S. House of Representatives passed the Quantum Computing Cybersecurity Readiness Act, requiring federal agencies to migrate their information technology systems to post-quantum cryptography.

This legislation, which still needs to be approved by the U.S. Senate, builds on the continued efforts of the National Institute of Standards and Technology (NIST) to develop post-quantum cryptography standards. In July 2022, NIST released its first four quantum-proof algorithms. Shortly thereafter, the CRYSTALS-Kyber public-key encryption and key encapsulation algorithm, recommended by NIST, was cracked using artificial intelligence combined with side-channel attacks.

Even today's fastest computers have a hard time cracking security keys due to their complexity. It would take years for a system to be able to crack standard keys, even under the best of circumstances. This is what makes encryption such a valuable security defense (HATTAR, 2023).

Quantum computing seems to drastically change this scenario, reducing the time required from years to a few hours. Although the situation can quickly get complicated, experts believe that many popular methods of public-key cryptography today, such as RSA,

Diffie-Hellman, and elliptic curve, may be relatively easy for quantum computers to solve in the future (HATTAR, 2023).

While quantum-based attacks are still in the future, organizations should think about how to protect data in transit when encryption is no longer effective. Best practices include segmenting networks, leveraging private 5G networks, and adopting zero trust architectures (HATTAR, 2023).

The growing concern about cyberattacks related to quantum technology may not be imminent, but it is not unfounded either. Cybersecurity professionals must remain agile in the face of new threats and paradigm shifts. As we move towards this next challenge, we must keep ourselves on a solid foundation.

The author mentions that we are moving towards a future with quantum computing, so it is important to prepare your organization now for this emerging threat, as well as deal with other threats affecting your business today. A defense-in-depth approach acts as a hedge against different attack vectors. It provides organizations with comprehensive coverage and a robust defense against various types of attacks (HATTAR, 2023).

CHALLENGES FOR SMART CONTRACTS IN THE AGE OF QUANTUM COMPUTING

ADVANTAGES, RISKS AND VULNERABILITIES OF *SMART CONTRACTS*

According to Cavalcanti (2020), *smart contracts* are considered a relatively new contractual instrument in the legal system, and all their possible applications are still far from being fully revealed, mainly because blockchain technology is constantly evolving. With this technology, there is a potential to gain speed, practicality, security, and effectiveness in the legal routine, as smart contracts allow the automatic execution of judicial agreements and sentences.

Pereira (2014) mentions that a contract is a bilateral legal transaction that requires consent. It must comply with legal requirements and, as a negotiable act, aims to achieve specific objectives. According to the author, a contract is "an agreement of wills, in accordance with the law, with the purpose of acquiring, protecting, transferring, preserving, modifying or extinguishing rights" or, in other words, "an agreement of wills with the purpose of producing legal effects".

Diniz (2014), in turn, states that a contract is "an agreement between two or more wills, in accordance with the legal order, with the objective of establishing a regulation of interests between the parties, with the purpose of acquiring, modifying or extinguishing legal relationships of a patrimonial nature".

According to Coelho (2016), a contract is defined as a bilateral or multilateral legal transaction that generates obligations for one or all parties involved, corresponding to rights held by them or by third parties. Therefore, there is no contract without the characteristic intention of legal transactions, since the intentional human conduct contained in the contract is the declaration of a will.

In general, Brazilian legislation does not impose a specific form for the execution of agreements. It arises from the general theory of contracts and from article 107 of the Civil Code that there will only be a specific form for a contract when the law expressly provides for it. Thus, as long as there is mutual agreement and it does not violate public order, the parties are free to draft contracts, including using programming language (USTER, 2021).

In turn, Brazilian courts recognize the importance of electronic contracts and, in particular, smart contracts, as can be seen in a recent decision of the Court of Justice of the State of São Paulo:

> It is important to emphasize that the technologies that involve smart contracts and electronic contracts, despite the modernity they bring and the need for a new interpretation of these legal relationships every day, do not imply a departure from the fundamental concepts of Private Law. Current issues, which are increasingly transformed due to the Communication Society, are the challenges that Law and Jurisprudence need to overcome in order not to be left behind (TRT-9th Region).

For these reasons, it is possible to recognize the acceptance of smart contracts by the Brazilian legal system as a new way of carrying out a bilateral legal transaction, always in accordance with the general theory of contracts and regulatory standards.

Therefore, there are positive and negative points in the adoption of *smart contracts* that contribute to the debate and evolution of the topic. Among the significant attractions are the efficiency generated by the instant conclusion and execution of the contract without the need for state intervention; the guarantee of compliance represented by the impossibility of one of the parties failing to fulfill its obligations; the reduction of disputes due to the drop in delinquency; the facilitation of e-commerce by eliminating the trusted third party in the business chain; the security provided by the high degree of accuracy in relation to the identity of the remote contractor (preserving anonymity); and the potential of smart contracts and blockchain to revolutionize the Internet of Things.

On the other hand, among the challenges and risks of adopting *smart contracts* are the integration of the entire society in the digital environment; the possibility of failure in the coding algorithm (albeit minimal); the impossibility of predicting all possible circumstances, which can lead to execution contrary to the will of the parties; bad faith in the preparation of the programming script; the deferred or continuous execution of a *smart contract* it may be

affected by factual or legislative changes; the impossibility, through current technology, of resolving subjective issues that affect the performance of the contract; be subject to the same defects of consent or capacity problems as traditional contracts; restriction of the performance of the Judiciary and its auxiliary bodies, resulting in the loss of the power of preventive protection and the reduction of the power of reparatory protection (*status quo ante).*

MITIGATION STRATEGIES

The Brazilian legal system can adopt several mitigation strategies to deal with the challenges and risks associated with *smart contracts*. These strategies aim to ensure legal certainty and the effectiveness of these contracts in the Brazilian context.

One of the strategies is the legislative update. The legislator can promote the updating of existing laws to specifically address *smart contracts*, establishing clear and appropriate rules for their use. This can include the legal definition of smart contracts, the determination of the formal requirements for their validity, and the regulation of specific issues related to the execution and resolution of disputes (Cavalcanti, 2020).

Additionally, courts can adopt a flexible interpretation of existing laws to accommodate smart contracts. This implies a broad interpretation of existing legal concepts, in order to cover smart contracts, as well as the application of general principles of law to resolve specific issues related to these contracts (TRT-9th Region).

The development of alternative dispute resolution mechanisms specific to *smart contracts*. Considering the automated and autonomous nature of these contracts, it may be necessary to create arbitration or electronic mediation mechanisms, as well as specialized courts or dispute resolution chambers dedicated to smart contracts (Cavalcanti, 2020).

It should be noted that international cooperation is fundamental. Given that *smart contracts* are a global technology, it is important to promote international cooperation to develop common standards and guidelines for their use. This may involve participation in international forums, the exchange of information and experiences with other countries, and the adoption of international conventions or treaties that address smart contracts (Cavalcanti, 2020).

These strategies, when adopted together, can contribute to mitigating the challenges and risks associated with *smart contracts* in the Brazilian legal system. It is important to emphasize that technological evolution is constant, and the legal system must be prepared to adapt and keep up with these changes (Cavalcanti, 2020).

BLOCKCHAIN SECURITY IN THE AGE OF QUANTUM COMPUTING

THE IMPORTANCE OF BLOCKCHAIN SECURITY

It is understood that the importance of using *blockchain* in the Brazilian judiciary is still limited and is in the experimental phase, not being widely adopted (ANDRIGHI, 2018). However, there are already some initiatives underway. In 2018, the Court of Justice of the Federal District and Territories (TJDFT) carried out a test of recording procedural information on a private blockchain, aiming to verify the effectiveness of the technology in judicial proceedings and ensure the authenticity of the information (ANDRIGHI, 2018).

In 2022, the Court of Justice of Santa Catarina (TJSC) developed the *LGPD JUS* application, which uses *blockchain* technology to ensure the security of user requests when validating their accounts (PORTO, LIMA JÚNIOR and SILVA, 2019). Another point that should be highlighted is that the Labor Court of the 3rd Region (TRT-3) recommended the use of *blockchain technology* for the registration of evidence in a case, and the TRT-2 recognized the registration of evidence on the *blockchain* as valid (GUSSON, 2020).

The National Council of Justice (CNJ) also launched the "Justice 4.0" platform in 2020, which allows the decentralized and secure registration and consultation of procedural data. The platform is in the testing phase and will be expanded to other courts in the future (ANDRIGHI, 2018).

In the private sector, the Azevedo Bastos Notary, in partnership with the start-up *OriginalMy*, offers digital authentication services to legal entities through a blockchain network (PORTO, LIMA JÚNIOR and SILVA, 2019).

Despite these initiatives, there is still much to be explored in terms of the potential and impact of *blockchain* technology on the Brazilian legal sector. Investment, development, and understanding of the topic are necessary so that blockchain can be widely adopted and used as evidence in the Brazilian judiciary (BURATTO, 2022).

POTENTIAL BLOCKCHAIN VULNERABILITIES AND APPROACHES TO STRENGTHEN SECURITY IN THE JUDICIARY

As for potential Blockchain vulnerabilities and approaches to strengthening, one of the main advantages is the greater possibility of intervention by the judicial system to maintain the balance of contracts. With the application of modern principles in contracts, it is necessary to humanize contractual relations and overcome outdated ideas based on liberal convictions, bringing the interest of the Social State in the regulation of contracts. This involves a weighing of the principles, where state intervention (social function of the contract) prevails over contractual freedom (autonomy of will).

In view of the numerous demands faced by the Judiciary, especially in Brazil, where there is a great deal of judicial demand, it is worth considering the implementation of technologies that enable a better functioning of the judicial system, with a focus on speed and the reinforcement of related constitutional principles, such as the reasonable duration of the process and speed.

Decree No. 10,332 instituted the Digital Governance Strategy, which is organized by principles, objectives, and initiatives, and one of these initiatives is *blockchain*. The fact that the Federal Government recognizes the importance and benefits of this technology, planning its creation and implementation as soon as possible, demonstrates its relevance.

In the legal world, it will be no different. The aforementioned decree, in its Objective 8, which deals with the public services of the future and emerging technologies, in initiative 8.3, provides that the federal government plans to make datasets available through blockchain solutions in the federal public administration by 2022. In initiative 8.4 of the same objective, on the implementation of resources for the creation of a blockchain network of the Federal Government that is interoperable, using reliable identification and secure algorithms.

The National Council of Justice (CNJ) issued Resolution No. 75/2009, which deals with public examinations for entry into the judiciary. In its Annex VI, letter F, it addresses Digital Law, highlighting the need for general notions of smart contracts, blockchain, and algorithms. This is just another demonstration of the relevance of *blockchain* in current times and, consequently, in Law. Given its proven value and the various areas in which it can be used and applied, it is necessary to analyze its application in order to incorporate it into different branches of law, seeking to make it feasible through its implementation.

GROWTH OF INNOVATIONS IN QUANTUM COMPUTING, BLOCKCHAIN, AND SMART CONTRACTS: AN ANALYSIS BASED ON THE FINDINGS OF BARON AND HOPPE (2018)

It should be noted that as we delve into the intricate relationship between quantum computing, blockchain, and smart contracts, the analysis in the study reveals profound implications of these innovations. Supported by the findings of Baron and Hoppe (2018), it highlighted how smart contracts and *blockchain* have reshaped practices in online operations, establishing a new paradigm for secure and decentralized transactions.

However, as we delve deeper into quantum computing, significant challenges emerge that threaten the security of these pioneering infrastructures become evident (Kappert, Karger, and Kureljusic, 2020). The rapid evolution of quantum computing poses a

concrete threat, requiring agile and proactive responses.

In this scenario, quantum cryptography emerges as a new tool, proposing a revolutionary approach to combat the risks posed by quantum computing (Ilie, Knottenbelt, and Stewart, 2020). Therefore, advanced methods offer an extra layer of protection, making it indispensable as we approach the quantum era.

Thus, the conclusions of our study (Macário, Morais, and Silva, 2022) raise a warning about the imminent challenges and the urgency of improved security strategies. The future of online operations holds countless possibilities, but it is vital that we are equipped to preserve the integrity of these innovations in the face of the uncertainties that lie ahead. Understanding the current context and available alternatives is critical to ensuring that the merits of *blockchain* and smart contracts are not obscured by the progress of quantum computing.

As we look to the future, it is relevant not only to continue, but also to expand our research. We must explore the robustness of quantum cryptography, understand the implications of quantum computing on frameworks such as blockchain, and furthermore investigate the potential vulnerabilities of smart contracts by considering new methods of protection.

The attention devoted to the potential of quantum computing and *blockchain* technology is growing every day. In Brazil, we can already observe initiatives such as the e-Citizenship Program and proposals for new laws, such as bill 1979/2022 and 1458/2022. These actions demonstrate a strong interest in developing regulations for these emerging technologies.

In the United States, laws such as the *National Quantum Initiative Act of 2018* (S. 3143) and the *Quantum Computing Cybersecurity Preparedness Act of 2022* (H.R. 7535) have been passed, arousing curiosity and encouraging studies in the field of quantum computing, as well as highlighting the importance of protecting these technologies.

The implementation of these legislative measures reinforces the need to take a precautionary and informed approach to ensure that innovations such as quantum computing and blockchain technology are utilized in a safe, efficient, and compliant manner with legal and regulatory guidelines. It is important to emphasize that this increase in knowledge does not mark the end of our journey, but rather the beginning of a trajectory in which we must delve into the universe of these technologies.

CONCLUSION

Blockchain *technology* has the potential to bring innovations to the field of Law in various relationships and situations. Throughout this article, the impact of this technology in the legal field was demonstrated, analyzing its advantages and highlighting the need to further explore its applications and use, especially in the face of the challenges of *smart contracts* in the age of quantum computing, another point was the analysis on the security of *blockchain* was also carried out.

It can be said that *Blockchain* emerges as a disruptive technology, making the presence of central intermediaries unnecessary for the realization of operations. As a result, the risks associated with dependence on intermediaries or their absence are suppressed by this decentralized, reliable and transparent system, which has been gaining prominence in the world, as well as in Brazil, in the legal system.

The expansion of *Blockchain* is inevitable as we move towards a future that is increasingly interconnected with technology. It works as a large globalized ledger, intrinsic to the development of new relationships, ensuring their security and transparency, thus allowing the Law to be operationalized in a concise way in digital relations.

Through the study, it can be verified that the legal feasibility of entering into *smart contracts* in the Brazilian legal system, highlighting its bilateral nature and the direct relationship with the development of *blockchain*.

The risks and benefits in adopting this contractual instrument were also addressed, contributing to the understanding of the topic. In view of all this, it is possible to conclude that *smart contracts* represent an evolution in the automation of contractual promises, with the potential to change, in the short term, the way contractual relationships occur in the legal system, bringing new parameters in law.

REFERENCES

1. Abijaudê, J. W., Greve, F., & Sobreira, P. de L. (2021). Blockchain e contratos inteligentes para aplicações em IoT, uma abordagem prática. In A. M. S. Andrade & R. S. Wazlawick (Orgs.), *40ª Jornada de Atualização em Informática (JAI 2021)* (pp. 1-12). Porto Alegre: Sociedade Brasileira de Computação. Disponível em: https://doi.org/10.5753/sbc.6757.3.4

2. Alchieri, E. A. P., Tomelin, L. R., Bessani, A. N., & Fraga, J. da S. (2011). Aspectos práticos sobre o consenso bizantino entre participantes desconhecidos. In *Workshop de testes e tolerância a falhas (WTF), 12, 2011, Campo Grande/MS. Anais [...]*. Porto Alegre: Sociedade Brasileira de Computação. (pp. 63-76). ISSN 2595-2684. Disponível em: https://doi.org/10.5753/wtf.2011.23090

3. Alecrim, J. S. C. (2019). *Análise crítica da sistemática de compras governamentais pela perspectiva de novas tecnologias de contratos inteligentes*. Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação. Brasília. Disponível em: http://bdtd.ucb.br:8443/jspui/handle/tede/2655

4. Andrighi, F. N. (2018). Blockchain e o Poder Judiciário: uma análise sob a perspectiva da segurança jurídica. *Revista de Direito, Estado e Telecomunicações, 12*(1), 609-624.

5. Bashir, I. (2017). *Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained*. Packt Publishing.

6. Blog TD SYNNEX. (2024). 7 principais mitos sobre Blockchain. Disponível em: https://blog-pt.lac.tdsynnex.com/7-principais-mitos-sobre-blockchain

7. Boechat, G. (2021). Contratações abertas: uma análise da Nova Lei de Licitações e Contratos Administrativos (n° 13.133/2021) à luz dos princípios de Governo Aberto. *Revista da CGU, 14*(25), 64-79. Disponível em: https://doi.org/10.36428/revistadacgu.v14i25.493

8. Brasil. Tribunal de Contas da União. (2020). TCU realiza estudo inovador sobre a tecnologia Blockchain e elabora guia para orientar os gestores. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/tcu-realiza-estudo-inovador-sobre-a-tecnologia-blockchain-e-elabora-guia-para-orientar-os-gestores.htm

9. Buratto, R. (2022). Blockchain e o Poder Judiciário: uma análise sob a perspectiva da segurança jurídica. *Revista de Direito, Estado e Telecomunicações, 12*(1), 643-658.

10. Cavalcanti, M. O. M., & Nóbrega, M. (2020). Smart contracts ou “contratos inteligentes”: o direito na era da blockchain. *Revista Científica Disruptiva, 2*(1), 98.

11. Chicarino, V. R. L., Jesus, E. F., Albuquerque, C. V. N., & Rocha, A. A. de A. (2017). Uso de blockchain para privacidade e segurança em internet das coisas. In R. C. Nunes, E. D. Canedo, & R. T. de Sousa Júnior (Orgs.), *XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2017*. Porto Alegre: Sociedade Brasileira de Computação. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/view/84/370/634-1

12. Coelho, F. U. (2016). *Curso de Direito Civil: Contratos* (Vol. 3). São Paulo: Editora Revista dos Tribunais.

13. Diniz, M. H. (2014). *Compêndio de Introdução à Ciência do Direito* (23. ed.). São Paulo: SaraivaJus.

14. Estados Unidos. (2018). *National Quantum Initiative Act of 2018*. S. 3143. Disponível em: https://www.congress.gov/bill/115th-congress/senate-bill/3143. Acesso em: 18 out. 2023.

15. Estados Unidos. (2022). *Quantum Computing Cybersecurity Preparedness Act of 2022*. H.R. 7535. Disponível em: https://www.congress.gov/bill/117th-congress/house-bill/7535. Acesso em: 18 out. 2023.

16. Fachini, T. (2023). *Smart contracts: o que é, como funciona e aspectos legais*. Disponível em: https://www.projuris.com.br/blog/smart-contract/. Acesso em: 6 mar. 2023.

17. Hidary, J. D. (2021). *Quantum computing: an applied approach* (2ª ed.). Cham: Springer.

18. Hattar, M. (2023). *DATA PROTECTION: How Quantum Computing Will Impact Cybersecurity*. Disponível em: https://www.securityweek.com/how-quantum-computing-will-impact-cybersecurity/. Acesso em: 10 jan. 2023.

19. Gusson, L. A. (2020). Smart Contracts: Uma Análise Jurídica. *Revista de Direito, Estado e Telecomunicações, 12*(1), 1-20.

20. Macário, L. M. A., Morais, M. M. S. de, & Silva, M. A. X. da. (2022). O advento da computação quântica e seus riscos para o paradigma blockchain/smart contracts. In M. C. B. Motta & M. A. M. Rezende (Orgs.), *Pensando as novas tecnologias* (pp. 15-32). Deerfield Beach, FL: Pembroke Collins.

21. Mattiello, F., Silva, G. G., Amorim, R. G., & Silva, W. B. (2012). Decifrando a Computação Quântica. *Caderno de Física da Universidade Estadual de Feira de Santana (UEFS)*, *10*(1-2).

22. Mello, U. (2018). Como a Computação Quântica Promete Revolucionar Nosso Conhecimento. Disponível em: http://idgnow.com.br/ti-corporativa/2018/05/06/como-a-computacao-quantica-promete-revolucionar-nosso-conhecimento/. Acesso em: 15 jan. 2024.

23. Mozelli, R. (2023). Cientistas dão primeiro passo rumo a computadores quânticos moleculares. Disponível em: https://olhardigital.com.br/2023/12/08/pro/cientistas-dao-primeiro-passo-rumo-a-computadores-quanticos-moleculares/. Acesso em: 12 jan. 2024.

24. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Technical report. Bitcoin Org. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 14 jan. 2024.

25. Nicolau, A. S. (2010). Computação Quântica e Inteligência de Enxames Aplicados na Identificação de Acidentes de uma Usina Nuclear PWR. *Dissertação de Mestrado em Ciências em Engenharia Nuclear*. COPPE, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro.

26. Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355-364. Disponível em: https://doi.org/10.1016/j.giq.2017.09.007. Acesso em: 14 jan. 2024.

27. Pereira, C. M. da S. (2014). *Instituições de direito civil*. Rio de Janeiro: Forense.

28. Porto, A. C. R., Lima Júnior, E. F., & Silva, P. A. (2019). Blockchain e a Autenticação de Documentos Eletrônicos: uma análise sob a perspectiva do Direito Notarial e Registral. *Revista de Direito, Estado e Telecomunicações, 12*(1), 625-642.

29. Revista Eletrônica do TRT-PR. (2023). Curitiba: TRT-9ª Região, *12*(118).

30. Savelyev, P. A., & Yavitz, A. Q. (2017). Analyzing Social Experiments as Implemented: A Reexamination of the Evidence from the Highscope Perry Preschool Program. *Quantitative Economics, 1*(1), 1-46.

31. Soares, M. J. (2024). O sistema de justiça na blockchain. Disponível em: https://www.conjur.com.br/2022-mar-30/porto-soares-justica-blockchain. Acesso em: 10 jan. 2024.

32. Tartuce, F. (2020). *Manual de Direito Civil* (Vol. único, p. 540).

33. Uster, L. (2021). *Contratos Inteligentes (smart contracts): possibilidade e desafios no ordenamento jurídico brasileiro* (1. ed.).