Nativa, Sinop, v. 13, n. 2, p. 234-246, 2025.
Pesquisas Agrárias e Ambientais
DOI: https://doi.org/10.31413/nat.v13i2.19055

ISSN: 2318-7670

Consensus Mechanism for Environmental Blockchain: Proof-of-Eco-Awareness (PoEa)

Daniel Weigert CAVAGNARI *[1], Lia Maris Orth Ritter ANTIQUEIRA [2],

[1] Universidade Tecnológica Federal do Paraná, Curitiba, PR, Brasil.
[2] Universidade Tecnológica Federal do Paraná, Ponta Grossa, PR, Brasil.
*E-mail: cavagnari@me.com

Submitted: 03/31/2025; Accepted: 05/07/2025; Published: 05/xx/2025.

ABSTRACT: There are numerous consensus mechanisms existing in various blockchain networks, regardless of the process that requires independence, agility, and credibility in digital records. Therefore, the objective of this study was to create a consensus mechanism process (pseudocode) exclusive to environmental occurrence records, allowing the validation of records and blocks with specific and careful environmental criteria. Despite the efficient and practical dynamics of other existing consensuses, the justification for its creation was to enumerate treatments catering to nature and biodiversity. Environmental occurrence records require a sensitive and qualified view of the data handled because they involve nature, society, and life. As a methodology, descriptive and bibliographic research was implemented to understand the functioning of the most common consensuses, each with its particularities. Additionally, symbols were applied to represent these occurrences, enabling digital interpretations of generally and purely analog contents, such as a simple rain event, now understood as a code that represents it, regarding its environmental impact. Furthermore, official codes representing natural or technological disaster occurrences were applied. These symbols will allow the classification of these occurrences for the technical selection of data validators.
Keywords: environmental consensus; environmental occurrences; ecological algorithm; environmental classification; environmental validation.

Mecanismo de consenso para *Blockchain* Ambiental: Prova de consciência ecológica (PoEa)

RESUMO: São inúmeros os mecanismos de consenso existentes em diversas redes *blockchain*, seja qual for o processo que necessite de independência, agilidade e credibilidade em registros digitais. Assim, o objetivo deste estudo foi de criar um processo (pseudocódigo) de mecanismo de consenso, exclusivo para registros de ocorrências ambientais, permitindo validar registros e blocos com critérios próprios e cuidadosos para o meio ambiente. A justificativa para criação, apesar da dinâmica eficiente e prática dos demais consensos existentes, foi o de enumerar tratamentos que atendessem a natureza e a biodiversidade. Registros de ocorrências ambientais necessitam de visão sensível e qualificada para os dados tratados, porque envolvem a natureza, a sociedade, a vida de modo geral. Como metodologia, fora implementada uma pesquisa descritiva e bibliográfica, conhecendo o funcionamento dos consensos mais comuns e cada qual com sua particularidade. Ainda, foram aplicadas simbologias para representatividades, possibilitando interpretações digitais de conteúdos, geralmente e puramente analógicos, como uma simples chuva, agora compreendida como um código que a representa, na sua forma como impacta no meio ambiente. Também, foram aplicados códigos oficiais que já representam ocorrências de desastres naturais ou tecnológicos. Essas simbologias permitirão a classificação dessas ocorrências para a seleção técnica dos validadores desses dados.
Palavras-chave: consenso ambiental; ocorrências ambientais; algoritmo ecológico; classificação ambiental; validação ambiental.

1. INTRODUCTION

Cryptocurrencies have become part of everyday life as a cultural element, more as digital assets than as actual currencies, as traditionally understood. Their distinguishing feature lies in a common triad: security, transparency, and decentralization (TAPSCOTT, 2017). This means they exist not through centralized or unilateral decisions, but because they are public, distributed, and secure. These characteristics are made possible by the underlying technology: blockchain (IANSITI; LAKHANI, 2020).

However, cryptocurrencies are not the only systems enabled by this technology. Once officially launched, the Drex (Digital Real Experiment) - Brazil's digital currency - will further illustrate blockchain's potential. Although Drex is not a cryptocurrency, but a fiat currency issued by the Central Bank of Brazil, it will incorporate blockchain-based features such as traceability, security, and data validation mechanisms like consensus protocols that authenticate and store information in blocks.

According to the Central Bank of Brazil (2024), Drex's blockchain employs the Proof-of-Authority (PoA) consensus mechanism. It is more sustainable as it does not rely on competitive problem-solving, as in other consensus algorithms, and therefore does not consume excessive energy. Additionally, due to its streamlined operation, PoA allows greater network scalability, helping prevent overload on blockchain nodes (i.e., participating users).

The key feature of PoA is the selection of network validators - participating users with verified identities and reputations - who bring an added layer of trust to the system (ZHANG et al., 2019).

Although the consensus mechanism is not the sole factor ensuring the security of blockchain technology, it is central to the system's operation, as it enables the creation, validation, and permanent recording of blocks and transactions on the network (CARREIRA et al., 2023).

Moving forward, this dynamic will be addressed: creating a consensus mechanism designed to operate on a blockchain for recording environmental occurrences. These could include records of events, historical data, environmental incidents, impacts, or any information that allows for the registration of evidence related to the environment, similar to what is already done in digital databases maintained by official Brazilian agencies, such as IBAMA, ICMBio, Civil Defense, among others.

The main issue here is not that existing consensus mechanisms, such as the one used for Drex, cannot be used; rather, it is necessary to consider that these records related to environmental occurrences are not merely simple, objective fields like date, amount, recipient, and payer, as in financial transactions and uniform processes.

Depending on the complexity of the information, especially considering the locations where the occurrences originate, numerous details are crucial and must be properly handled before being saved in a permanent record.

It is important to emphasize that these occurrences involve the environment, society, and living beings.

1.1. Blockchain Technology

According to Marchesin (2022), blockchain is a data structure (such as organized records, tables, and information) that lacks centralized control or a single hosting base (such as a central computer). This defines its decentralized nature: all participants possess, manage, and share information; no central authority or management exists.

Any information registered within a blockchain must undergo an evaluation and validation process before being permanently recorded. This is the role of the consensus mechanism. An algorithm must verify and confirm data entered into a blockchain-based file before it can be effectively written to the ledger (WALKER, 2018).

If the data is accurate, consistent, and trustworthy, it is permanently recorded as a block, and the updated blockchain is propagated to all file holders.

As Kuntz (2022) notes, although blockchain's concept and processes are simple, they require specific engineering, such as block recording, encryption, and key management. As cryptocurrency transactions are securely managed through blockchain, other processes - logistics, document handling, and more - can also be securely executed. This security goes beyond traditional digital methods..

1.2. Methodology

A descriptive and bibliographic research methodology was employed to define a consensus mechanism for validating environmental data records using blockchain technology. The aim was to investigate the technical processes that govern the implementation of various algorithms and their operational logic and practical applications (GIL, 2022).

It is important to note that blockchains handle computational records that may serve multiple purposes, such as cryptocurrency transactions, logistics operations, and others. Each has its own methods of classifying and interpreting data.

Consensus mechanisms are designed to validate and organize record data before forming the blocks that compose a blockchain network. Therefore, interpreting environmental records requires a degree of sensitivity, given their specific characteristics (FAHIM et al., 2023).

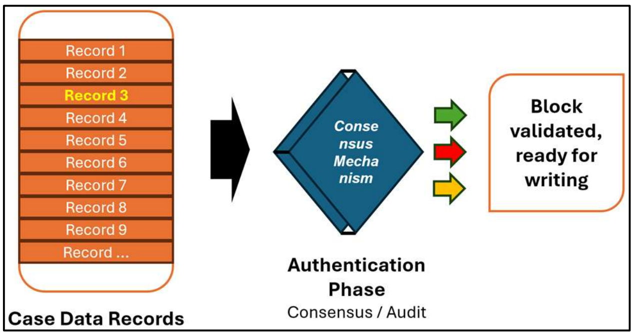

Figure 1. Performance of the consensus algorithm.
Figura 1. Atuação do algoritmo de consenso.

Differences among environmental occurrences require a qualified analysis. Some may cause positive or negative impacts, and in many cases, disasters. To properly validate such occurrences, it is essential to assign technically trained professionals to this task.

Although many events can be perceived as either beneficial or harmful, the degree of complexity and, most importantly, the consequences involved demand a more qualified perspective, since not all events are the same, and whether they are considered good or bad may depend merely on one's point of view.

A light rainfall may be beneficial, moistening farmland in one region while leading to flooding in another. Planting a tree may seem beneficial for all. Yet, these two events are not equivalent; both can be categorized and carry relevant information. Rain can turn into a flash flood, and depending on the species, a planted tree may alter the environment in ways that negatively affect biodiversity.

Therefore, a system of pre-classifications will be adopted to determine whether environmental occurrences are of anthropogenic or natural origin, given their potential consequences for society or the environment. This system aims to determine the expertise required from agents responsible for validating the data within the consensus mechanism.

The classification serves one specific purpose: to identify qualified nodes for validating each type of environmental record. Whenever necessary, these nodes must be represented by experienced and knowledgeable professionals.

Tables 1 and 2 will facilitate this process and provide a symbolic and functional classification for any environmental occurrence. They are based on Skinnerian Gains and Losses (CAVAGNARI; ANTIQUEIRA, 2023).

Skinner's theory is applied here as a logic model for interpreting human and natural actions on the environment. It categorizes their consequences as reinforcements and punishments (symbols), whether positive or negative. This approach organizes ecological impacts into gains and losses, composing a functional and sensitive environmental balance.

Table 1. Classification of Environmental Occurrences Based on Skinnerian Gains and Losses (Anthropogenic Responsible).
Table 1. Skinnerian Gains and Losses (Anthropogenic Responsible).

Affected Party	Actions and Reactions That Cause Consequences to the Affected	Skinnerian Gain or Loss	Symbol
Environment	Anthropogenic action that provides a gain or benefit to the environment	Positive Reinforcement	AE/R+
	Efforts by the responsible party to remove or avoid actions that could harm the environment	Negative Reinforcement	AE/R-
	Actions that harm the environment but may be reversible or result in future learning	Positive Punishment	AE/P+
	Actions that harm the environment in an irreversible or long-term manner	Negative Punishment	AE/P-
Society	Anthropogenic action that generates environmental gain for society	Positive Reinforcement	AS/R+
	Efforts to remove or avoid actions that could harm society	Negative Reinforcement	AS/R-
	Actions that harm society but may be reversible or lead to future learning	Positive Punishment	AS/P+
	Actions that harm society in an irreversible or long-term manner	Negative Punishment	AS/P-

Source: Cavagnari; Antiqueira (2023).

Table 2. Skinnerian Gains and Losses (Responsible Nature).
Tabela 2. Ganhos e Perdas Skinnerianos (Responsável Natureza).

Affected Party	Actions and Reactions That Cause Consequences to the Affected	Skinnerian Gain or Loss	Symbol
*Environment	Natural occurrences that may bring gain or benefit to the environment	Positive Reinforcement	NE/R+
	Natural occurrences that remove or correct previous alterations to nature (self-adjustments)	Negative Reinforcement	NE/R-
	Natural effects on the environment that may be reversible or bring future learning	Positive Punishment	NE/P+
	Natural effects on the environment that may be irreversible or long-term	Negative Punishment	NE/P-
*Society	Natural occurrences that generate environmental gains for society	Positive Reinforcement	NS/R+
	Natural occurrences that remove or correct prior alterations to nature	Negative Reinforcement	NS/R-
	Natural events that affect society, but may be reversible or lead to future learning	Positive Punishment	NS/P+
	Natural events that affect society and may be irreversible or long-term	Negative Punishment	NS/P-

Source: Cavagnari; Antiqueira (2023). Note: *Actions of nature directed at the environment or society often generate societal costs, even when beneficial to the environment. **Assessing natural occurrences and their consequences on the environment or society requires qualified expertise (e.g., geologists, forestry engineers).

The classifications presented in Tables 1 and 2 provide a logical framework for identifying environmental occurrences, whether disaster-related or not, whether anthropogenic or natural. These events may or may not cause environmental impact, affecting the environment or society, which may be positive or negative. A single occurrence may carry more than one classification symbol.

Applying the logic outlined in the tables makes it possible to associate any environmental event with a corresponding symbolic classification based on Skinnerian principles, always with care and proper documentation.

It is important to emphasize that the purpose of this framework is not to assign a final status or "label" to an occurrence, but rather to establish a hierarchy of assessment. The aim is not to classify events as good or bad, but to determine who can evaluate them properly.

Digital records that rely on consensus mechanisms, such as those found in blockchain systems, require clear typification to assign agents responsible for data validation correctly.

Environmental events may often appear simple due to their everyday nature. For instance, consciously and properly planting a tree is generally beneficial. Spilling oil on a beach is immediately perceived as highly damaging.

However, when it comes to natural events such as earthquakes, storms, or floods, the question of who benefits or who is harmed cannot be assessed by just anyone. Technical expertise is essential, not only for measurement but also for interpretation grounded in experience and scientific knowledge.

Take, for example, a volcanic eruption. It may drastically reshape a local landscape and create new biodiversity, representing, in Skinnerian terms, a positive punishment from nature to the environment, since it brings long-term ecological gains. On the other hand, such an event may cause the disappearance of an entire island along with its species, characterizing a negative punishment, where nature causes irreversible loss.

Even in such examples, oversimplified or common-sense classifications risk being misleading. That is why qualified professionals are essential for the classification process. Based on Tables 1 and 2, such symbolic categorization becomes a determinant factor in selecting blockchain record validators. Depending on the nature and severity of an event, whether human-caused or natural, these occurrences must be assessed and validated by competent experts.

Consider an example using Table 2: a record of pollination during early spring, geolocated in a specific region and documented by a local beekeeper. Such an occurrence may be assigned the code NE/R+, which indicates that nature generated a benefit to the environment (i.e., positive reinforcement, R+).

Due to the technical complexity of this validation, the consensus process for confirming this code may involve biologists or agronomists. The consensus algorithm itself is guided by symbolic logic derived from B.F. Skinner's behavioral theory may assist in selecting appropriate validators before submitting the record for approval.

In cases involving the classification of disasters, the COBRADE system (*Classificação e Codificação Brasileira de Desastres*) is applied. Public emergency and rescue agencies, such as Civil Defense and Fire Departments, use this official Brazilian classification and coding system for documentation and registry purposes (CAVAGNARI; ANTIQUEIRA, 2024).

COBRADE is a nationally specific system that was developed and adopted exclusively in Brazil. It catalogs disaster-related occurrences in official databases such as the Digital Atlas and Diário Oficial (Official Gazette).

Table 3 presents COBRADE classifications, which generate codes for digital disaster records that may also be found in public data repositories.

A corresponding code will be assigned as a classification key within the consensus mechanism for all environmental records, allowing for the appropriate distribution of validation responsibilities. In disaster-related cases, preference will be given to the official COBRADE code, where applicable.

Table 3. Brazilian Classification and Codification of Disasters – Cobrade Groups.
Tabela 3. Classificação e Codificação Brasileira de Desastres – Grupos do Cobrade.

Natural Disasters	Technological Disasters
1.1. Geological	2.1. Radioactive Substances
1.2. Hydrological	2.2. Hazardous Materials
1.3. Meteorological	2.3. Urban Fires
1.4. Climatological	2.4. Civil Engineering Works
1.5. Biological	2.5. Transport of Passengers and Non-Hazardous Cargo

Source: Ordinance No. 260, February 2, 2022.

Figure 2 illustrates the classification process: disaster-related occurrences classified by COBRADE are routed to specific professionals for record validation. Likewise, in non-disaster cases, occurrences are classified using B.F. Skinner's framework also guides the selection of qualified professionals for record validation.

It is important to note that the aim is not to develop a fully functional consensus algorithm at this stage, but rather to design the process and operational logic, a pseudocode for authenticating, creating, and recording blocks in a blockchain network. These stages require deep technical knowledge in computer science and applied cryptography for Distributed Ledger Technologies (DLTs) and blockchains.

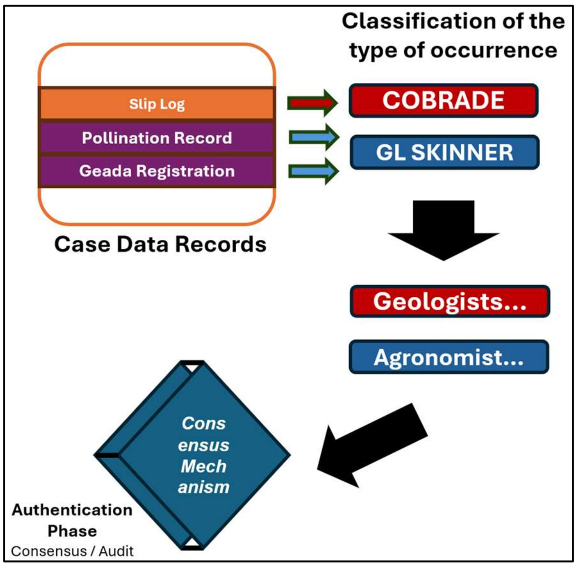

Figure 2. Case Classification for Validation.
Figura 2. Classificação da Ocorrência para Validação.

Environmental occurrences may take diverse forms and, as such, do not always demand highly technical or even publicly reported data. For example, rainfall along a riverbank may be digitally recorded by an environmental agency using meteorological volume data and brief field notes provided by a private company.

2. RESEARCH: blockchain and consensus mechanisms

Blockchain technology is now widely used in processes beyond its global debut with Bitcoin. Thus, it is impossible to discuss blockchain security without referring to cryptocurrencies, since cryptocurrencies can only be created through consensus based on algorithms and user participation (WALKER, 2018).

Before exploring how (and why) data blocks are written to a blockchain, it is essential to highlight the technology behind data security. This security is achieved through several mechanisms, such as the fact that each blockchain user stores a portion or the entirety of the blockchain data file. This is made possible by peer-to-peer (P2P) technology (KUNTZ, 2022).

According to Munhoz; Cavagnari (2019), P2P technology originated in the early days of the internet (1980s) and became widely known during the Napster era (1999–2002) for the unauthorized distribution of music files. In this system, music was not downloaded from a single source but from a network of users, each holding a fragment (node) of the file. The complete file was reconstructed from these pieces. A consensus algorithm (or consensus mechanism) refers to how blockchain participants (nodes) are designated to verify the information recorded in the blocks and transactions. The block is rejected and removed from the blockchain if any inconsistency is found, such as invalid digital signatures or date mismatches (CARAVINA, 2017).

In Bitcoin, for example, each block generates a unique number based on encrypted data. This number is hidden behind a digital puzzle known as a nonce. It is used only once and is required for the validator competition. Because the nonce is cryptographically complex, solving it requires immense computational power (KUNTZ, 2022).

Participants in the Bitcoin blockchain who compete to solve this puzzle are known as miners. The first to solve it earns the right to audit and write the block, receiving a bitcoin reward. This consensus process is called Proof of Work (PoW), a competitive validation method (KUNTZ, 2022).

Many other consensus algorithms vary depending on the type of blockchain, whether for cryptocurrencies or other use cases. The consensus algorithm defines the blockchain validation process's rules, flow, and security.

2.1. Consensus Mechanisms

A blockchain is a technology used to manage the recording of data blocks, structured information units. For this mechanism to work properly, it must guarantee freedom and security. However, it must ensure that data can be verified and permanently recorded. This is where consensus becomes essential: only validated, truthful data is written to the chain. Once written, data cannot be reversed; it becomes a permanent record (CARAVINA, 2017).

For example, even if a cryptocurrency blockchain is fully secure, the damage can be significant if a block is written with duplicate data due to a technical error or fraud. Imagine a case where a user accidentally or maliciously transfers cryptocurrency twice without intending to. This would result in financial loss, highlighting why the consensus stage is critical (KUNTZ, 2022).

Thus, consensus mechanisms are responsible for selecting, within the blockchain algorithm, nodes (participating users) to authenticate both records and blocks by evaluating the following criteria (KUNTZ, 2022):

a) Verification of digital signatures.
b) Validation of account balances (in the case of cryptocurrencies) to ensure sufficiency for the transaction.
c) Detection of duplicate records (whether accidental or fraudulent).
d) Block creation, i.e., permanent data writing.
e) Dispatch of the block to the network's chain of nodes.
f) Penalization of fraudulent or unethical behavior.
g) Among others.

This verification process is essential to ensure that records are not altered or contain unsupported information, such as a transaction between two accounts where the originating balance does not match the available funds. If there are insufficient funds, how could a transfer legitimately occur?

According to Fahum et al. (2023), this is one reason why decentralization is considered a security principle. Centralized systems are vulnerable to unilateral decisions and the risk of malicious or arbitrary actions, a power that carries significant responsibility.

This verification step is part of the judgment process for block writing and is designed to prevent errors or fraud. However, each consensus model also contains unique features and procedural specifics, from the selection of participating nodes (based on behavior, engagement, identity, reputation, etc.) to technical and operational factors such as data format, block size, processing time, and throughput (ZHANG et al., 2019).

Table 4 presents a selection of widely known consensus algorithms and their key differences. It provides insight into how consensus participants (nodes) are selected, the degree of decentralization achieved (or whether the mechanism risks forming a parallel control structure), and the impact on network scalability (capacity, speed, and energy consumption) and environmental sustainability.

To avoid an overload of concepts, consensus mechanisms that are structurally similar to those already listed, and despite being referenced in the bibliographic sources, have been omitted from the table for clarity and focus.

Table 4. Popular Consensus Algorithms.
Tabela 4. Algoritmos de Consenso Popular.

Consensus	Workings	Degree of Decentralization	Scalability / Sustainability
Proof-of-Work (PoW)	Highly random node selection is the concept of a miner. Whoever cracks the code first treats the block and receives a prize. Ex: Bitcoin.	High (any node can join the network). The need for high processing power can privilege and create parallel control and centralization.	Low scalability. Not very sustainable. Exacerbated use of energy to unravel the digital puzzle.
Proof-of-Stake (PoS)	Average randomness in node selection. The nodes that own the most digital assets are chosen because they are more solid and interested. Ex: Ethereum.	Despite the high level of decentralization, the technical condition of being a potential participant can regionalize or centralize power.	High scalability and sustainability. There is no excessive access and competition to mine.
Proof-of-Authority (PoA)	Low randomness. The identity verification process selects validators with an established reputation and identity. Ex: Drex.	Low (Requires proof of reputation). There are a few participants. The sacrifice of reputation conditions more ethical postures.	High scalability and sustainability. There is no excessive access and competition to mine.
Delegated Proof of Stake (DPoS)	Low randomness. Token holders (digital asset) choose delegates and witnesses. The more tokens, the greater the weight in the votes. Delegates create blocs; witnesses help in consensus. Ex: Bisares	Low (Network participants only. Choice by votes). Delegates must create and validate blocks, following the criteria. Any deviation is replaced.	Very high sustainability and scalability. There is no competition to mine, and the number of validators is reduced.
Proof of Importance (PoI)	Average randomness. The most active participants (holders of more coins, activity records, etc.) are chosen from the most present, most integrated. The most important ones. Ex: NEM (*New Economy Movement*).	Medium (The most active, highest-scoring participants are chosen). The diversity of us suppresses the possibility of cartels.	Very high sustainability and scalability. There is no competition to mine, and the number of validators is reduced.
Proof of Elapsed Time (PoET)	High randomness. Similar to PoW, but with time control, preventing high processing powers from setting the shortest time. Used to transact tokens, *smart contracts*, IoT and AI data.	Low (Nodes must have specialized hardware: SGX). The possibility of decentralization is very low. The distribution of time defines an equity, as everyone has compatible processing.	High scalability and sustainability. There is no excessive access and competition to mine.

Consensus	Workings	Degree of Decentralization	Scalability / Sustainability
Ordering Based Consensus (OBC)	High randomness. Similar to PoW, but with a time limit. Used for *supply chain records*, *smart contracts*, and medical records, among other processes.	Low. Resistant to defective knots. Lowers the possibility of decentralization, given the time control.	High scalability in terms of throughput and transactions. High sustainability. There is no competition to mine
Proof-of-Vote (PoV)	High randomness, similar to PoW and PoS. All nodes are called to vote on block authentication, which is used for product tracking, digital asset management, and more.	Very low, because it is very democratic.	High scalability and sustainability. There is no excessive access and competition to mine.
Proof-of-Capacity ou Proof-of-Space (PoC / PoSpace)	High randomness. Similar to PoW and PoS. They use the storage capacities of users, from their machines. Ex: Burstcoin.	High (any node can join the network). The need for space capacity may be privileged, but less than the processing power.	Medium scalability given the need to solve a puzzle. Medium sustainability. Despite the competition, it does not require processing power, but storage.

Source: ZHANG et. al (2019); FAHIM et. al (2023); OLIVEIRA et. al (2020); FERDOUS et. al (2020); YU et. al (2019).
Note: The sustainability criterion is based on reducing computer energy consumption. Competitive mining systems (puzzle-solving) require high processing power and significant energy use. Scalability primarily depends on network usage, specifically the Internet (simultaneously connected users). The more scalable a system is, the less likely users are to congest the network.
Fonte: ZHANG et. al (2019); FAHIM et. al (2023); OLIVEIRA et. al (2020); FERDOUS et. al (2020).
Nota: O critério de sustentabilidade baseia-se na redução do uso de energia em computadores. Sistemas de mineração competitivos (quebra-cabeça) exigem alto poder de processamento e consequentemente de energia. A escalabilidade baseia-se principalmente no uso da rede, internet (usuários conectados simultaneamente), quanto mais escalável, significa que menos usuários congestionam a rede.

Table 4 shows that these algorithms share a common goal: creating, auditing, and validating each data record and block. Each process focuses on selecting participants and evaluating how they may contribute to potential issues, especially regarding energy consumption and, by extension, environmental impact. This is particularly relevant in the case of the Proof-of-Work (PoW) algorithm, which relies on a competitive puzzle-solving process. The participant who uses the most processing power wins and is rewarded, resulting in excessive energy use for computational processing (CARAVINA, 2017).

This is not the case for more recent mechanisms, which allow processes to be adapted to the specific dynamics and needs of what is being recorded. These include new applications such as smart contracts, tokens, and logistics contexts that demand integrity, lower susceptibility to control or cartelization, and sustainability (SOARES, 2022).

3. DISCUSSION: Environmental Consensus Mechanism (Proof-of-Eco-Awareness, PoEa)

According to Barsano and Barbosa (2017), environmental management should aim to implement practices that ensure biodiversity preservation and conservation, recycling, and reduced environmental impacts on natural resources. This includes rehabilitating degraded areas, reforestation, and sustainable exploitation of natural resources. The scope also extends to environmental risk and impact studies and reusing non-serviceable waste.

Therefore, the authentication mechanism must align with environmental management principles when creating environmental occurrence records, whether for historical documentation or information management, using blockchain technology for secure and permanent storage.

According to Machado; Saccol (2016), environmental management begins with responsibility. Individuals and companies must feel compelled to act more responsibly and effectively for the collective well-being to live or participate in a healthy environment. Social responsibility is the starting point from which variations emerge to shape comprehensive environmental governance.

The individuals and organizations committed to these principles should form the nodes in an environmental blockchain network, creating records that contribute to building a place's environmental history, even minimally impactful ones.

Drawing on the Proof-of-Authority (PoA) concept, in which identity and participant reputation are central, validating blocks containing sensitive environmental records may be crucial for ensuring data quality (KUNTZ, 2022).

However, it is important to note that not all block sets of occurrence records require high-level validation. Some occurrences may be minor yet just as sensitive, and may not warrant rigorous consensus processes.

This leads to the proposal of block flexibility (e.g., in terms of recording time or size), as seen in the mechanisms discussed earlier. Each one accommodates specific needs and contexts. Similarly, an environmental consensus model may follow its own rules, shaped by the dynamics of environmental data.

In many cases, regardless of how isolated the event may be, block validation must be based on ethical standards and often on technical or scientific data if it involves a significant environmental occurrence. The reputation of the validator is paramount in such situations.

Additionally, validators and participants in an environmental blockchain do not need to be permanent ecosystem members, such as residents or researchers. Support entities (e.g., civil defense, fire departments, police) that intervene during incidents may be qualified to observe, document, and authenticate environmental records.

It is also worth noting that environmental occurrences take many forms and do not always require extensive technical input or media coverage. For instance, rainfall along a riverbank may be recorded digitally, measured by meteorological agencies, and briefly reported in a weather bulletin.

Such a record could be confirmed through participatory methods, where the local community validates the event and the block is accepted. This process may also be automated, relying solely on algorithmic validation without human intervention. Conversely, a rain event leading to landslides or floods must be thoroughly documented. Advanced validation with clearly defined responsibilities would be necessary to ensure the accuracy of the corresponding block.

Environmental events that may cause societal or ecological damage must be treated differently from routine occurrences. The validation method must be adapted accordingly, depending on the event's location and nature.

In cryptocurrency blockchains, like Bitcoin or Ethereum, each recorded block grants a defined monetary reward to the validating node, which is an incentive for maintaining the process (CARAVINA, 2017).

Direct monetary compensation may not be feasible in environmental blockchains, though other forms of value may exist. For instance, prizes could be awarded based on the region where the environmental record was made. Often, the value lies in recording itself, a benefit shared with the entire community and broader society.

Alternatively, beyond the collective benefit, companies and governments may earn carbon credits or tax reductions as compensation for responsible environmental data recording. Communities, in turn, may gain access to public services or improved oversight, representing meaningful gains in well-being.

It is important to recognize that a blockchain-based environmental record is technically permanent, lasting for generations. To assume that its mere existence justifies the system is utopian. An intentional, value-driven design and use must be aligned with ecological responsibility.

2.2. Block Creation, Authentication, and Recording

The main function of the consensus mechanism is to create blocks based on data records. Once these records are authenticated, they are permanently recorded, forming the blockchain network (ZHANG et al., 2019).

The block creation process differs from that of cryptocurrencies in the context of environmental occurrence records. Instead of cash flow, there is a flow of lived experience and occurrences. The place's biography is the transacted value.

According to Zhang et al. (2019), in a blockchain network, consensus is a mechanism that enables the distributed network to reach agreement on the value of shared data, providing a consistent and reliable state even when one or more nodes are untrustworthy due to corruption or hardware failure. Therefore, the functioning of environmental records should rely on processes that account for the particular dynamics involved. This justifies the need for a uniquely environmental consensus mechanism that is secure and ecologically conscious. Ecological consciousness also involves recognizing the value of those with deep knowledge of the subject.

Suppose an environmental occurrence is recorded simply as a light spring rain. In that case, this does not mean that there are no technical institutions to determine the volume of rainfall or that the event lacks importance. And if the location in question exceeds the scope of technical measurement, witnesses and evidence may suffice. While such rainfall may seem trivial, depending on the area to which the data refers, it may be essential for explaining future or recurring phenomena.

Moreover, there may be no news coverage for everyday events recorded and experienced by communities as part of the place's natural biography. People may record observations like "sunny day," "strong wind," "rain," "cold," or "heat." A single record may seem insignificant, but dozens or hundreds of such entries can collectively signal larger events. Even so, the biography itself already holds value.

Thus, based on the characteristics of the consensus algorithms examined here and their potential and requirements for managing a blockchain network, this study proposes criteria for block creation, authentication (validation), recording, and distribution in a blockchain system.

2.2.1. Validator Selection

In most consensus mechanisms, validation occurs randomly. That is, in cases where there are no specific restrictions, only competition to solve a puzzle and earn a reward (as in Proof of Work), or where validators are selected based on their stake and participation in the network, such as in Proof of Stake (FAHIM et al., 2023). In this context, the validator must ensure that many data elements, such as dates, signatures, and values, make sense. This does not imply a lack of technical requirements but highlights the difficulty of finding someone qualified for such work.

This difficulty may be even greater for a blockchain with environmental occurrence records. Certain records require specific technical expertise. For example, recording a windstorm involves triangulating data for a specific area and measuring wind speed, rainfall levels, and temperature, among other metrics, which, even when accurate, must be interpreted and validated by qualified experience.

It is therefore essential that validators of environmental consensus be selected through two distinct pathways:

– Internal Selection: Users actively contribute data or information to the network. Examples include local community members monitored by the blockchain, researchers, or environmental monitoring companies.
– External Selection: Users connected to participants or invited entities, such as technical institutions, civil defense agencies, police, fire departments, etc., who possess or can access the necessary technical capacity.

As previously discussed, the required technical capacity depends on the nature of the event being recorded.

As part of the selection criteria, the concept of delegates and witnesses, used in the DPoS (Delegated Proof of Stake) consensus mechanism (see Table 4), is considered particularly suitable for validating environmental blocks, due to its emphasis on responsibility and security.

According to Fahim et al. (2023), the DPoS mechanism, like PoS, divides validator roles into three groups: witnesses, delegates, and workers. Participants in the blockchain network choose witnesses, validators and block creators. Those holding more digital assets have greater voting power in selecting these witnesses.

Delegates are responsible for governance. They propose and vote on protocol changes, updates, and other critical decisions affecting the blockchain's dynamics. They represent the will of the network participants. Workers submit proposals to the network, from process improvements to algorithmic changes (FAHIM, 2023).

In the case of simpler occurrence records, such as ordinary rainfall or community-led tree planting, technical information may support validators through algorithms or even artificial intelligence. These are referred to as automatic validations or pre-validations. For example, as previously noted, algorithms may classify events based on the Skinner GL model (Tables 1 and 2) or COBRADE (Table 3). Depending on the classification, the more technical analysis is required, the stricter the validator selection criteria. This classification may be either automated or suggestive.

Thus, similar to the DPoS model, environmental records require a validator selection process based on Delegate and Witness, which ensures accountability and the necessary caution for environmental integrity.

Once the records are created and classified, the roles of Delegates and Witnesses would be divided as follows:

- Witnesses: These are responsible for confirming the recorded information. They may be chosen from within the network or nominated by participants. For instance, a civil defense representative monitoring an occurrence, though not part of the network, may act as a witness. Witnesses can be permanent or randomly selected, depending on the classification of the occurrence.
- Delegates: Elected by the network's participants. They may be directly or indirectly involved as technical contributors, but must have verified qualifications and identity. Delegates are responsible for monitoring the activities of all participants, including the witnesses. They are also tasked with defining special rules for block recording and proposing specific procedures, such as allowing deletion or continuation of records and the creation of future blocks. Delegates may be pre-defined depending on the geographic context or appointed based on operational demand. A pre-registered pool of Delegates is recommended to ensure a rotation system.

To clarify the role of these participants, specifically Delegates and Witnesses, a simulation is presented based on how participants would be selected within an environmental blockchain. This example focuses on the information recording process in a Conservation Unit (CU) surrounding a dam, including both the dam and its natural surroundings:

1) Participants in this blockchain include residents and businesses, the regional sanitation company, a satellite-based climate monitoring center, a biodiversity research institute, and faculty researchers from a nearby university.
2) As programmed, the consensus algorithm randomly selects Witnesses from among the network's participants each week to observe and review the records being submitted.
3) Users more actively engaged in the network earn greater voting power when selecting delegates.
4) Delegates are officially identified candidates willing to serve in this role.
5) The algorithm assigns a maximum term of two years for each Delegate.
6) New candidates replace delegates who fail to act in two consecutive validation requests.
7) Delegates must possess technical credibility and reputation. They must either validate the records themselves (according to classification level) or nominate qualified professionals to do so under their responsibility.
8) The motivation to become a Delegate comes from the rewards offered. The responsible Delegate(s) receive a reward for every validated block.
9) The reward, established by the blockchain network in partnership with the federal government, may be tax exemptions, income tax deductions, or other government-regulated incentives.

To illustrate the validation process, a simulation of environmental events in this blockchain network is outlined:

1) One morning, local residents notice a strong windstorm. A resident initiates an environmental record.
2) Other residents confirm or expand upon the report. An algorithm checks for duplicate entries of the same event.
3) The windstorm causes trees to fall and triggers a dam overflow. Civil defense and fire departments, as well as local news outlets, are notified.
4) The climate monitoring company triangulates and records real-time data. A second record is created: dam overflow.
5) Civil defense identifies flooding and begins evacuating residents. A third record is proposed: flooding.
6) Additional participants, including the climate agency, input supplementary data.
7) Civil defense and fire department technicians contribute key data to support classification of the events (e.g., using COBRADE or Skinner GL models).
8) Certain data points and classifications can be suggested or generated automatically by algorithms or AI tools.
9) After all records related to the initial rainstorm (rain → wind → windstorm → overflow → flood) are created, they remain pending validation.
10) Dozens of entries are unified into specific events. Algorithms pre-validate data for consistency (e.g., time, date, values, triangulation).
11) Automatic data, including temperature, humidity, and atmospheric pressure, is gathered from monitoring agencies and environmental sensor stations throughout the CU.
12) Records enter a waiting period for auto-confirmation, pending formal reports from civil defense and emergency response.
13) An algorithm categorizes records as complete, incomplete, or awaiting additional information.
14) Complete records enter the next phase, where available, Delegates are selected.
15) Delegates (or their nominated experts) verify the information. Witnesses participate in the audit process.
16) Events tagged with COBRADE or Skinner GL classifications trigger the assignment of specific professionals for observation.
17) The algorithm flags incomplete, suggestive, or ready-to-finalize records.
18) Delegates and Witnesses begin formal validation. Once complete, the block is digitally signed (by Delegates) and permanently recorded on the blockchain.
19) The validators' contributions are logged. They receive certification of participation, potentially with carbon credit or professional development benefits. This is recorded eternally as part of an "environmental participation résumé."
20) Certification provides verifiable evidence of the Delegate's work and supports potential tax benefit claims.

This simulation shows that environmental, natural, and societal events, not purely financial incentives or calendarbased cycles, drive the validator selection process. It reflects the natural lifecycle of ecosystems. Specific operational criteria for each blockchain, such as the rules governing delegate replacement or inactivity, can be customized based on its location.

The validator selection process in environmental blockchain systems should consider the following principles:

a) The nature, type, and form of the occurrences depend on the environmental context where the blockchain operates.
b) A single event may evolve into multiple distinct records (e.g., rain → wind → storm).
c) Many records can be generated automatically using calibrated algorithms and appropriate technology (e.g., sensors).
d) Delegates are essential for validating records that require specialized expertise.
e) Event classification systems (e.g., regulatory, disaster response, or taxonomy-based) help define appropriate validation workflows.
f) Incentives such as rewards, benefits, or certifications must be implemented to foster engagement and interest.
g) Each natural environment may define its reward logic for validators. However, at a minimum, each validator should receive a permanent participation certificate, immutably recorded on the blockchain.

2.2.2. Block Creation

A block is a set of created and grouped records. Once enough records are aggregated, a temporary or candidate block (i.e., not yet finalized) exists. Because of this block's presence, validators are selected.

The finalized block is immutable; it cannot be changed once sealed. This underscores the importance of establishing rigorous criteria: "immutable" is not an exaggeration in this context.

The provisional block aggregates, reviews, and classifies records. It is available to all network nodes and openly marked as "under validation." At this stage, each record has one of two statuses: open or closed.

- Open records are still under review and not ready for final validation or recording. These may be eliminated if not completed within the set rules or deadlines.
- Records can also be flagged for future continuation. Environmental events may evolve or lead to new incidents, which must be structured in the network's architecture.

The block is finalized once Delegates verify it and it is not contested by Witnesses. At this point, metadata such as block headers (e.g., timestamp, size) and block creation data are compiled.

2.2.3. Block Validation, Authentication, and Recording

According to Kuntz (2022), validation and authentication involve auditing and reviewing a block's contents. Standard blockchain checks are performed, including hash comparisons and digital signatures. Additionally, some records may be canceled without compromising the integrity of the entire block. A block may also be held temporarily if the related event is ongoing or under technical review. Validation rules depend on the nature of the event and the monitored location.

Record auditing can be performed by a team of professionals, composed of delegates. Participants may include civil defense personnel, police, firefighters, journalists, researchers, etc.

These individuals may act as active auditors (direct network participants) or passive auditors (contributing indirectly via reports shared with the network).

Witnesses, regardless of their expertise, serve to oversee the validation process.

Before block creation, the algorithm may select key fields in the records for pre-evaluation, highlighting critical points or suggesting areas for closer scrutiny. AI can support this process in specific environments.

Evaluation criteria vary by location, but the algorithm can automatically validate basic technical data. For instance, a temperature report of -5 °C in Salvador, Brazil, during summer would be flagged. A local criteria table can guide these sanity checks.

Delegates are responsible for completing missing technical fields, such as rainfall measurement, wind speed, and triangulation. These should normally be filled out during record creation. If not, and if no Delegate can supplement the missing data, the record may be discarded.

Once all records are validated and authenticated, the block header is finalized with security and metadata information. The block is then broadcast to all nodes.

Recording is irreversible. However, as these are not monetary transactions but occurrence records, complementary notes or corrections may be added in future blocks. A parallel algorithm can manage linking keys and ensure relational consistency across related blocks.

Figure 3 (not included here) illustrates a potential data creation flow for Block 1, accounting for occurrence continuity (inheritance). Participants fill out predefined record forms, which are compiled into the block.

The block is created with these records in the next phase and goes through consensus or auditing. As shown in Figure 3, records 4 and 10 were eliminated due to missing data that could not be supplemented, or due to divergences or inconsistencies. In this phase, records 3 and 9 are also marked as likely to continue in the occurrences or be directly inherited (such as flooding, for example). Records 4 and 10 in the illustration are disregarded in the block recording phase. The block is recorded. As exemplified in the illustration, six blocks were recorded definitively later, and evidence appears in record 8 of block 7, as a consequence linked to record 3, still from block 1.

The eco-awareness mechanism can control these inheritances in its algorithm. As reported, these are environmental records of occurrences affecting the environment, living beings and diversity. Continuity is certain in most occurrences.

Nativa, Sinop, v. 13, n. 2, p. 234-246, 2025.
Pesquisas Agrárias e Ambientais
DOI: https://doi.org/10.31413/nat.v13i2.19055
ISSN: 2318-7670

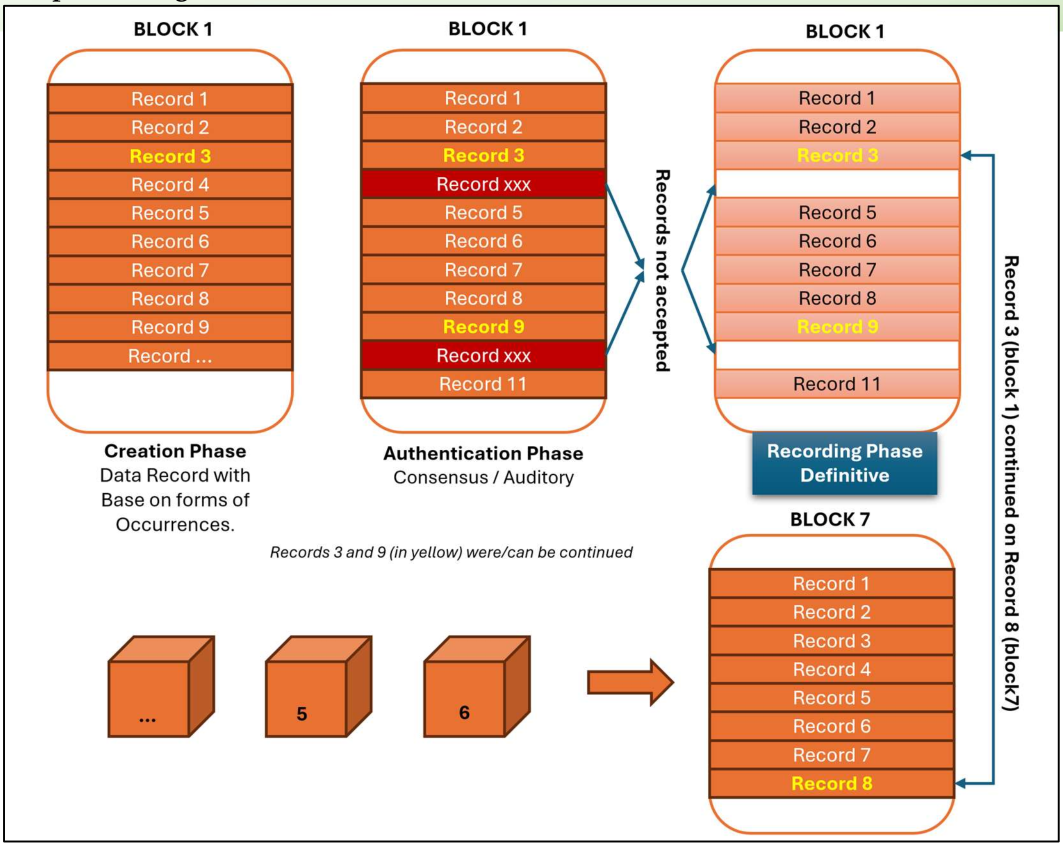

Figure 3. Simulation of Registration, Creation, Consensus, and Recording of Blocks on the *Blockchain* (With Inheritance Registration).Figura 3. Simulação de Registro, Criação, Consenso e Gravação dos Blocos no *Blockchain* (Com registro herança).

4. FINAL CONSIDERATIONS

Environmental events can lead to incidents and impacts that affect life and the environment, now and in the future. These events may be positive, bringing benefits or learning, or negative, resulting in discomfort or irreversible consequences.

From a technical standpoint, the consensus mechanism and its algorithm can be compared with others previously studied (see Table 4), particularly in how validator selection is minimally randomized, a necessary condition for ensuring the integrity of environmental records.

Furthermore, the mechanism avoids centralization of power or control by specific groups, thanks to the rotation requirement for Delegates. It is highly scalable, consuming minimal network processing resources, which results in significant energy efficiency and sustainability.

It is also evident that even the simplest records, while possibly submitted by lay observers, would not be accepted lightly by a well-designed consensus mechanism. Such a mechanism would reject data that is exaggerated or lacking in substantiating evidence.

Participation's inclusive nature is crucial. Anyone can contribute to the environmental biography recorded via blockchain. This broad engagement enhances the richness and comprehensiveness of environmental records, from the simplest to the most complex.

The perspective of those living near the monitored site, agencies that oversee and report on events, and those providing life-saving services is essential to the data recording and validation process. Scholars and students who observe, study, and document such occurrences also play a key role in shaping validation criteria and practices.

Moreover, the classification of occurrences should go beyond disaster frameworks like COBRADE to include a wide spectrum of environmental events, from planting a seedling to managing a forest fire. This creates a digital identity that supports validation and proper documentation.

Another key factor is the selection of validators, particularly Delegates who assume responsibility and contribute recognized expertise, and Witnesses who certify the data validation process. Their work is rewarded through technical incentives, social recognition, and personal reputation.

PoEa is not merely a technical proposal. It represents a new paradigm for validating sensitive environmental data, grounded in ethical, ecological, and collaborative principles..

5. CONCLUSIONS

This study proposed the foundations for a consensus mechanism tailored to environmental occurrences: the Proof-of-Eco-Awareness (PoEa). This model reflects the inherent complexity of life and the dynamic, evolving nature of environmental events.

To develop this model, several research stages were required to translate complex and constantly changing information into a structured system, while considering the unique traits of nature and living organisms.

The ability to classify environmental occurrences beyond predefined disaster categories allowed the establishment of logical processes for validator selection, block creation and recording, leveraging blockchain technology.

Although each environmental site may require specific data fields or customized logic, a consensus mechanism for environmental blockchains, based on ecological awareness, ensures that records are generated consciously and contextually, aligned with the integrity that environmental stewardship demands.

Thus, this consensus model is expected to serve as the foundation for blockchain-based environmental recording, monitoring, and management in forests, conservation units, protected areas, neighborhoods, cities, and parks, anywhere nature and society coexist within an environmental system.

6. REFERENCES

ALVARENGA, A. L. **DeFi - Criptomoedas e as Finanças Descentralizadas**. Disponível em: <https://ler.amazon.com.br/?asin=B099P33ZMC>. Acessado em: 07 Jul. 2021.

Banco Central do Brasil – Bacen. **Drex – Digital Brazilian Real**. Disponível em: < https://www.bcb.gov.br/en/financialstability/drex_en >. Acessado em: 06 Jun. 2024.

BARSANO, P. R.; BARBOSA, R. P. **Gestão Ambiental**. São Paulo: Editora Saraiva, 2017. 128p.

BRASIL. MDR - Ministério da Integração e do Desenvolvimento Regional. **Classificação e Codificação Brasileira de Desastres (COBRADE)**. Disponível em: <https://www.gov.br/mdr/pt-br/centrais-de-conteudo/publicacoes/protecao-e-defesa-civil-sedec/DOCU_cobrade2.pdf>. Acessado em: 03 Mar. 2024.

BRASIL. Ministério do Meio Ambiente (MMA). Conselho Nacional do Meio Ambiente (CONAMA). **Resolução CONAMA Nº 1, de 23/01/1986**. Dispõe sobre critérios básicos e diretrizes gerais para a avaliação de impacto ambiental. Disponível em: < https://www.ibama.gov.br/sophia/cnia/legislacao/MMA/RE0001-230186.PDF>. Acessado em: 20 Abr. 2022.

BRASIL. Presidência da República. **Lei 9.795 de 27 de abril de 1999**. Institui a Política Nacional de Educação Ambiental. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/l9795.htm>. Acessado em: 07 Jun. 2021.

CARAVINA, A. **Bitcoin e Altcoins – fácil, prático e completo**. eBook Kindle, 2017. 1534p.

CARREIRA, G.; MELO, J.; ROQUE, L. **Real Digital e a utilização de Hyperledger Besu na AWS**. Disponível em: <https://aws.amazon.com/pt/blogs/aws-brasil/real-digital-e-a-utilizacao-de-hyperledger-besu-na-aws/ >. Acessado em: 30 Nov. 2023.

CARVALHO, F.; PAULA, L. F. R. de; SICSÚ, J.; SOUZA, F.; STUDART, R. **Economia Monetária e Financeira - Teoria e Política**. São Paulo: Elsevier Educacional, 2021. 408p.

CAVAGNARI, D. W.; ANTIQUEIRA, L. M. O. R. Balanço ambiental Skinneriano: reforço e punição como ganhos e perdas e registro digital. **Nativa**, v. 11, n. 3, p. 384-395, 2023. https://doi.org/10.31413/nat.v12i1.16781

CAVAGNARI, D. W.; ANTIQUEIRA, L. M. O. R. Registros Digitais de Ocorrências Ambientais para o Brasil: Desastres Naturais e Tecnológicos. **Nativa**, v. 12, n. 1, p. 102-117, 2024. https://doi.org/10.31413/nat.v12i1.16781

CAVAGNARI, D. W. Cryptocurrency e uma nova economia. In: **Blockchain e Criptomoedas**. Curitiba: Intersaberes, 2024. 150p.

DA PEREIRA, A. C.; SILVA, G. Z.; CARBONARI, M. E. E. **Sustentabilidade, responsabilidade social e meio ambiente**. São Paulo: Editora Saraiva, 2011. 216p.

DIAS, R. **Gestão ambiental - responsabilidade social e sustentabilidade**. 3 ed. Rio de Janeiro: Atlas, 2017. 248p.

ETHEREUM.org. **The Merge**. Disponível em: <https://ethereum.org/en/roadmap/merge/>. Acessado em: 30 Jun 2023.

FAHIM, S.; RAHMAN, S. M. K.; MAHMOOD, S. *Blockchain*: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV. **International Journal of Mathematical Sciences and Computing**, v. 9, n. 3, p. 46-57, 2023. https://doi.org/10.5815/ijmsc.2023.03.04

FERDOUS, Md. S.; CHOWDHURY, M. J. M.; HOQUE, M. A.; COLMAN, A. *Blockchain* Consensus Algorithms: A Survey **ArXiv**, e2001.07091, p. 1-39, 2020. Disponível em: <https://arxiv.org/pdf/2001.07091>. Acessado em: 07 Mai. 2025.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7 ed. Rio de Janeiro: Atlas, 2022. 208p.

HOLZER, W. O conceito de lugar na geografia cultural-humanista: uma contribuição para a geografia contemporânea. **Geografia**, v. 10, p. 113-123, 2003.

HUANG, Q.; CERVONE, G.; ZHANG, G. A cloud-enabled automatic disaster analysis system of multi-sourced data streams: An example synthesizing social media, remote sensing and Wikipedia data. **Computers, Environment and Urban Systems**, v. 66, p. 23-37, 2017. https://doi.org/10.1016/j.compenvurbsys.2017.06.004

KUNTZ, J. ***Blockchain* Ethereum – fundamentos de arquitetura, desenvolvimento de contratos e aplicações**. São Paulo: Casa do Código, 2022. 295p.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 5 ed. São Paulo: Atlas, 2003. 312p.

LANSITI, M.; LAKHANI, K. R. **The truth about *Blockchain*.** Disponível em <https://hbr.org/2017/01/the-truth-about-*blockchain*>. Acessado em: 05 Dez. 2020.

MACHADO, V. de S.; SACCOL, J. **Introdução à gestão ambiental**. Porto Alegre: SAGAH, 2016. 114p.

MARCHESIN, K. B. K. ***Blockchain* e Smart Contracts: As Inovações no Âmbito do Direito**. São Paulo: Editora Saraiva, 2022. 114p.

MARCONI, M. de A.; LAKATOS, E. M. **Metodologia Científica**. 8 ed. Rio de Janeiro: Atlas, 2022. 256p.

MASSADAR, R. **Mineração de criptomoedas: tudo o que você precisa saber.** Disponível em <https://financeone.com.br/mineracao-de-criptomoedas-tudo-precisa-saber/>. Acessado em: 11 Jul. 2021.

NORTON, T.; ROHWER, M. **O potencial do *Blockchain* para a Sustentabilidade.** Disponível em: <https://www.thomsonreuters.com.br/pt/juridico/blog/o-potencial-do-*blockchain*-para-a-sustentabilidade.html>. Acessado em: 11 Ago. 2020.

OLIVEIRA, M. T. de; REIS, L. H. A.; MEDEIROS, D. S. V.; CARRANO, R. C.; OLABARRIAGA, S. D.; MATTOS, D. M. F. *Blockchain* reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications. **Computer Networks**, v. 179, e107367, 2020. https://doi.org/10.1016/j.comnet.2020.107367

PÁDUA, E. M. M. **Metodologia da pesquisa: abordagem teórico-prática**. 3 ed. Campinas-SP: Papirus, 2017. 144p.

PHILIPPI JR, A. (Coord). **Coleção Ambiental - Gestão de natureza pública e sustentabilidade**. Barueri: Manole, 2012. 1108p.

PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do Trabalho Científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2 ed. Novo Hamburgo: Feevale, 2013. 276p.

SIMEPAR_Sistema de Tecnologia e Monitoramento Ambiental do Paraná. **Boletim Climatológico.** Disponível em: <http://www.simepar.br/prognozweb/simepar/timeline/boletim_climatologico>. Acessado em: 07 Jul. 2021.

SOARES, M. J. P. **Ethereum – Breve História e Suas Possibilidades.** eBook Kindle, 2022. 24p.

STEPHEN, A. **Worldchanging: a user´s guide for de 21st century**. New York: Harry N. Abrams Edition Unstated edition, 2008. 600p.

TAPSCOTT, D. ***Blockchain* Revolution**. São Paulo: SENAI, 2017. 392p.

WALKER, W. ***Blockchain*: Aplicações no Mundo Real e Compreensão: Como a *Blockchain* Pode Ser Aplicada em Seu Mundo**. eBook Wayne Walker, 2021. 42p.

WILLIAM, S. **Criptografia e segurança de redes: princípios e práticas**. 6 ed. São Paulo: Pearson Education do Brasil, 2015. 560p.

WORLD ECONOMIC FORUM - PWC. **Fourth Industrial Revolution for the Earth Series. Building block(chain)s for a better planet - September 2018**. Disponível em: <https://www.pwc.com/gx/en/sustainability/assets/*blockchain*-for-a-better-planet.pdf>. Acessado em: 19 Jul. 2021.

YU, B.; LIU, J.; NEPAL, S.; YU, J.; RIMBA, P. Proof-of-QoS: QoS based *blockchain* consensus protocol. **Computers & Security**, v. 87, e101580, 2019. https://doi.org/10.1016/j.cose.2019.101580

ZHANG, P.; SCHMIDT, D. C.; WHITE, J.; DUBEY, A. Chapter Seven - Consensus mechanisms and information security Technologies. **Advances in Computers**, v. 115, p. 181-209, 2019. https://doi.org/10.1016/bs.adcom.2019.05.001

Authors' Contributions: D.W.C. – conceptualization, research, methodology, data collection, proofreading, scientific reading, conceptualization, submission, writing (review and editing) and publication; L.M.O.R.A. – advisor, supervision, review. All authors read the article in its final version and approved its publication.

First author's dedication: "In memory of Dilma Adelaide, who passed away on May 7, 2025. Her loving presence and tireless dedication deeply impacted my life."

Institutional committee review: Not applicable.

Ethics Committee: Not applicable.

Data availability: The study data can be obtained upon request from the corresponding author via e-mail.

Conflict of Interest: The authors declare no conflicts of interest with other researchers or institutions..