6

PUBLICUM

Blockchain in Contemporary Private Law: Perspectives from Brazilian Law

Guilherme Ramos de Morais
Universidade Federal de Minas Gerais-UFMG, Programa de Pós-Graduação em Direito, Belo Horizonte/Minas Gerais, Brasil. E-mail: guiramos123@gmail.com

Abstract
This article explores the potential uses of blockchain technology in contemporary private law, with a particular focus on the Brazilian legal system. The author lists the main characteristics of blockchain, as an incremental, immutable, and reliable chain of blocks, and its potential to reconfigure private relationships. The study examines the various ways blockchain applies to the legal sphere (smart contracts, corporate deliberations, DAOs, IoT, IIoT, asset tokenization, evidence production, and arbitration), especially under Brazilian civil law. The methodology consists of a qualitative and analytical approach, based on a critical literature review and a legal-dogmatic analysis of texts relevant to the topic, highlighting Bambara and Allen (2018) for the technical foundations of blockchain among other specialized references concerning its legal applications. The article demonstrates blockchain's transformative potential, offering a new paradigm of legal certainty and decentralized trust, capable of impacting everything from contract theory to supranational corporate structures.

Keywords
Law and Technology; Blockchain; Private Law; Decentralization; Trust.

Blockchain no direito privado contemporâneo: perspectivas do direito brasileiro

Resumo
Este artigo explora as potencialidades do uso da tecnologia blockchain no direito privado contemporâneo com especial enfoque no sistema legal brasileiro. O autor elenca as principais características do blockchain enquanto cadeia de blocos incremental, imutável e confiável, e seu potencial para reconfigurar as relações privadas. O estudo analisa as variadas formas de incidência do blockchain no direito (smart contracts, deliberações societárias; DAOs; IoT; IIoT; tokenização de ativos; produção probatória e arbitragem), todas analisadas sob a perspectiva do direito brasileiro. A metodologia consiste em uma abordagem qualitativa e analítica, fundamentada em revisão bibliográfica crítica de textos pertinentes ao tema, com destaque para a obra de Bambara e Allen (2018), que dispõe os

fundamentos técnicos do blockchain, além de outras referências especializadas no que diz respeito às suas implicações jurídicas. O artigo demonstra o potencial transformador do blockchain, que oferece um novo paradigma de segurança jurídica e descentralização da confiança, com capacidade para impactar desde a teoria contratual até estruturas societárias supranacionais.

Palavras-chave

Direito e Tecnologia; Blockchain; Direito Privado; Descentralização; Confiança.

Sumário

Introduction

Since the dawn of humanity, the problem of trust has been a central aspect of society. From census records (birth, death, marriage, population growth, and similar records) to the security of financial transactions (currency backing, authenticity, and value) and real estate dealings (certification of property boundaries, title registration), everything depends on the trust placed in something or someone to certify the accuracy of information. Trust is, therefore, the foundation of legal transactions in a broad sense.

It is well established that the protection of trust is not a recent phenomenon but a fundamental condition for social equilibrium and for the conclusion of legal transactions. Likewise, the mechanisms that guarantee trust are not new. In pre-Columbian South America, there was already a system of binary codes, akin to Boolean logic, whereby information could be expressed alternately as positive or negative (0 or 1). This was the Inca Khipu.

The word khipu derives from Quechua, the official language of the Inca Empire, and referred to a cord-based device used to record information of both statistical and narrative nature (Urton, 2003, p. 1). The Spanish colonizers initially did not know what this device was used for. The colonizer Hernando Pizarro reported that, when his crew took objects from an Inca warehouse, the person in charge of the records, the khipukamayuq (literally “knot maker” or “keeper”), untied some knots from his khipu (Urton, 2003, p. 3). Early colonial reports indicate that the Incas stored

vast amounts of information through this system, ranging from demographic censuses to ritual data, and from genealogical trees to resource organization (Urton, 2003, p. 3).

The khipu itself consisted of a central (primary) cord to which secondary cords were attached (Urton, 2003, p. 4). On each secondary cord, additional subsidiary knots were tied, and so on (Urton, 2003, pp. 4–5). The association between knots and empty spaces was interpreted through a symbolic system that extracted numerical or linguistic information from the structure of the khipu (Urton, 2003, p. 5). It was the duty of the khipukamayuq, the central authority, to ensure the security, reliability, and immutability of the information (Urton, 2003, p. 3).

Centuries after the khipu, humanity conceived more advanced mechanisms for storing information, although methods relatively similar to those adopted since the Inca period continue to be used. Among these mechanisms (technologies), blockchain stands out. Much like the khipu, it consists of an incremental chain of blocks, characterized by its immutability and reliability. However, unlike the Inca technology, information sharing has evolved to such an extent that *trust* can, in the traditional sense of blockchain, be conferred upon the collective of users in a decentralized virtual environment. This technology has the potential to transform private relations, from the protection of elements inherent to human personality to complex transnational corporate arrangements.

This article seeks to examine the potential applications of blockchain technology across its diverse manifestations within the contemporary legal system, especially under Brazilian civil law. To this end, the paper is structured as follows: an introduction; an analytical overview of the technical foundations of blockchain, including its core concepts, main typologies, and operational advantages and limitations; and a discussion of its legal applications—particularly in the context of smart contracts, corporate governance and deliberations, decentralized autonomous organizations (DAOs), the Internet of Things (IoT) and the Industrial Internet of Things (IIoT), asset tokenization, digital evidence, and arbitration. The paper concludes with final remarks reflecting on the broader implications of blockchain for legal theory and practice.

The methodology adopted in this article follows a qualitative and analytical approach, based on a critical literature review and a dogmatic-legal analysis. Regarding blockchain technology, its main features, and technical elements, the analysis draws primarily on the work of Bambara and Allen (2018). For the remaining topics, specialized references pertinent to each specific area were employed. The legislative analysis, in turn, focused on the Brazilian legal framework, especially regarding private law. Within these methodological limits, the study adopts a deductive perspective to examine how emerging technologies may interact with traditional legal categories.

As part of an ethical and transparent approach to the use of artificial intelligence, it is prudently noted that grammatical revision and suggestions for possible stylistic improvements

were performed with the assistance of generative AI tools, such as GPT-4.5 and Gemini AI Pro 2.5. No generative artificial intelligence was used to replace the author's intellectual contribution. The ethical and responsible use of these tools was strictly limited to the revision of content originally produced by the author, as instruments in the service of human productivity.

1. The structures and main characteristics of blockchain technology

This chapter presents the fundamental aspects of blockchain technology. Accordingly, it addresses, in this order, foundational concepts, the main typological forms of its application, and its operational advantages and limitations. These elements are essential for the doctrinal reflections presented in the subsequent chapters.

1.1. Fundamental Concepts

Initially proposed by Satoshi Nakamoto (2008), blockchain is a form of information storage based on a chain of interconnected blocks.1 For each new block to be added to the chain, all preceding encrypted blocks must be validated (Bambara & Allen, 2018, p. 1). Once a block has been inserted into the chain, retroactive modification of the information contained in any previous block is not permitted (Bambara & Allen, 2018, p. 2). In the classical conception of blockchain, the verification of data accuracy is carried out by the users of the chain themselves, thereby eliminating the need for a traditional central authority (Bambara & Allen, 2018, p. 2; Pimenta, 2023, pp. 222–223).2

From these initial considerations, the fundamental elements that characterize blockchain can be identified: (i) the existence of isolated, encrypted units for storing information (blocks);3 (ii) the correlation among blocks within a procedural chain;4 (iii) the decentralization of

[1] According to Pimenta (2023, p. 222), blockchain emerged as a means of addressing the trust problem underlying Bitcoin. Indeed, although this technology effectively enables the operation of Bitcoin, it is by no means limited to this application, as will be examined below.

[2] Pimenta (2023, p. 219) summarizes the classical problem of managing security mechanisms through the Byzantine Generals Problem. Allegorically, it envisions a scenario in which several Byzantine generals must coordinate an attack or a retreat. However, there is no effective way for them to communicate, and worse, there is the possibility that one of them may be a traitor. Thus, the challenge lies in establishing a consensus without centralizing decision-making in any single general, while still ensuring the reliability of the information provided by each of them.

[3] Each block has a specific storage capacity. Once that capacity is reached, the block is added to the chain of blocks (Moreira, Delgado & Santos, 2021, p. 28). The process of validating the information contained within the block is, in turn, commonly known as mining (Moreira, Delgado & Santos, 2021, pp. 29–30).

[4] Each block refers to the preceding one, known as the parent block, through a unique identifier called a hash (Moreira, Delgado & Santos, 2021, p. 32). In this way, an authentic chain of blocks is formed. Its structure is described as procedural because the chain is in constant formation, without a predefined format.

the verification process concerning the integrity of the blocks and, consequently, of the chain itself;5 and (iv) the exponential increase in processing power required as the chain expands.6 As the central purpose of this article is not to provide an exhaustive account of the technical elements of blockchain, the explanations provided so far are sufficient to support the subsequent analysis.

1.2. Blockchain Typologies

As explained by Moreira, Delgado and Santos (2021) and by Bambara and Allen (2018), the types of blockchain vary according to the architecture of the information validation process among users. Accordingly, three main types of blockchain have emerged: public, private, and permissioned.

Public blockchain functions both as a public database and as a publicly accessible software, while preserving the fundamental principles of blockchain, such as the decentralization of information certification, cryptography, content immutability, and processing scalability (Bambara & Allen, 2018, pp. 13–14).7 In a public blockchain, anyone can have broad access to the network, and can also act as a node, namely, a participant responsible for validating information. In this model, all users collectively take part in the validation and access of encrypted data. Its main application lies in cryptocurrencies. Due to its characteristics, the public blockchain most closely aligns with Satoshi Nakamoto's (2008) original proposal, as observed by Bambara and Allen (2018) and Pimenta (2023). It is, in fact, the model most widely employed for digital currencies (Catchlove, 2017, p. 4). The private blockchain, in turn, is characterized by restricted access and modification permissions granted only to specific users. In other words, individual authorization is necessarily

[5] The decentralization of data validation is a fundamental aspect of blockchain operation. The revolutionary nature of this technology, in terms of information storage, lies precisely in the absence of a central validation authority. This is why Satoshi Nakamoto (2008) described it as a peer-to-peer network. However, this element is partially overcome by variations of the traditional blockchain model, such as private and permissioned systems.

[6] To validate a new block, all previous transactions must also be verified, starting from the genesis block (Moreira, Delgado & Santos, 2021, p. 29). For this validation to occur, different consensus mechanisms (validation techniques) are employed, such as proof of work (solving complex mathematical problems), proof of stake (validation according to the quantity or attributes of the information), and proof of authority (validation carried out by specific authorities, usually in private or permissioned blockchains). The longer the chain, the greater the validation time and the computational power required for its execution (Moreira, Delgado & Santos, 2021, p. 30). This model, which demands a constant increase in computational power, is among the key elements ensuring the immutability and security of this technology.

[7] The authors illustrate the functioning of public blockchain by referring to cloud storage programs such as Dropbox. This example, however, is problematic because, as the authors themselves emphasize, for a system to qualify as a public blockchain, it is not enough that all users have access to the information. It is also necessary that no central authority exists to validate the data, hence the need for data encryption, and that information can only be added following the established insertion protocol, meaning that deletion is not permitted. In the case of Dropbox, data may or may not be encrypted; information may or may not be deleted; and there is, unquestionably, a central authority: the Dropbox platform itself. Therefore, shared cloud storage technologies, when encrypted, more closely resemble a permissioned or private blockchain.

granted by a central authority (Bambara & Allen, 2018, p. 14; Catchlove, 2017, p. 4). This type of blockchain is primarily adopted by banks, corporations, and state institutions (Catchlove, 2017, p. 4).

The permissioned (or consortium) blockchain is one in which a central authority distributes the consensus mechanisms among users (Bambara & Allen, 2018, p. 14; Catchlove, 2017, p. 4). Each user holds part of the verification mechanism delegated by the central authority. Once new information is jointly validated by these users, it is added to the chain. By combining features of both public and private blockchains, this model is referred to as partially decentralized (Bambara & Allen, 2018, p. 14). This type of blockchain is the one widely used in collaborative arrangements among nations at the diplomatic level (Catchlove, 2017, p. 4).

1.3. Operational Advantages and Limitations of Blockchain

Following the discussion of blockchain's operational foundations and structural types, its advantages can be summarized in two main attributes: immutability and auditability. Regarding its immutability, the storage of encrypted information in blocks that are verified in a decentralized manner makes any alteration of the chain virtually impossible. The attribute of immutability is fundamental to financial operations. Indeed, Bambara and Allen (2018, p. 5) justify the very existence of blockchain as a means of improving the financial system, in which transactions must be extremely faithful to reality, both with respect to the value of the currency itself and to the amount of currency necessary to execute a transaction. [8] Such immutability has profound legal and institutional implications, as it directly addresses the fundamental problem of trust.

Indeed, it constitutes a genuine mechanism for solving the problem of trust *ex ante*. Unlike the *ex post* perspective, in which the legal system generally treats trust in a repressive manner, as a consequence of the breach of obligations between economic agents (Pimenta, 2023, p. 203). This can be corroborated by Article 389 of the Brazilian Civil Code: if the obligation is not fulfilled, the damage must be compensated. This occurs even when trust governs the legal relationship between the parties (as can be observed in the postulate of objective good faith, Article 113 of the Brazilian Civil Code, including its related duties of information, protection, loyalty, and cooperation).

[8] It is not that altering the chain is strictly impossible. Moreira, Delgado, and Santos (2021, p. 42) and Lima and Neto (2021) indicate that powerful computers may surpass the processing capacity of the entire chain, which would allow its rewriting. It is also possible for a bifurcation (fork) to occur in the chain, enabling the creation of parallel chains (Moreira, Delgado, and Santos, 2021, p. 42). However, this second case is not originally conceived for altering the information within the chain, but rather to correct a possible error in certain blockchain architectures that make it possible for information to be duplicated due to a flaw in the chain's format.

However, blockchain technology solves the problem of trust *ex ante*[9] in a decentralized manner. In this sense, *blockchain* is a transformative force in the structure of legal transactions. Susskind's (2017, pp. 33–38) argument is particularly relevant, as he argues that technology is one of the main driving forces of change in the legal sector.

Related to the attribute of immutability, the blockchain, in its traditional public form, is widely accessible to all users (nodes), allowing any user to verify the authenticity of each piece of information individually. It is, therefore, an auditable technology, which tends to reinforce the trust placed by users. However, it is not a technology immune to failures or manipulations, and for external observers without access to the cryptographic key, accessing the information is virtually impossible.

The blockchain infrastructure has raised important questions, particularly regarding scalability and privacy. Starting with scalability, criticisms about the blockchain's energy consumption are often raised. Ok, Barnty, and Joseph (2025) point out that energy consumption tends to vary according to the consensus mechanism employed. According to these authors, among the three mechanisms mentioned in footnote 6 (proof of work, proof of stake and proof of authority), proof of work has a high level of energy consumption (used in Bitcoin); proof of stake has a low level of energy consumption (also according to Bambara & Allen, 2018, p. 120) (used in Ethereum 2.0)[10]; and proof of authority has a very low level of energy consumption (used in Hyperledger). In the case of Bitcoin, which uses the most energy-intensive consensus mechanism, the estimated annual consumption up to 2025 ranged from 100 to 150 TWh (terawatt-hours, or 10^{12} Wh) (Ok, Barnty and Joseph, 2025, p. 9), equivalent to about 20% of Brazil's total energy consumption in 2023 (see 2024 report, base year 2023; Brazil, 2024).[11] In comparison, the entire global banking system consumes 263 TWh (Ok, Barnty and Joseph, 2025, p. 9). In other words, a single digital currency alone accounts for nearly 50% of the energy consumption of the world's banking system and 20% of Brazil's annual energy consumption.

[9] The blockchain is not the only *ex ante* approach to the problem of trust. As explained by Pimenta (2023, pp. 205-210), financial institutions and certification authorities in a broad sense (i.e., an entity that validates transactions, such as a notary's office, for example) also intervene in legal relationships to ensure the authenticity of transactions. This form of intervention in private relationships, however, corresponds to the traditional model, which is distinct from the decentralized model of blockchain

[10] Initially, Ethereum used the proof-of-work mechanism. However, after its migration to proof-of-stake in 2022, its energy consumption decreased by 99.9% (Ok, Barnty and Joseph, 2025, p. 10).

[11] Other analyses, such as that of the Cambridge Bitcoin Electricity Consumption Index, estimate that annual energy consumption is around 225 TWh. Data from this research also indicate that the mining efficiency of bitcoins has decreased sharply over the years, confirming the exponential increase in the difficulty of mathematical operations required for validating and adding new information to the blockchain (Cambridge Centre for Alternative Finance, 2025). Therefore, since the beginning of the historical series, energy consumption has increased while mining efficiency has decreased, showing a clear inverse proportional trend.

Regarding privacy, traditional blockchain technology is partially incompatible with the protection of personal data.[12] As explained by Moreira, Delgado, and Santos (2021), the absence of a central authority effectively eliminates the figure of the data controller, which is essential for the governance and management of personal information. Furthermore, as stated by Bayle et al. (2018), reconciling a public blockchain network with personal data protection can only be achieved either through the complete encryption of data, a feature inherent to the traditional blockchain model, or through the implementation of an external controller, a solution that alters the original decentralized nature of the system and brings it closer to permissioned or private network structures.

Thus, the main concepts related to blockchain have been presented, particularly concerning its structure, typologies, and operational advantages and limitations. These elements tend to recur throughout the specialized literature on the subject.

2. Applications of Blockchain in law

Having outlined the fundamental concepts of blockchain, the discussion now focuses on how this technology is capable of reconfiguring traditional legal institutions of private law (such as contracts and corporations) and public law (including procedural, registral, among others).

2.1. Smart Contracts

Smart contracts have two main characteristics: their conclusion in a digital environment[13] and the self-executability of contractual obligations. One relates to the contractual instrument, while the other pertains to the performance of obligations. It is on these theoretical premises that McKinney (2018, p. 321) established his concept of smart contracts, namely, self-executing agreements in which the parties, through reciprocal exchanges of promises or performances, are bound by a transparent set of rules previously defined in an electronic environment.

[12] An even more controversial matter concerns the right to be forgotten, whether in its erasure or rectification aspect. A solution addressed by Costa (2021, pp. 190–191), with reference to French data protection law, would be the possibility of destroying private cryptographic keys, which would render inaccessible the data encrypted by public keys within a decentralized blockchain network. The author additionally proposes the use of the bifurcation (forking) technique, as discussed in footnote no. 8, whereby a new and separate branch of the blockchain could be created to isolate or neutralize specific records.

[13] The mandatory digital format is the reason why the examples provided by Andrade and Colombi (2021, p. 21) as smart contracts are imprecise. Andrade and Colombi cite as examples of smart contracts those involving the automated execution of obligations, such as vending machines, the use of tokens in public telephones, and the distribution of water in Egyptian temples. However, self-executability constitutes only one of the cumulative requirements of smart contracts, which therefore exclude the application of these historical examples to the modern concept of smart contracts.

From a substantive standpoint, the smart contract possesses the requirements inherent to contracts in general: offer, acceptance, consideration, intent to contract, capacity, and lawful object (McKinney, 2018, p. 323; Andrade & Colombi, 2021, p. 27). The distinguishing element, however, lies in the contractual instrument and in the digital execution of the agreement. The following discussion explores how these traditional contractual elements are reinterpreted and operationalized in the digital setting of smart contracts.

Regarding the contractual instrument and its form, smart contracts consist of translating the parties' intent into an electronic format through the use of blockchain principles (Catchlove, 2017, pp. 6–7). In other words, each interaction with the contractual instrument depends on the use of a digital signature or key (Catchlove, 2017, p. 7). Thus, by leveraging blockchain's immutability attribute, contractual terms exhibit a rigid structure and demand high levels of linguistic precision (Catchlove, 2017, p. 9). However, the high level of certainty attributed to computational language is fictitious. Smart contracts translate the parties' declarations of intent into computational language, which, in turn, are expressed in natural language (spoken, written, read, and heard). Therefore, every linguistic expression is subject to interpretation, even those that rely on the classical Boolean model.[14]

If no specific form is legally required, except for public deeds involving real estate worth more than thirty times the current minimum wage, as provided by Article 108 of the Brazilian Civil Code, there is no formal obstacle to executing smart contracts under Brazilian law. In general, the rule is freedom of form, and formal solemnity is the exception, which is consistent with the smart contract model.[15]

The second defining feature of smart contracts lies in their self-executing nature. However, self-execution is not a feature exclusive to smart contracts. For at least two centuries, negotiable instruments have dealt with the self-enforceability of obligations, as in the case of credit instruments backed by an underlying contract, such as commercial invoices (*duplicatas*) and promissory notes. Due to the negotiable nature of such instruments and the separation of their enforcement from any discussion of the *causa debendi*, mere nonperformance authorizes the creditor to enforce the credit. In this specific example, the execution depends on the direct intervention of third parties, which distinguishes it from smart contracts.

[14] As stated by Alves, Kobus, and Fawaz (2021, p. 94), smart contracts are not exempt from ambiguities. On the contrary, computational language presents its own limitations, much like natural language: future uncertainties, disagreements over the content of the code, among other aspects highlighted by the authors.
[15] The subjective elements of will remain fully applicable to smart contracts, especially the classical defects of legal transactions (mistake, ignorance, deceit, coercion, lesion, and fraud) as set forth in Articles 138 to 165 of the Brazilian Civil Code, as well as the grounds for invalidity of legal acts provided in Article 166 and so on.

There is, however, a classic example of self-execution independent of third-party intervention: the penitential earnest money (penitential deposit) provided in Article 417 of the Brazilian Civil Code. When the contractual obligation is not performed, the party who received the arras retains them, and the contract is thereby terminated (Article 418, I, of the Brazilian Civil Code). In other words, in the event of contractual nonperformance, the creditor is immediately compensated.[16] Hence, self-execution is not, in itself, an element exclusive to smart contracts.

In fact, the self-executing nature of smart contracts is characterized by two elements that distinguish it from the traditional forms of self-execution mentioned above: the algorithmic enforcement of the consequences of nonperformance and the absence of any need for third-party intervention. The logic of smart contracts is objective: once event x occurs, consequence y automatically follows (Catchlove, 2017, p. 8; Alves, Kobus & Fawaz, 2021, p. 88).

Related to the algorithmic aspect of the contract, blockchain enables decentralization in the authorization and validation of transactions: the authority of validation is assigned to consensus mechanisms (Catchlove, 2017, p. 3).[17] This model allows transactions to occur anonymously (Catchlove, 2017, p. 4), which, in theory, would violate the validity requirement of legal transactions concerning the verification of a capable agent (Article 104, I, of the Brazilian Civil Code). However, such a violation would exist only in theory, for two main reasons: public blockchains do not necessarily operate under anonymity, and it is possible for the chain itself to verify the integrity of a node's capacity if such capacity functions as a prerequisite for participation in the network.[18] In other words, there would be a consensus among the blocks that all nodes in the chain are operated by capable agents. This would not, strictly speaking, be a violation of Article 104, I, of the Brazilian Civil Code. The agent is capable, the demonstration of that capacity that becomes more complex, though still valid.

This eminently hypothetical scenario merely illustrates the limits of contractual theory discussions in areas that remain underexplored in the literature on smart contracts. However, in ordinary situations, smart contracts aim to reduce transaction costs (Alves, Kobus & Fawaz, 2021, p. 85), not to increase them by introducing risks that previously did not exist, such as enabling transactions between anonymous parties in a blockchain environment.

[16] On this point, it is appropriate to note that penitential earnest money constitute an actual form of compensation. This understanding is well established in the case law of Brazilian higher courts. For example, see REsp No. 1,669,002/RJ (Superior Court of Justice, Third Panel, Rapporteur: Justice Nancy Andrighi; Judgment on September 21, 2017; Publication on October 2, 2017).

[17] In turn, related to this aspect, the immutability of blockchain prevents the terms agreed upon by the parties from being unilaterally modified by either of them or by malicious third parties.

[18] Here lies the importance of a typological analysis of blockchain models, such as the one in Subsection 2.2, as it allows for the identification of issues of this nature and the indication of possible solutions directly related to contract law.

Another sensitive issue inherent to the theory of contractual breach concerns contract revision. According to the classical doctrine of frustration (doctrine of impracticability), unpredictable factors that disrupt the contractual balance may allow flexibility of the *pacta sunt servanda* principle through the addition of the *rebus sic stantibus* clause. In the context of smart contracts, such flexibility is particularly difficult to achieve, mainly due to the emphasis on the immutability of contracts. Once the term has been negotiated and established, its modification becomes exceedingly difficult.

Considering these aspects, the application of the doctrine of impracticability to smart contracts could occur through a prior algorithmic configuration allowing for contractual suspension in unforeseen situations that significantly affect the balance of the agreement between the parties. Even in the absence of such a provision, it would be the duty of the state authority to correct any distortions, even if the contract has already been fully executed in virtual environment.

Given these considerations, the elements presented above indicate that nontraditional form and execution constitute the qualifying aspects of smart contracts.[19] Accordingly, these are the elements that tend to affect theories of contract law and, most notably, theories concerning contractual (non)performance.

2.2. Corporate Law and Deliberations

In corporate law, one of its possible applications lies in shareholders' meetings and meetings of partners or the board of directors, notably in the annual general meeting (AGM). Regarding the AGM, Lafarre and Elst (2018, p. 8) indicate that it serves a threefold function for shareholders: as a means of information (information function), as a forum for discussion (forum function), and as a mechanism for decision-making (decision-making function). According to the authors, this format has remained unchanged for centuries. Blockchain technology integrates into the context of AGMs through the model of private blockchains (accessible only to shareholders), with potential application in all the listed functions (pp. 15–16).

Among the benefits indicated by Alves, Kobus, and Fawaz (2021, pp. 91–93) and Lafarre and Elst (2018, pp. 15–18) are: (a) the reduction of opacity; (b) the decrease in bureaucracy regarding the need to publish corporate acts in widely circulated media; (c) the reduction of transaction costs related to decision-making; (d) the decrease in behaviors aimed at circumventing legally required

[19] Brazilian Bill No. 4/2025, which addresses the reform of the Brazilian Civil Code, has appropriately employed the concepts related to smart contracts presented throughout this article. The draft clearly states that "Smart contracts are those in which some or all contractual obligations are defined or executed automatically by means of a computer program, through the use of a sequence of electronic data records, ensuring the integrity and accuracy of their chronological order."

procedures, especially those related to quorum; and (e) the immutability of corporate records. On the other hand, the use of blockchain in corporate deliberations tends to undermine the very purpose of such deliberative meetings, namely, deliberation itself.

There is, therefore, a need to balance the binomial Speed vs. Deliberation in corporate assemblies. As can be seen from Article 1.072, head clause, of the Brazilian Civil Code, the purpose of the shareholders' meeting is to enable decision-making, which presupposes the need for deliberation, a process that, in turn, includes a dialogical aspect. However, the same Code waives dialogicity in Article 1,072, §3, which, through extensive interpretation, could be applied to decisions made in a blockchain environment. Nevertheless, the risk of dispersing decision-making power may give rise to the phenomenon of vetocracy, which will be addressed in the following subsection.

2.3. Decentralized Autonomous Organizations

Among the new forms of arrangements between individuals made possible by blockchain are Decentralized Autonomous Organizations (DAOs). These are corporate arrangements created through smart contracts that operate on blockchain technology (Costa & Marques, 2019, p. 64).

Blockchain technology enables individuals to organize themselves into unprecedented, creative, efficient, and community-based arrangements. It is within this open-source-inspired collaborative model that these organizations emerge (Brummer & Seira, 2022, p. 3). With the use of smart contracts, the relationship among members and the organization's own decision-making processes reaches levels of automation uncommon in traditional corporate structures (Brummer & Seira, 2022, p. 3). Moreover, since there is generally no legal framework to formalize and institutionalize these arrangements, participants tend to adopt pseudonyms (Brummer & Seira, 2022, p. 3).

From the simple identification of the defining elements of DAOs arise questions concerning legal personality and civil liability. Given that the purpose of this specific organizational arrangement is to promote the greatest possible fluidity and dynamism in business relations, and since there is no predetermined legal form, its configuration within the Brazilian legal system corresponds to that of a non-incorporated partnership. Among unincorporated entities, DAOs appear to align most closely with unregistered partnerships whose existence vis-à-vis third parties may be proven by any means, with unlimited and joint liability among partners (Articles 986 to 990 of the Brazilian Civil Code).

Nothing prevents other corporate structures from being adopted by DAOs, as proposed by Brummer and Seira (2022). The caveat, however, is that traditional arrangements (such as simple

partnerships, limited liability companies, and corporations) contain elements that are, to some extent, incompatible with the DAO model, particularly the nominal or potential identification of their members. This argument is reinforced by the fact that, due to the decentralization inherent to blockchain, DAOs transcend borders, making it difficult to determine the applicable legal system governing the organizational arrangement itself and its participants (Bambara & Allen, 2018, p. 97).

The difficulty of applying traditional corporate models to DAOs became evident in the emblematic case of CityDAO. This phenomenon began with the enactment of Wyoming's Decentralized Autonomous Organization Supplement (Senate File 38) in July 2021, which made it possible to adopt the limited liability company structure for DAOs in the State of Wyoming. A few months later, on October 29, 2021, CityDAO, a company, purchased a 160,000-square-meter plot of land in Wyoming, called Parcel 0 (Taken, 2022). Essentially, ownership rights were registered in the name of CityDAO, but the rights of use and enjoyment of the property were tokenized (Taken, 2022). Each small virtual fraction of the property was designated a plot, which users could acquire by purchasing the tokenized asset on the blockchain (Taken, 2022). From then on, decisions concerning the virtual city became subject to deliberation within the blockchain ecosystem, and token holders symbolically regarded themselves as citizens of the virtual city (Jean, 2023).

However, within this virtual city model, subsequent problems emerged that serve to illustrate the governance limitations of DAOs. In May 2022, CityDAO was the target of a hacker attack due to vulnerabilities in the social network Discord (Crawley, 2022). Essentially, the hacker, impersonating the city's administrator responsible for land sales, announced a sudden price reduction for parts of the property, leading users to transfer their tokens to the hacker instead of the legitimate administrator—causing losses of nearly USD 100,000 (Crawley, 2022). Another problem arose later: due to the large number of users, governance of the crypto-city became virtually impossible from the standpoint of individual voting influence. In other words, high quorum thresholds were required for decision-making, which gave rise to the phenomenon of vetocracy, in which groups of users lack decision-making power due to the dispersion of voting power (Rong & Mao, 2023, p. 16). Thus, as Rong and Mao (2023, p. 16) suggest, DAOs may ultimately increase coordination costs. As previously exposed in Subsection 3.1, the subjacent idea of *blockchain* is to reduce transaction costs, not increase them. This example illustrates a concrete scenario in which blockchain poses an economic rebound effect.

The elements presented in this subsection indicate that, although DAOs appear to be a promising organizational arrangement due to the efficiency of the open-source model, this very model can give rise to serious governance problems which, if not properly addressed, may render the management of the organization itself unfeasible.

2.4. Internet of Things (IOT)

Analogous to smart contracts — which consist of applying blockchain to virtually self-executing contracts — the application of blockchain to property itself has become popularized as smart property. This concept is directly related to the Internet of Things (IoT)[20], that is, the connection of physical objects to the internet, especially for purposes of home or urban automation (Bambara & Allen, 2018, p. 42).[21] Pimenta (2024, p. 46) adds that interconnected objects must operate in the cloud so that they can receive and send instructions to other connected objects.

The use of blockchain in *smart properties* reinforces the positive attributes of the blockchain itself. Starting with security, blockchain minimizes the risks traditionally associated with the centralization of information processing in smart devices (Silva; Teixeira & Santana, 2021, p. 227). Consequently, it facilitates the very verification of the identity of the device with which the network communicates (Silva; Teixeira & Santana, 2021, p. 227). Blockchain also provides security for the information stored in or produced by these devices, particularly due to the immutability attribute of the *block chain*, a feature previously discussed. Furthermore, blockchain promotes the decentralized interoperability of smart devices, including for the automated execution of smart contracts (Silva; Teixeira & Santana, 2021, p. 228).

Mercan and Akkaya (2021) indicate that blockchain can turn devices connected to the IoT into genuine autonomous economic agents. In what is known as the machine-to-machine (M2M) economy, interactions between devices of various kinds enable the decentralization of microeconomic transactions, especially in cryptocurrencies (Mercan & Akkaya, 2021). Examples include autonomous electric vehicles that pay for their own charging or tolls, refrigerators that automatically request item restocking, among others (Mercan & Akkaya, 2021, p. 119).

However, there is currently no specific regulatory framework on this topic in Brazilian law. In such cases, the regulation of smart properties spans three distinct yet interconnected legal frameworks. The first is the General Data Protection Law (LGPD, Federal Law no 13.709/2018), which governs the large-scale collection of data necessary for blockchain operation within the IoT context. The second is the Internet Civil Framework (Federal Law No. 12.965/2014), which defines the responsibilities of providers and applications, as well as connection and access retention, all essential aspects of IoT. Finally, there is the adaptation of general contract theory and property

[20] A concept that, according to Silva, Teixeira, and Santana (2021, p. 210), was first introduced in 1999 by Kevin Ashton, co-founder of the MIT Auto-ID Center, during a presentation on the industrial application of this technology.

[21] The context of integration between technologies arising from computing and the internet for the production or distribution of goods and services is what has popularly come to be known as the Fourth Industrial Revolution or Industry 4.0 (Pimenta, 2024, p. 45).

law to the particularities of this unprecedented legal phenomenon. It is, therefore, a field that demands extensive dogmatic study.

Considering that different blockchain models can be integrated into IoT, the problems inherent to each type of model also extend to it. For instance, a centralized blockchain model poses greater security risks (when compared to a decentralized one), as well as higher costs for device integration and interoperability issues (Silva; Teixeira & Santana, 2021, p. 218). In other words, although integrating blockchain with IoT offers several advantages, specific risks tend to arise depending on the type of blockchain implemented in the integration of smart devices.

2.5. Industrial Internet of Things (IIOT)

Analogous to IoT, the application of the concepts discussed in the previous subsection (interconnection of objects to the internet using cloud technology) to industry in the strict sense has been termed the Industrial Internet of Things (IIoT) (Pimenta, 2024, p. 45). Thus, in IIoT, the network of cloud-connected objects operates to manage production or distribution chains for goods and services (Pimenta, 2024, p. 46).[22] Among the advantages directly associated with applying blockchain to production chains are the reduction of agency conflicts, since decision-making is transferred from corporate management to the machines themselves, reduction of raw material waste and energy consumption with maximized machinery use, reduced default rates, and increased worker safety (Pimenta, 2024, p. 48).

A critical issue, however, concerns liability for damages caused to third parties in fully automated production chains (Pimenta, 2024, p. 48). As Frazão (2019, pp. 505–506) points out, the civil liability of managers persists for automated decisions. Although the author refers, in that particular paper, to automated decisions within artificial intelligence contexts, the conclusions seem equally applicable to IIoT. Denying the liability of managers would encourage "organized irresponsibility," effectively creating a genuine exemption from liability (Frazão, 2019, p. 505). In the case of IIoT, by analogy to Frazão's analysis (2019, p. 506), the adoption of automation technologies via blockchain could follow a *culpa in eligendo* liability regime, that is, liability arising from a breach of the duty of diligence and care.

Automation technologies serve merely as facilitators for industrial activity and must therefore be subject to constant human oversight, both in the selection of the technology (in a preventive manner) and its actual use. Another possible approach to this issue, as suggested by

[22] This concept, as presented by Pimenta (2024), reveals that IIoT and smart factories are defined by the strict concept of enterprise set forth in Article 966 of the Brazilian Civil Code, namely, an organized economic activity aimed at the production or circulation of goods or services.

Pimenta (2024, pp. 53–54), would be to apply liability for harm caused by things, as provided in Articles 936 to 938 of the Brazilian Civil Code. It is also possible to apply liability for harm caused by defective products or services (Articles 12 to 17 of the Consumer Protection Code) in cases involving harm to consumers in the legal sense, that is, any person who purchases or uses a product or service as the final recipient (Article 2 of Brazilian Federal Law No. 8.078/1990).

Therefore, the IIoT raises relevant issues, especially in terms of liability in the exercise of business activity.

2.6. Asset Tokenization

Tokenization consists of the process of transforming assets into negotiable computational units. According to Bambara and Allen (2018, p. 36), a digital token is the conversion of a physical asset into a digital asset with the possibility of subsequent conversion into physical or fiat currency. Regarding the tokenization of securities, the application of blockchain technology to these assets aims to enable third-party participation in the company's own routine, in addition to serving as a means to facilitate agreements between shareholders and entrepreneurs for the management of dividends (Alves, Kobus & Fawaz, 2021, p. 93).

Another form of applying asset tokenization through blockchain is through sale of tokens (token sales or initial coin offerings). As Pimenta (2023, p. 266, author's translation) explains:

> The initial coin offering begins with the description of a project for which resources are to be raised, all in a digital document called a White Paper. This document circulates on the internet to attract investors. If there is interest, the investor does not obtain securities, but rather tokens, which confer rights in relation to the investment recipient.

Although similar to the crowdfunding model, the sale of tokens is not identical to it. In crowdfunding, there are centralized platforms that manage operations and issue securities; whereas in token sales, trust is decentralized (i.e., there is no central authority) (Pimenta, 2023, p. 267). It therefore resembles the futures commodities market more closely than crowdfunding (Pimenta, 2023, p. 267).

In regulatory terms, this application of blockchain is still in an early stage of development in Brazil. Brazilian Federal Law No. 14.478/2022, although it addresses virtual assets and crypto-crimes, does not specifically regulate asset tokenization. The main objective of this law is in fact to curb new possibilities of money laundering through virtual assets. There is no specific regulation regarding the lawful use of this technology; such regulation is expected to be issued in the future (Article 8 of the Law). Nevertheless, the Brazilian Securities and Exchange Commission (CVM), in Guidance Opinion No. 40/2022, expressly stated that although NFTs are not listed as securities, they may be treated and regulated as such (translation by the author):

> The concept of a security has an instrumental nature and aims to define the scope of securities regulation and, consequently, the competence of the CVM. Therefore, in cases where a given crypto-asset qualifies as a security, the issuers and other parties involved are required to comply with the rules established for the securities market and may be subject to CVM regulation.

Another use case for cryptographically generated tokens made available on a blockchain network is that of non-fungible tokens (NFTs) as digital ownership certificates. This applies, for example, to digital artworks. It is the case of "Everydays: The First 5,000 Days", a digital artwork by the artist Beeple, sold for approximately 69.3 million dollars in 2021 (Cruz, 2021). The artist compiled 5,000 images of drawings published daily on his Instagram® account, without interruption, over 13 years since May 1, 2007 (Cruz, 2021). The work was authenticated via blockchain and paid for with the digital currency Ethereum. It thus represents an authentic form of conversion of real-world assets (such as a piece of art) into virtual assets (NFTs), with feasibility for subsequent conversion into fiat currency.

The examples listed above demonstrate that blockchain directly affects traditional notions of property, which compels the development of new legal theories to adapt existing institutions or to create new ones that are suitable for this emerging legal framework.

2.7. Digital Evidence

From a procedural standpoint, blockchain proves particularly useful for the production and preservation of evidence.[23] If incorporated into typical means of evidence (testimonial, documentary, expert, among others), this technology has relevant qualities for attesting to the truth of facts. And, once again, the main attribute that leads to this conclusion is the immutability.

If the purpose of evidence, as provided in Article 369 of the Brazilian Code of Civil Procedure, is to prove the truth of facts, then a technology that ensures the material (and ideological) integrity of the fact to be proven would be ideal. And if, in civil proceedings, where the search for formal truth prevails, the practical effects of this technology are promising, they are even more accentuated in criminal law, in which the pursuit of substantive truth is a duty of the State itself. This is reflected, for example, in the articles that authorize the judge to order the production of evidence *ex officio* in criminal proceedings (Articles 156, I and II; 196; 209; 242; and 404 of the Brazilian Code of Criminal Procedure).

[23] Since it constitutes an atypical means of producing evidence, the rule set forth in Article 369 of the Brazilian Code of Civil Procedure prevails, whereby the parties may use morally legitimate means to prove the facts, even if such means are not expressly provided for in the Code. In addition, blockchain can be used as a tool to ensure the integrity of typical forms of evidence, safeguarding, for example, the entire chain of custody of documentary evidence: from the origin of a given document to its submission in the case record.

However, blockchain does not offer only advantages for evidentiary production: there are issues that must be addressed regarding its procedural use. The main problem associated with the use of this technology in the evidentiary process does not concern the digital verification of authenticity itself. As explained by Almeida and Ferreira (2020), technologies capable of producing evidence, especially documents originating from virtual environments, such as screenshots of messages related to social media offenses, have existed for years. One example is OriginalMy, a platform through which the evidentiary document is generated and linked to a unique hash code stored on the company's own system.

In fact, the main issue with the use of blockchain in the evidentiary context lies in the assumption that the blockchain is truly immutable. This is the concern raised by Luo (2022), that questions who is ultimately responsible for the custody of the information. In the case of OriginalMy, the data in custody are administered by a private company. In other words, there are risks related to the unilateral management of data by the company. The Chinese experience referred to by Luo (2022) suggests combining blockchain technology with state-operated authenticity verification platforms. However, the underlying problem remains the same, only the premise changes, that is: the State is presumed to be more reliable than a private company.

From the analysis of these issues, one can also identify the limits of traditional procedural means of proof. Despite the operational advantages that blockchain could offer, there are problems mainly related to the custody of information, which directly affects the authenticity of evidence.

2.8. Arbitration

From a procedural and institutional perspective, blockchain enables the improvement of traditional forms of dispute resolution. This is the case for arbitral disputes occurring within blockchain environments, particularly for resolving conflicts involving smart contracts.

Lima and Guia Neto (2021, p. 115) suggest that the application of traditional (state) means of dispute resolution to smart contracts is inadequate for at least three reasons: difficulties in enforceability, party anonymization, and jurisdictional conflicts. On the other hand, to mitigate the negative effects that distributed jurisdiction could cause to conflict resolution, Lima and Guia Neto (2021, p. 118) suggest the adoption of intra-chain arbitration. In this manner, the inherent decentralization of blockchain and the anonymization of the parties, and governance mechanisms are implemented for the selection of arbitrators and the enforceability of obligations.

An example of this application is the Kleros platform, which resolves intra-chain disputes through Ethereum. Essentially, jurors (arbitrators) participating in the platform are registered in

advance and are remunerated with cryptocurrencies directly by the platform according to the degree of decisional convergence. In other words, an arbitrator will be compensated proportionally to how much their decisions converge with those of the other arbitrators. There is also an appeals system against “first instance” decisions. All this information was drawn from Lima and Guia Neto (2021, pp. 122–124).

Another solution, closer to traditional heterocompositive models of dispute resolution, concerns the hybrid model, in which the parties of a smart contract use an “oracle”, which is, in essence, an arbitrator or arbitral chamber in its traditional sense (Lima and Guia Neto, 2021, p. 122). In other words, it is an arbitration agreement embedded within the smart contract.

Conversely, blockchain may also be used to implement arbitral proceedings not linked to smart contracts. In this regard, as noted by Lima and Guia Neto (2021, p. 131), in the case of Brazilian law, the platform would need to comply with the requirements of Federal Law No. 9,307/1996, particularly with respect to the principle of reasoning in arbitral awards (Article 26, item II of the Law). That is, the traditional intra-chain model could not be used, since in such systems the party involved generally learns only the outcome of the decision, but not the reasons that led the arbitrator to that conclusion.

The advantages associated with the use of blockchain in arbitral proceedings are also related to its classical attributes, notably the integrity and immutability of evidence and case elements; the auditability of every element produced throughout the arbitral process; the possibility of automatic enforcement of the award; and the facilitation of cross-border enforceability (Lima and Guia Neto, 2021).

3. Final Remarks

Blockchain is a promising technology from the standpoint of governance, information security, and document management. Its key attributes, immutability, decentralization, and transparency, enhance the potential uses of this technology. Although originally conceived as a fully decentralized model, as proposed by Satoshi Nakamoto (2008), new arrangements have emerged, giving rise to private and permissioned (consortium-based) blockchains, each with distinct applications.

The effective implementation of this technology has produced impacts on private and procedural law. Smart contracts have emerged as self-executing contracts within virtual environments operating within predominantly private blockchains. In these contracts, questions of autonomy of will, contractual immutability, and interpretation of contractual clauses challenge traditional concepts of contract theory. In corporate law, decision-making now takes place entirely

in virtual blockchain environments, raising questions about the relationship between the speed of corporate deliberations and a fundamental feature of assemblies, that is, dialogicity.

Novel arrangements such as DAOs (Decentralized Autonomous Organizations) have emerged, structuring entire societies in decentralized virtual environments through blockchain. Within the DAO context, even less conventional arrangements, such as virtual cities, are testing the limits of property governance. Applications of the Internet of Things (IoT) have also arisen, incorporating blockchain into the interconnectivity of smart devices, bringing about new and unprecedented risks and advantages in the use of movable goods.

Related to IoT, the Industrial Internet of Things (IIoT) holds the potential to reduce agency conflicts and further increase the efficiency of production chains, though it tests the boundaries of civil liability theory. The possibility of asset tokenization also emerges, raising questions about its legal nature vis-à-vis traditional securities frameworks and highlighting important criminal law concerns, particularly regarding potential implications for money laundering crimes. Finally, in the procedural sphere, blockchain creates new possibilities for the production of evidence and enhances traditional heterocompositive models, such as arbitration.

From the analysis of all these applications, it becomes clear that blockchain technology effectively tests the limits of traditional legal theories across various doctrinal branches (civil, corporate, registry, procedural, and criminal law). The reinterpretation of traditional legal theories is, therefore, not only necessary but indispensable for adequately addressing the new paradigms imposed by blockchain.

References

ALMEIDA, Marcelo Pereira de; FERREIRA, Diogo de Castro**.** O blockchain como meio de prova no Direito Processual Civil brasileiro. **Revista Juris Poiesis**, Rio de Janeiro, v. 23, n. 33, p. 335-349, 2020.

ALVES, Giovani Ribeiro Rodrigues; KOBUS, Renata Carvalho; FAWAZ, Dunia Hammoud. Tecnologia blockchain para otimização das transações empresariais no Direito Societário. **International Journal of Digital Law**, Belo Horizonte, v. 2, n. 2, p. 79-98, may/aug. 2021.

ANDRADE, Daniel de Pádua; COLOMBI, Henry. Smart contracts: por um adequado enquadramento no Direito Contratual Brasileiro. *In*: CHAVES, Natália Cristina; COLOMBI, Henry (orgs.). **Direito e tecnologia: novos modelos e tendências**. Porto Alegre: Editora Fi, 2021. p. 17-35.

BAMBARA, Joseph J.; ALLEN, Paul R. **Blockchain: a practical guide to developing business, law, and technology solutions**. New York: McGraw Hill Education, 2018.

BAYLE, Aurélie; KOSCINA, Mirko; MANSET, David; PEREZ-KEMPNER, Octavio. When Blockchain Meets the Right to be Forgotten: Technology Versus Law in the Healthcare Industry**. In: Proceedings of the IEEE/WIC/ACM International Conference On Web Intelligence** *(WI)*, 2018, Santiago.

BRASIL. Comissão de Valores Mobiliários. Parecer de Orientação CVM nº 40, de 11 de outubro de 2022. **Os Criptoativos e o Mercado de Valores Mobiliários.** Brasília, 2022.

BRASIL**. Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Institui o Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Accessed on: 5 jul. 2025.

BRASIL. Empresa de Pesquisa Energética. **Anuário estatístico de energia elétrica 2024: ano base 2023**. [S. l]: EPE, 2024. Available at: https://www.epe.gov.br/sites-pt/publicacoes-dados-abertos/publicacoes/PublicacoesArquivos/publicacao-160/topico-168/anuario-factsheet-2024.pdf. Accessed on: 5 jul. 2025.

BRASIL. **Empresa OriginalMy**. OriginalMy: coletor de provas, solução em blockchain. Available at: https://originalmy.com/. Accessed on: 30 oct. 2025.

BRASIL. **Lei Federal n. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília: Congresso Nacional, 1990. Available at: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

BRASIL. **Lei Federal n. 9.307, de 23 de setembro de 1996**. Brasília: Congresso Nacional, 1996. Dispõe sobre a arbitragem. Available at: https://www.planalto.gov.br/ccivil_03/leis/l9307.htm. Accessed on: 5 jul. 2025.

BRASIL**. Lei Federal n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília: Congresso Nacional, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Accessed on: 12 jun. 2025.

BRASIL. **Lei Federal n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Congresso Nacional, 2014. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 29 out. 2025.

BRASIL. **Lei Federal n. 13.105, de 16 de março de 2015**. Código de Processo Civil. Brasília: Congresso Nacional, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Accessed on: 13 jun. 2025.

BRASIL. **Lei Federal nº 13.709, de 14 de agosto de 2018**. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Brasília: Congresso Nacional, 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: 29 out. 2025.

BRASIL**. Lei Federal n. 14.478, de 21 de dezembro de 2022**. Dispõe sobre as diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de

serviços de ativos virtuais. Brasília: Congresso Nacional, 2022. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Accessed on: 5 jul. 2025.

BRASIL. **Projeto de Lei Federal n. 4, de 2025.** Dispõe sobre a atualização da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), e da legislação correlata. Brasília: Senado Federal, 2025. Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/166998. Accessed on: 5 jul. 2025.

BRASIL. Superior Tribunal de Justiça. Terceira Turma**. Recurso especial n. 1.669.002/RJ.** Relatora: Ministra Nancy Andrighi, 21 de setembro de 2017. Diário da Justiça Eletrônico, 2 out. 2017.

BRUMMER, Chris; SEIRA, Rodrigo. Legal Wrappers and DAOs. **SSRN Electronic Journal**, [S.l.], p. 1-31, 30 maio 2022.

CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE. **Cambridge Bitcoin Electricity Consumption Index** (CBECI). Cambridge: CCAF, 2025. Available at: https://ccaf.io/cbnsi/cbeci. Accessed on: 23 oct. 2025.

CATCHLOVE, Paul. Smart contracts: a new era of contract use. **SSRN Electronic Journal**, [S.l.], p. 1-24, 1 dez. 2017.

COSTA, Daniel Rodrigues. A (in)compatibilidade do blockchain com as leis de proteção de dados pessoais. *In*: PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE GRAAF, Jeroen (Coord.). **Direito, tecnologia e inovação*: v. 3: aplicações jurídicas de blockchain.*** Belo Horizonte: Expert Editora Digital, 2021. p. 175-204.

COSTA, José Augusto Fontoura; MARQUES, Leonardo Albuquerque. Contratos inteligentes, OAD e nova economia institucional: perspectivas para a interpretação e aplicação de ajustes celebrados em computação descentralizada a partir de estudo de caso sobre a vulnerabilidade da codificação no ambiente do Ethereum. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 18, n. 6, p. 61-90, jan./mar. 2019.

CRAWLEY, Jamie. 'Blockchain City' CityDAO falls victim to $95K hack via Discord. **CoinDesk**, New York, 14 jan. 2022. Available at: https://www.coindesk.com/business/2022/01/14/blockchain-city-citydao-falls-victim-to-95k-hack-via-discord. Accessed on: 5 jul. 2025.

CRUZ, Felipe Branco. Obra de arte digital é vendida por US$ 69 milhões em leilão. **Veja**, São Paulo, 11 mar. 2021. Available at: https://veja.abril.com.br/cultura/obra-de-arte-digital-e-vendida-por-us-69-milhoes-de-dolares-em-leilao/. Accessed on: 5 jul. 2025.

FRAZÃO, Ana. Responsabilidade civil de administradores de sociedades empresárias por decisões tomadas com base em sistemas de inteligência artificial**.** *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters Brasil, 2019. p. 482-521.

JEAN, Renée. Wyoming's first digital land buy wasn't Story's historic Wagon Box Inn, it was CityDAO near Yellowstone. **Cowboy State Daily**, Cheyenne, 14 maio 2023. Available at: https://cowboystatedaily.com/2023/05/14/wyomings-first-digital-land-buy-wasnt-storys-historic-wagon-box-inn-it-was-citydao-near-yellowstone/. Accessed on: 5 jul. 2025.

LAFARRE, Anne; VAN DER ELST, Christoph. Blockchain technology for corporate governance and shareholder activism. [S. l.]: **Social Science Research Network** (SSRN), 2018. (European Corporate Governance Institute – Law Working Paper, n. 396/2018). Available at: https://ssrn.com/abstract=3135209. Accessed on: 28 set. 2025.

LIMA, Gabriel Ribeiro de; GUIA NETO, Marcos Luiz dos Mares. Arbitragem em blockchain: juridicidade e perspectivas. *In*: PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE GRAAF, Jeroen (Coord.). **Direito, tecnologia e inovação*: v. 3: aplicações jurídicas de blockchain*.** Belo Horizonte: Expert Editora Digital, 2021. p. 108-138.

LUO, Xinkai. Blockchain como novo veículo da prova digital: uma experiência chinesa. **Revista Acadêmica da Faculdade de Direito do Recife**, Recife, v. 94, n. 2, p. 26-49, 2022. DOI: 10.51359/2448-2307.2022.253028. Available at: https://periodicos.ufpe.br/revistas/index.php/ACADEMICA/article/view/253028. Accessed on: 5 jul. 2025.

MCKINNEY, Scott A.; LANDY, Rachel; WILKA, Rachel. Smart contracts, blockchain, and the Next Frontier of Transactional Law. **Washington Journal of Law, Technology & Arts**, [S, l], v. 13, n. 3, p. 313-347, 2018.

Mercan, Suat; Akkaya, Kemal. Building Next Generation IoT Infrastructure for Enabling M2M Crypto Economy. **Open Journal of Internet of Things (OJIOT)**, v. 7, n. 1, 2021. Available at: https://www.ronpub.com/OJIOT_2021v7i1n11_Mercan.pdf. Accessed on: 29 oct. 2025.

MOREIRA, Arthur Salles de Paula; DELGADO, Camila Campos Baumgratz; SANTOS, Gabriel Gonçalves. Repensando a tecnologia blockchain: por que nem tudo o que você leu até hoje era verdade? *In*: PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE GRAAF, Jeroen (Coord.). **Direito, tecnologia e inovação*: v. 3: aplicações jurídicas de blockchain.*** Belo Horizonte: Expert Editora Digital, 2021. p. 23-60.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. [S.l.]: Bitcoin.org, 2008. Available at: https://bitcoin.org/bitcoin.pdf. Accessed on: 3 jul. 2025.

OK, Emmanuel; BARNTY, Barnabas; JOSEPH, Oloyede. Energy consumption of blockchain networks. **ResearchGate**, [S. l.], fev. 2025. Available at: https://www.researchgate.net/publication/389175548. Accessed on: 5 jul. 2025.

PIMENTA, Eduardo Goulart. **Direito do mercado financeiro e de crédito**. 3. ed. Belo Horizonte: Editora Expert, 2023.

PIMENTA, Eduardo Goulart. **Estrutura jurídica da empresa na era digital**. 4. ed. Belo Horizonte: Editora Expert, 2024.

RONG, Helena; MAO, Zeslene. **Deep-dive into CityDAO***: An Experiment in Collective Land Ownership and Decentralized Governance*. Cambridge: Belfer Center for Science and International Affairs, 2023. 32 p. Available at: https://www.belfercenter.org/sites/default/files/2024-08/CaseStudy_TAPP_CityDAO_Helena_Rong.pdf. Accessed on: 5 jul. 2025.

SILVA, Glacus Bedeschi da Silveira e; TEIXEIRA, Luiz Felipe Drummond; SANTANA, Mariana Damiani. Smart contracts concluídos por smart devices: entre o consentimento e o comportamento social típico**.** *In*: PARENTONI, Leonardo; MILAGRES, Marcelo de Oliveira; VAN DE

GRAAF, Jeroen (Coord.). **Direito, tecnologia e inovação***: v. 3: aplicações jurídicas de blockchain.* Belo Horizonte: Expert Editora Digital, 2021. p. 205-264.

SUSSKIND, Richard. **Tomorrow's Lawyers: an introduction to your future**. 2. ed. Oxford: Oxford University Press, 2017.

TAKEN, Chance. **CityDAO Parcel 0 NFT Drop**. *Blog CityDAO*, 3 maio 2022. Available at: https://city.mirror.xyz/ClTclr9uF6818MjoNjNSMCRLGH-YtIiJKeYNHWJFKAk. Accessed on: 5 jul. 2025.

URTON, Gary. **Signs of the Inka Khipu: Binary Coding in the Andean Knotted-String Records**. Austin: University of Texas Press, 2003. 202 p.

VERHEIJ, Bart. The Study of Artificial Intelligence as Law. *In*: CUSTERS, Bart; FOSCH-VILLARONGA, Eduard (orgs.). **Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice**. The Hague: T.M.C. Asser Press, 2022. p. 477-502.

WYOMING (EUA). **Senate Enrolled Act nº 73 (SF 0038), Decentralized Autonomous Organizations**, 21 abr. 2021. (Cap. 162). Cheyenne: Wyoming Legislature, 2021. Available at: https://www.wyoleg.gov/2021/Enroll/SF0038.pdf. Accessed on: 5 jul. 2025.

.....

Guilherme Ramos de Morais
Advogado. Doutorando em Direito pela Universidade Federal de Minas Gerais (2025 - Atual). Mestre em Direito pela Universidade de Brasília (2022). Pós-graduado na Universidade do Estado do Rio de Janeiro. Bacharel em Direito pela Universidade de Brasília (2020). Atualmente, é pesquisador com ênfase em processamento de linguagem natural aplicado ao direito. Possui experiência de pesquisa em direito constitucional, processo civil, processamento de linguagem natural e inteligência artificial aplicados ao direito.

.....

Enviado em: 04/11/2025

Aprovado em: 21/06/2026