Acta Universitatis Danubius
JURIDICA

Blockchain and Legal Authority: Decentralization, Regulation, and Legitimacy in the Age of Code

Andy Corneliu Pușcă[1]

Abstract: The article looks at how blockchain technology is reshaping the foundations of legal authority, focusing on the emergence of post-institutional law and the transformation of sovereignty, legitimacy, and regulatory framework. It is based on the literature on "Lex Cryptographia" (Wright & De Filippi, 2015), decentralized governance models and hybrid regulatory approaches, critically assessing their relevance in the current legal context. Using doctrinal analysis and a comparative review of the literature, the study integrates perspectives from law, technology and governance theory. The results highlight the shift from state-centric legal authority to algorithmically executed norms, the coexistence of pluralistic normative systems, and the emergence of hybrid governance models that combine code-based rules with traditional law safeguards. These transformations challenge the established concepts of jurisdiction, liability and legitimacy, with important implications for legislators, courts and international governance bodies. The article proposes an interpretive framework for understanding the legal implications of blockchain and advocates a balanced integration of technological innovation with fundamental principles of law, in order to preserve fairness and accountability in decentralized environments.

Keywords: decentralised governance; algorithmic regulation; legal pluralism; digital sovereignty; hybrid legal systems

[1] PhD, Associate Professor, Danubius International University of Galati, Romania, Address: 3 Galati Blvd., 800654 Galati, Romania, Corresponding author: andypusca@univ-danubius.ro.

1. Code and Legal Authority in Transformation

In the history of law, every great technological rupture has generated a crisis and, at the same time, a reconfiguration of legal authority. If the alphabet allowed the codification of the law, and the printing press ensured its spread, the blockchain proposes a new type of code – not only as a technology, but as a normative tool. In this light, "Lex Cryptographia" (Wright & De Filippi, 2015) is not just a technological concept, but a profound challenge to the traditional legal order.

This new normative model involves rules written into the code, executed automatically and validated by the consensus of the network. Instead of a central authority, we have a distributed architecture, in which governance is built dynamically, in real time, through the anonymous collaboration of participants. This network works in parallel with classical legal systems and calls into question the legitimacy of hierarchically imposed rules. That is why many authors speak of a form of "illegality" (De Filippi et al., 2022) – an order that does not deny the law, but neither does it traditionally recognize it.

In this autonomous order, smart contracts function as self-executing rules. Authority no longer derives from law, but from technological functionality. The problem becomes all the more complex as technology, by its transnational and opaque nature, tends to escape democratic and legal control. The state, accustomed to deciding, regulating and sanctioning, is confronted with a normative infrastructure that bypasses its institutions and can outline areas of "extralegality".

On the other hand, in this tension between the state and the code, new forms of balance are also taking shape. Some states choose to integrate blockchain as a governance tool (Yeung, 2018), others prefer to tolerate it, and the most prudent ones try to regulate it. This opens up a fertile field of reflection on the reconfiguration of authority: how can legitimacy be rewritten in a world where the law is translated into programming language?

Symbolically, the computer code becomes the modern equivalent of the law engraved in stone: immutable, automatic, enforceable. But in contrast to traditional codes, digital code is created and maintained by fluid, often anonymous communities with no clear accountability or control mechanisms. This is where the tension arises between the legal tradition – built on the principles of transparency and accountability – and the new forms of algorithmic authority. Is this an emancipation of law or the beginning of an era of normative opacity? It is precisely these dilemmas that define the beginning of a new paradigm: post-institutional law.

In this context, the legal authority is challenged to evolve not only in terms of normative content, but especially in terms of institutional structure. Laws written by Parliament can be supplemented or contradicted by automatic rules validated by networks, which means that legitimacy is no longer an exclusive attribute of the state. A form of normative pluralism is being born, in which human instances and digital codes can compete or cohabit. Thus, the transformation is not only a superficial one, but a profound one: it is a mutation in the epistemological foundation of law.

2. Decentralization of Decision-Making – From Sovereignty to Algorithmic Consensus

Blockchain technology not only proposes an alternative infrastructure for recording and verifying transactions, but also a fundamentally different method of decision-making. In decentralized networks, such as DAOs (Decentralized Autonomous Organizations), rules are voted, modified, and enforced through automatic or semi-automatic mechanisms, in which authority is disseminated.

DAOs operate on the basis of tokenized voting – that is, voting rights are proportional to economic participation. This may seem democratic, but it raises questions about fairness and representativeness. Alternative models, such as reputation-based voting or "conviction voting", try to mitigate the dominance of capital over decision (Sims, 2021). In the absence of institutional filters or review mechanisms, these forms of participation can generate automatic decisions, devoid of nuance or legal context.

In addition, the decision in blockchain is simultaneously technological and political. Consensus mechanisms – proof-of-work, proof-of-stake or other variants – involve the active involvement of network actors in the validation of norms. In this framework, the "law" is no longer imposed, but negotiated through technical protocols. This continuous reconfirmation of norms, through the collective action of nodes, radically transforms the dynamics of authority: from institutional verticality to distributed horizontality. Thus, the very architecture of normative power is modified.

However, this apparent decentralization hides a new form of concentration. Access to decision-making is conditional on capital, technical expertise or network position. Thus, an algorithmic oligarchy is taking shape, in which those who control the infrastructure implicitly control the norm. Instead of democratic governance, we have a legitimacy derived from calculation – efficient, but often opaque. This is

where the risk of a "decentralized technocracy" arises in which the decision escapes public control.

Smart contracts contribute to this logic. They transform the execution of the norm into an automatic act, which leaves no room for equity, remedy or interpretation. In traditional law, any norm can be challenged, reanalyzed, reconfigured. In blockchain, the norm becomes performative: what is executed is already "decided". This confusion between decision and execution calls into question the very deliberative essence of law. In addition, the difficulty of challenging a decision taken by a smart contract creates the premises for an automatic jurisprudence, without the right to appeal.

In conclusion, the decentralization of legal decision-making does not automatically mean democratization. Without a critical reflection on algorithmic mechanisms and without institutions to accompany technology, we risk replacing institutional authority with a technological authority, less visible, but equally normative. There is a need for new forms of connection between the code and the norm, between the network and the community, so that the decision is not only technically correct, but also democratically legitimate.

3. Blockchain and Legal Regulation – Between Regulatory Vacuum and Legal Integration

The emergence of blockchain infrastructures has revealed major difficulties for current legal systems. From smart contracts and DAOs (Decentralized Autonomous Organization) to digital identity and decentralized arbitrage, these tools do not easily fit into the positive law grid. In many cases, they operate in a parallel logic, bypassing the classical principles of civil or public law.

A DAO is an association of people who use blockchain technology to manage decisions and resources without a command center; Members hold their own tokens and can propose or vote on initiatives, and the operating rules are implemented through smart contracts, so that the organization's work is carried out automatically and transparently. The purpose of a DAO is to give each participant voting rights and remove a central entity's control over the direction of the organization.

A first major difficulty is related to jurisdiction. Transactions are globally distributed, and geographic location can no longer be used as a benchmark for law enforcement. In the absence of a physical point of contact, the application of private international

law becomes theoretical. The problem worsens when a state claims to apply its own law to a system that, technologically, cannot be "localized" (Ferreira, 2021). Under these circumstances, the concept of legal sovereignty requires a rewrite that takes into account the fluid and global nature of blockchain.

Smart contracts, while effective for simple transactions, raise legal enforcement difficulties in complex relationships. Not every obligation can be expressed in binary terms. The lack of a human instance of interpretation means that code error can equate to injustice – without recourse (Howell & Potgieter, 2021). This calls into question the applicability of the principle of fairness and opens the discussion on the need for a digital contract law adapted to technological realities.

Digital identity also creates friction. The pseudonymity of blockchain conflicts with data protection rules. More seriously, the immutability of the register can perpetuate errors or abuses without the possibility of remedy. The right to be forgotten becomes inapplicable, and responsibility – difficult to attribute (Sullivan & Tyson, 2023). In addition, decentralized digital identity implies a rethinking of the notion of legal capacity and the way in which relationships between people are built in the virtual space.

A detailed understanding of the technical concepts is essential to appreciate the legal implications of blockchain. In the digital space, pseudonym is based on the idea of an alternative identity: users choose a pseudonym to protect themselves, while still maintaining a constant presence on the network. Imagine a digital artist operating under a fictitious name when selling their works as NFTs (non-fungible tokens). He builds his reputation based on his chosen alias, and clients recognize his style and portfolio without knowing his real name. From a legal point of view, such a pseudonym offers a balance between privacy and responsibility, since the alias can be associated with a history of transactions and thus, if the perpetrator commits fraud, the authorities can correlate the virtual identity with the real person.

On the other hand, the immutability of the blockchain means that once entered, information can no longer be modified or deleted. A distribution company could use blockchain to record the route of each batch of food products; If a batch is mislabelled or contains allergenic ingredients, the erroneous registration remains permanently visible. The correction can only be made through a new entry that marks the cancellation, but the antecedent remains indefinitely. This permanence of data has implications for consumer law and compliance obligations, especially when the deletion of erroneous information is required.

To manage identity in such a system, decentralized identifiers (DIDs) have emerged. A DID is a unique identifier associated with a person or organization, directly controlled by the holder and resolvable in a descriptive document. For example, a student who receives the diploma in digital format and certifies it with a DID: the university issues the certificate, the student proves his control over the DID, and employers can verify the authenticity of the diploma without consulting a central register. Thus, DIDs allow for a portable and verifiable identity, independence from a particular state or platform, and also raise questions about the legal recognition of these identities.

Another innovation of the decentralized economy is decentralized autonomous organizations (DAOs). These are collective structures that use blockchain to coordinate members' decisions. Suppose a group of residents aims to finance the installation of solar panels in the community. Instead of setting up a classic association, they create a DAO: they issue tokens that give them voting rights, set the rules in a public smart contract, and purchase or investment decisions are made by member vote. In this way, control is distributed and maximum transparency; However, positive law must determine who bears responsibility if something is not working properly.

Although the digital world emphasizes decentralization, the classic model of the limited liability company (LLC) continues to play a crucial role. An LLC is a flexible legal structure that combines features of partnerships and corporations; Members can determine the division of profits as they wish, and their liability is limited to the social contribution. For example, a crypto investment fund can create an LLC vehicle so that token-holders are protected from personal liability and class actions have legal recognition.

These examples demonstrate how pseudonymity, immutability, DIDs, DAOs, and LLCs intertwine in the blockchain ecosystem and influence both practices and legal regulation. The entire architecture requires flexible regulatory solutions that ensure accountability and protection of rights, without inhibiting technological innovation.

Europe seems to be proposing a model of coexistence: EU legislation recognises blockchain not as an adversary, but as a governance challenge. In this paradigm, the law does not prohibit the code but accompanies it. The role of authority is no longer to dictate, but to mediate between innovation and public order. In this regard, hybrid regulatory models are emerging, in which the national authority collaborates with decentralized structures to create a dynamic and evolving regulatory framework.

On a philosophical and political level, the challenge is to rethink the foundation of authority in a world where the norm is executed without an intermediary, and regulation becomes algorithmic. How do we maintain legal coherence without stifling the transformative potential of new technology? The answer seems to lie not in resistance, but in the ability of the legal system to rethink itself from within. Thus, regulation becomes not only an act of control, but also an exercise of institutional imagination, which must keep up with the digital age.

4. Traceability and Accountability – Legal Dilemmas in Distributed Architectures

One of the fundamental promises of blockchain is absolute traceability: every transaction, modification, or interaction is recorded in an immutable ledger, replicated across the entire system. This property provides, in theory, a solid basis for participant empowerment and unprecedented transparency. However, in the absence of a command center or authority that directly assigns responsibility, the question arises: who is actually responsible in a decentralized network?

Distributed systems, such as DAOs or decentralized applications, operate based on a mix of automated rules (smart contracts), participant votes, and cryptographic validation mechanisms. Responsibility is no longer vertical but dispersed. An "illegal" or defective act can be the effect of a collective consensus or a code error, not a decision taken by a single actor. Here, legal liability faces an ontological challenge: we no longer have a "who", but a "what".

To manage this challenge, the literature proposes several solutions. Some are based on incorporating decentralized structures into traditional legal entities – for example, turning DAOs into limited liability LLCs/LLCs (Sims, 2021). Other proposals aim to create special legal entities for artificial intelligence or autonomous systems, which can answer to the law (Chaffer et al., 2024).

There are also technical mechanisms that can support traceability: cryptographic signatures, digital reputation, weighted votes and transparent public registers. In theory, they should provide a form of collective accountability. In practice, however, pseudonymity and the lack of a harmonised legal framework complicate the process of identifying and sanctioning unlawful behaviour. The classic concepts of guilt, intent or guilt are difficult to adapt to actions produced by automated protocols.

In the absence of a central arbitration court, some systems have developed alternative dispute resolution mechanisms: decentralized arbitration, with randomly chosen jurors (Gabuthy, 2023), or "digital sheriffs" – users who monitor and intervene in case of irregularities (Bergolla et al., 2021). These solutions bring a degree of community control, but raise questions about the legitimacy, competence and fairness of the process.

In addition, issues related to identity – both of individuals and actions – generate a legal gray area. If we cannot clearly attribute an action to an individual, who is liable in the event of damage? What is the status of a decentralized organization without legal personality, but with massive economic and social influence? Here, legal liability encounters a vacuum of legal ontology – a lack of conceptual frameworks to understand and frame the distributed digital reality.

In the face of these uncertainties, a hybrid regulatory trend is emerging: combinations between automatic compliance mechanisms (compliance by design) and human supervision, between code and law, between network and institution. In this sense, the most promising solutions do not come from a tightening of control, but from a collaboration between legal design and technological design.

Finally, as Varoufakis observed, technology is not neutral. In the absence of democratic deliberation and the regulatory framework that accompanies automation, we risk that transparency will paradoxically hide irresponsibility. If everything is seen, but no one can be held responsible, traceability becomes a simulacrum. That is why the law must rethink the notion of author, responsible and subject of the norm, in an ecosystem where the code not only reflects the law but executes it without appeal.

We can thus speak of a new generation of legal responsibility – one that is no longer based exclusively on intention or guilt, but on structure, design, participation and the ability to anticipate systemic effects. It is a challenge for doctrine, for institutions and for the architects of the new digital order.

5. Legitimacy and Normative Pluralism in the Blockchain Age

One of the most profound challenges posed by blockchain technology is not technical, but theoretical and constitutional: what does legal legitimacy mean in a system in which the norm no longer derives from the will of the sovereign, but from the consensus of the network? And how is normative pluralism articulated when

norms can be issued, executed, and modified by algorithmic communities outside state borders?

The concept of "Lex Cryptographia" (Wright & De Filippi, 2015) expresses the emergence of an alternative legal order, based on codified, immutable and automatically executed rules.

These norms were not voted in parliaments, they are not justified by moral or social values, but by technological functionality and operational efficiency. Thus, the "rule of code" becomes a source of legitimacy distinct from the traditional "rule of law". In this context, the computer code not only implements rules, but gradually replaces the classic normative authority.

A new form of legal pluralism is thus taking shape, in which blockchain rules coexist with those of state law. However, this pluralism is not institutionally recognized, but de facto: users choose which rules they follow, depending on the platform, community or protocol. The law becomes selective, contextual and partly optional. In this regard, Reyes (2017) suggests that blockchain infrastructures could be treated, legally, as foreign law systems – a proposal that paves the way for a conflicting law of code.

From a theoretical perspective, this transition from a centralized authority to a polycentric governance requires a revision of the fundamental concepts of constitutional law. The idea of a "smart social contract" (Carata et al., 2024) proposes a synthesis between the algorithmic code and democratic deliberation. Other theories, such as that of digital jurisdiction (Möslein, 2019) or distributed jurisdiction (Kaal & Calcaterra, 2017), try to provide a conceptual framework for this new legal space.

At the same time, blockchain generates emerging forms of community: transnational groups organized around a token or a DAO, which function as quasi-political entities, with their own rules, sanctions and legitimation mechanisms. These "cloud communities" (Orgad & Bauböck, 2018) no longer recognize the authority of the state except when it suits them, which undermines the coherence of classical legal systems and calls into question the universality of the rule of law.

This normative fragmentation brings benefits – innovation, adaptability, direct participation – but also risks: lack of coherence, difficulty in coordination and the danger of capturing legitimacy by technological elites. Legitimacy thus becomes a competitive stake: between the state and the network, between the code and the law, between the community and the individual. It is no longer a question of formal

obedience to authority, but of functional acceptance of a norm as just, useful or inevitable.

In this framework, the role of positive law is to propose models of integration. Some jurisdictions are developing regulatory bodies dedicated to distributed technologies (MiCA, eIDAS 2.0), others are proposing "regulatory sandboxes" to test new rules in a controlled regime. At the doctrinal level, the emergence of a unified body of rules for DLT infrastructures is suggested (Erbguth & Morin, 2018), capable of providing coherence in a dispersed regulatory landscape.

In the end, the central question remains: how do we maintain legitimacy in a world governed partly by code? The answer cannot come only from technological reason or traditional authority. We need a theoretical and institutional reconfiguration, in which the law not only tolerates normative pluralism, but structures it, mediates it and capitalizes on it in a democratic spirit.

It is likely that in the coming decades we will not witness the replacement of state law by blockchain, but a co-evolution: a hybridization dynamic, in which the code becomes part of the legal norm, and the state learns to govern through networks. This is precisely where the key to a new legitimacy lies: not in unilateral domination, but in a balancing of normative sources around the common values of justice, transparency and authentic participation.

6. Legal Epilogue – Post-Institutional Law?

In the age of blockchain, we are witnessing the emergence of an emerging legal paradigm that defies classic institutional frameworks: post-institutional law. This concept describes a profound reorganization of normative authority, in which traditional legal institutions lose their monopoly in favor of decentralized technical architectures. In this new context, norms are no longer the result of a legislative process, but the result of an automatically executable algorithmic consensus.

The regulatory regime generated by blockchain is based on autonomous infrastructures, in which the code becomes the supreme expression of the norm. "Rule of code" replaces "rule of law" as a regulatory mechanism, and "Lex Cryptographia" (Wright & De Filippi, 2015) becomes an instrument of post-national governance. Here, legal authority is incorporated directly into the source code and disseminated through smart contracts, without intermediaries, without courts, without the state.

Legitimacy mechanisms in this framework no longer derive from institutional democratic validation, but from active participation, digital reputation and economic incentives.

Blockchain platforms use tokenized voting, distributed consensus mechanisms, and DAO governance systems that redefine the concept of sovereignty. Thus, an algorithmic, emerging authority is taking shape, in which legal responsibility is divided between anonymous actors and automatic rules.

However, this radical transformation brings with it major challenges. On the one hand, the difficulty of identifying legal subjects in a pseudonymity-based system; on the other hand, the impossibility of applying coercive force outside the blockchain (Ferreira, 2021). Smart contracts, while effective, cannot handle situations that are complex, ambiguous, or require contextual interpretation (Howell & Potgieter, 2021).

Against the backdrop of these limitations, hybrid solutions are being developed: the integration of DAOs into traditional corporate structures (Sims, 2021), the emergence of "digital sheriffs" and decentralized arbitration (Gabuthy, 2023), as well as proposals for legal systems adapted to the distributed age. In parallel, the idea of the "smart social contract" (Carata et al., 2024) is taking shape, as a model of reconciliation between automation and deliberation.

Thus, post-institutional law should not be understood as an abolition of institutions, but as a transformation of them. Institutions are reconfiguring themselves around technology: they are no longer centers of power, but nodes in a validation network. Justice becomes, in turn, distributed, preventive, and, in some cases, algorithmic. A normative competition is emerging between the old regulatory structures and the new codes that govern interactions in blockchains.

But the fundamental question remains: can we talk about legal legitimacy without institutions? Or do we need a new generation of institutions, adapted to the code and the network, but faithful to the principles of law? Perhaps the answer lies in an intermediate model: a legal architecture that integrates the code without abdicating deliberation, that allows decentralization without relinquishing accountability, and that leverages technology in the service of equity.

In conclusion, post-institutional law is not the end of law, but the beginning of a new legal ontology: one in which institutions are digitized, norms are codified, and authority is fragmented. It is a challenge for legal thinking, but also an opportunity to reinvent law as a space for guaranteeing rights, even in networks without centers.

This article aimed to critically analyze how blockchain technology is reshaping the foundations of legal authority in the digital age. Starting from the idea that law is not an immutable system, but a living, adaptable framework, we have explored how the digital code becomes both an instrument and a source of normativity. In this regard, we have proposed a stratified reading of the phenomenon, from the transformation of the code into authority (Chapter 1), to the emergence of a post-institutional legal paradigm (Chapter 5).

In the course of this analysis, we have shown how the decentralization of decision-making (Chapter 2) weakens the classical notion of sovereignty, replacing it with new forms of algorithmic consensus, in which law is generated and executed in the network. We then identified regulatory gaps and possible pathways of legal integration (Chapter 3), highlighting the tension between technological innovation and regulatory conservatism. The chapter on traceability and accountability (Chapter 4) illustrated the difficulty of assigning responsibility in a pseudonymous and distributed ecosystem, and reflections on legitimacy and technological codification (Chapter 5) highlighted the competition between traditional and emerging legal norms.

The contribution of this article consists not only in the synthesis and doctrinal analysis, but also in the introduction of interpretative concepts that can support a rethinking of legal institutions in relation to blockchain architecture. I advocated for a critically constructive approach that does not demonize technology, but neither does it idealize it. At the heart of this analysis remains the idea that the law must retain its function as a guarantor of equity, even in a context in which the code tends to take over the role of the norm.

In the end, we are not proposing a break between law and technology, but a lucid reconciliation. The Code can become an instrument of justice, but it should not be confused with justice itself. Authority can be distributed, but responsibility needs to be rethought. And legitimacy – in whatever form it takes – must remain anchored in the values of law, not just in the efficiency of protocol.

References

Atzori, M. (2015). *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?* SSRN.

Carata, L. (2024). *Smart social contract and democratic governance*.

De Filippi, P., Mannan, M., & Reijers, W. (2022a). Blockchain as a Confidence Machine: The Problem of Trust and Challenges of Governance. *Technology in Society*, 70.

De Filippi, P., Mannan, M., & Reijers, W. (2022b). Blockchain and the Law: A Critical Evaluation. In R. Brownsword, E. Scotford & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation and Technology*. Oxford University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3317404.

Erbguth, J., & Morin, J. H. (2018). *Blockchain for Governments: Use Cases and Regulatory Challenges*.

Ferreira, J. (2021). Jurisdiction in Cyberspace: Blockchain and the Relevance of Territoriality. *International Journal of Law and Information Technology*, 29(2), 111-137.

Gabuthy, Y. (2023). Blockchain and Arbitration: A New Legal Order? *International Arbitration Law Review*, 26(1), 15-31.

Ghodoosi, F. (2019). The Blockchain Disruption: Smart Contracts and the Future of Commercial Law. *Hastings Business Law Journal*, 15(2), 175-202.

Goossens, J. (2021). Blockchain, privacy and the law: Reconciling technology with legal protections. *Computer Law & Security Review*, 41.

Gstrein, O. J., & Kochenov, D. (2020). Digital identity and distributed ledger technology: An uneasy legal relationship. *Computer Law & Security Review*, 36. https://ssrn.com/abstract=3433498.

Howell, B., & Potgieter, A. (2021). *Enforcing Smart Contracts in Traditional Legal Systems*. SSRN.

Jumelle, A. (2022). Reputation systems and decentralized accountability. *Digital Society Review*, 5(3), 66-89.

Kaal, W. A., & Calcaterra, F. (2017). *Blockchain Innovation and Jurisdictional Competition*. SSRN

Krishnamoorthy, R. (2024). Smart Compliance: Automated Legal Checks through Blockchain. *Journal of RegTech & AI Governance*, 2(1), 42-59.

Lu, Y. (2021). Blockchain and Sovereignty: Implications for the Rule of Law. *Journal of Legal Technology Risk*, 10(2), 118-135.

Mishra, S. (2023). Blockchain and Legal Integration: Challenges and Hybrid Models. *Journal of Digital Law*, 12(1), 17-40.

Reijers, W., & De Filippi, P. (2016). The Blockchain as a Narrative Technology: Investigating the Social Contract Architecture. *Philosophy & Technology*, 30(1), 1-28. https://link.springer.com/article/10.1007/s13347-016-0239-x.

Sillanpää, E. (2020). Automated Execution vs. Judicial Review: Legal Boundaries of Smart Contracts. *European Review of Private Law*, 28(6), 1203-1225.

Wright, A., & De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. SSRN.