PLOS Climate

RESEARCH ARTICLE

A proof-of-stake blockchain framework for transparent climate data verification

Thomas F. Heston[1,2]*

1 Department of Family Medicine, University of Washington, Seattle, Washington, United States of America, **2** Department of Medical Education and Clinical Sciences, Washington State University, Spokane, Washington, United States of America

* theston@uw.edu

Abstract

Trust in climate data remains a significant barrier to effective climate action. Skepticism about data manipulation and politicization reduces confidence and hinders evidence-based policy. Existing climate data systems lack transparent verification and accessible analytical tools, limiting accountability and stakeholder engagement. This study presents a reproducible framework that applies blockchain technology to provide transparent verification, analysis, and governance of climate data. The architecture includes three layers: a data ingestion layer that standardizes verified observations, a blockchain layer that ensures immutability and provenance through proof-of-stake consensus, and a statistical analysis layer that uses deterministic methods for anomaly detection and trend evaluation. The framework was tested using 8,403 hours of temperature data from the Manila, Philippines monitoring station during 2024. Analysis identified 33 temperature anomalies ranging from 36.9 to 38.0 °C that aligned with documented April–May 2024 heat waves, confirming the ability to detect genuine meteorological extremes. Estimated transaction latency was 1–2 seconds per observation, with on-chain storage requirements of about 138 kilobytes and off-chain storage requirements of 2.1 megabytes for a 90-day deployment. Estimated energy use for the same period was approximately 0.06 kilowatt-hours, representing a 97–99 percent reduction compared with proof-of-work systems. These findings demonstrate that the proposed framework can securely record, verify, and analyze climate data while consuming very little energy. By combining blockchain immutability with transparent statistical methods, this approach directly addresses the trust deficit in climate science and provides a foundation for verifiable, reproducible, and efficient climate information systems.

OPEN ACCESS

Citation: Heston TF (2026) A proof-of-stake blockchain framework for transparent climate data verification. PLOS Clim 5(6): e0000764. https://doi.org/10.1371/journal.pclm.0000764

Editor: Bo Li, Texas A&M University, UNITED STATES OF AMERICA

Received: October 31, 2025

Accepted: May 16, 2026

Published: June 11, 2026

Data availability statement: All data, analytical code, output files, and figure-generating code are publicly archived in Zenodo at https://doi.org/10.5281/zenodo.17429218. The repository includes the raw NOAA observation file, the Jupyter notebook implementing the quality-control and anomaly-detection pipeline, the sensitivity analysis, and the anomaly output file. NOAA data are public domain.

Introduction

Climate data systems face a fundamental tension between the need for institutional coordination and the demand for independent verification. Public trust in climate

Funding: The author(s) received no specific funding for this work.

Competing interests: The authors have declared that no competing interests exist.

science is necessary for the adoption of mitigation and adaptation policies, yet skepticism often centers less on the underlying physics of climate change than on whether institutions collect, store, and interpret climate data transparently and in a trustworthy way. When data provenance is unclear and analytical workflows cannot be independently checked, disputes about integrity can undermine confidence in both the evidence and the policies built on it. This study addresses that problem by examining whether a blockchain-based verification framework can improve transparency, reproducibility, and auditability in climate data systems.

Motivation

Evidence suggests that public trust in climate science is deeply tied to the perceived trustworthiness of experts, institutions, and the information they provide [1]. Skepticism about the trustworthiness of climate scientists' claims often involves beliefs that the science behind global warming has been invented or distorted for ideological reasons, financial reasons, or that their models are excessively inaccurate [2,3]. This distrust influences whether governments initiate mitigation and adaptation efforts, and strong opposition from skeptical segments of the public has thwarted efforts to create a low-carbon economy and sparked controversy over renewable energy development [4]. Furthermore, the rhetoric of data transparency has sometimes been weaponized by government agencies to exclude certain scientific research and weaken environmental and public health protections [5].

Improving transparency, security, and reproducibility is a critical challenge across diverse data systems. In cognitive and neuropsychological research, detailed reporting standards are necessary to ensure that study designs and analytical methods are reproducible [6]. In educational environments, strict identity management and access control limit system access to safeguard sensitive resources [7]. In the environmental sciences, although climate data are collected globally, restricted access and a lack of harmonized datasets can hinder scientific replication and lead to fragmented metadata [8,9]. Analyzing these complex climate models is technically demanding, often requiring specialized expertise and significant computational resources [10]. Furthermore, in healthcare, overcoming the vulnerabilities of centralized architectures requires advanced mechanisms, such as blockchain-enabled audit trails, to provide tamper-evident records and prevent unauthorized data manipulation in electronic health records [11].

Emerging digital technologies offer a possible remedy. Distributed ledger systems in other settings, such as healthcare, have demonstrated tamper-evident data storage and robust intrusion prevention, allowing any participant to verify that records remain unaltered while protecting networks from unauthorized access [12–15]. Proof-of-stake consensus mechanisms achieve this transparency with minimal energy use, making blockchain suitable for environmentally sensitive applications [16]. Early applications in carbon credit markets [17], renewable-energy certification [18], and peer-to-peer electricity trading [19] have demonstrated that decentralized verification can strengthen trust and accountability. However, these efforts have primarily addressed metadata provenance or financial instruments rather than integrating statistical analysis into a unified verification pipeline for raw observational data. Table 1 summarizes recent blockchain and data-integrity approaches relevant to climate data verification and identifies the specific gap each leaves unaddressed.

Contribution

This study develops and tests a reproducible blockchain-based framework for transparent verification, analysis, and governance of climate data. The architecture integrates three layers: a data ingestion layer that standardizes and validates observations, a blockchain layer that ensures immutability and provenance through proof-of-stake consensus, and a statistical analysis layer that applies deterministic methods for anomaly detection and trend evaluation (Fig 1). Unlike prior blockchain applications in climate domains, which have primarily addressed carbon credits, energy certificates, or sensor metadata, this framework integrates statistical analysis into the verification pipeline, creating an end-to-end auditable system from raw observation to analytical interpretation. Technical feasibility is evaluated using 8,403 hours of real-world temperature observations from Manila, Philippines, during 2024.

Organization of the paper

The remainder of this paper is organized as follows. The Materials and Methods section describes the data source, preprocessing and quality-control procedures, the statistical anomaly-detection method, and the conceptual blockchain verification model. The Results section presents dataset characteristics, detected anomalies, and estimated blockchain performance parameters. The Discussion examines proof-of-stake sustainability, comparison with existing verification systems, implications for climate policy, limitations, and future implementation pathways.

Table 1. Recent blockchain and data-integrity approaches relevant to climate data verification (2019–2025).

Study	Domain	Approach	Gap addressed by the present study
Boeckhout et al. (2018) [20]	Data governance	FAIR principles for data stewardship	No tamper-evidence or immutability
Imran et al. (2017) [21]	Cloud computing	Data provenance for cloud data integrity verification	Provenance metadata tracking only; lacks decentralized tamper-evident blockchain ledgers
González-Cebrián et al. (2024) [22]	Data management	FAIR-compliant dataset versioning with DOIs	Does not prevent retrospective alteration
Ichikawa et al. (2017) [13]	Mobile health	Tamper-resistant mobile health data via blockchain	Single-user health data; no multi-stakeholder verification
De Vries (2022) [23]	Blockchain energy	Ethereum PoW-to-PoS energy transition analysis	Energy analysis only; no data verification application
Pradhan et al. (2022) [19]	Energy trading	Lightweight peer-to-peer blockchain energy trading	Transaction verification; no observational data or analytics
Sabrina et al. (2022) [24]	IoT networks	Blockchain-based device identity management	Sensor metadata only; no analytical integration
Benaich et al. (2023) [25]	Healthcare EHR	Zero-trust blockchain with AES and zero-knowledge proofs	Healthcare-specific; no environmental data application
Niesya & Sayeed (2024) [26]	Healthcare supply chain	Review of blockchain adoption in supply chain management	Supply chain trust; no scientific data verification
F. Ullah et al. (2024) [11]	Healthcare EHR	Blockchain-enabled audit trails for health records	Healthcare-specific; no climate or environmental scope
Saeed et al. (2025) [17]	Carbon credits	Blockchain framework for carbon credit trading	Financial instruments only; no raw data verification
Haryani et al. (2025) [18]	Renewable energy	Blockchain renewable energy certificate system	Certificate metadata; no statistical analysis layer
Present study	Climate data	PoS blockchain with deterministic anomaly detection	—

Recent literature on blockchain and data integrity applications relevant to climate data verification (2019–2025). The final column identifies the specific gap that the present study addresses relative to each prior work.

https://doi.org/10.1371/journal.pclm.0000764.t001

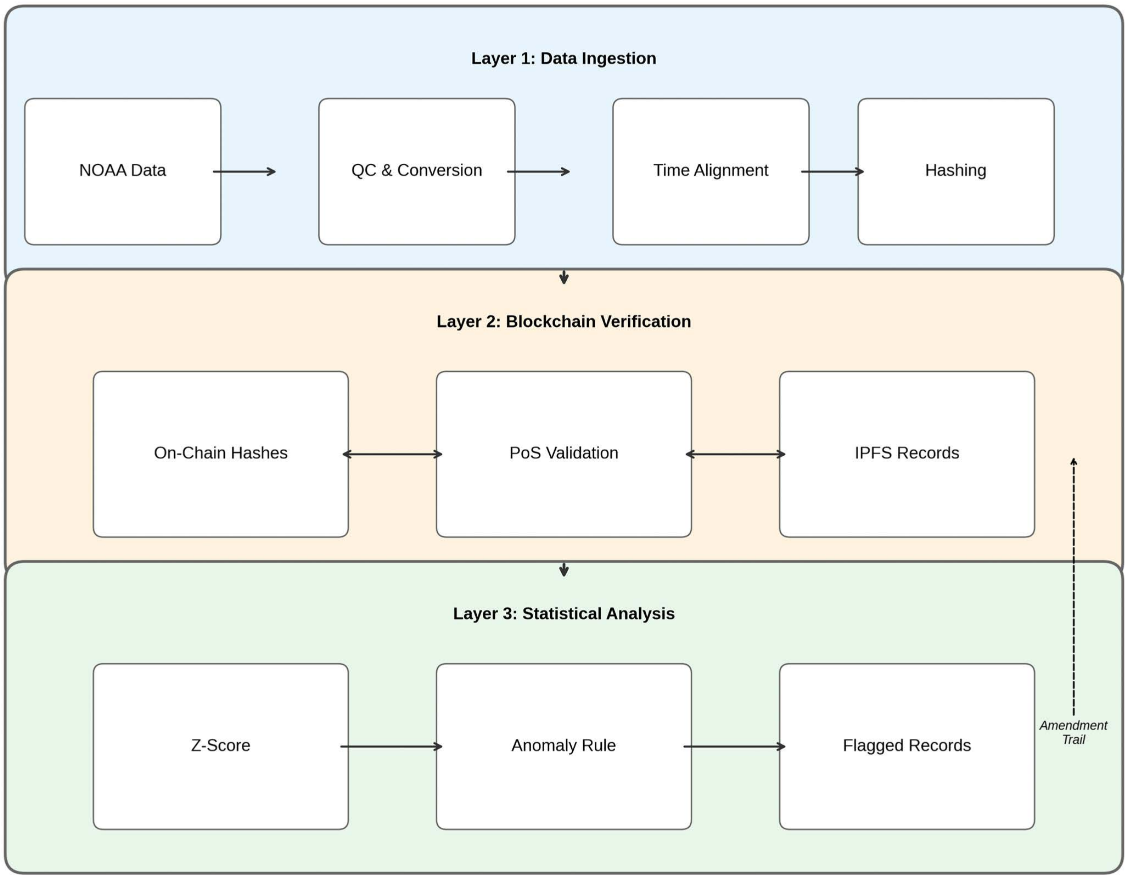

Fig 1. Three-layer architecture of the proposed blockchain-based climate data verification framework. Layer 1 ingests and validates raw observations, generating cryptographic hashes for each quality-controlled record. Layer 2 stores hashes on-chain via proof-of-stake consensus while maintaining complete records in off-chain distributed storage. Layer 3 applies deterministic statistical methods to detect anomalies. The dashed arrow indicates the correction-by-amendment protocol, in which error corrections are appended as new transactions without altering original records.

https://doi.org/10.1371/journal.pclm.0000764.g001

Materials and methods

This study developed a reproducible three-layer system that integrates data ingestion, blockchain-based verification, and statistical anomaly detection to improve transparency in climate data management. The framework was tested using real hourly temperature observations from Manila, Philippines, during 2024 [27].

Data source and preprocessing

Hourly air temperature observations were obtained from the NOAA Integrated Surface Database for Station 984290 (Manila, Philippines; 14.52°N, 121.02°E) (Global Hourly - Integrated Surface Database (ISD), 2021). The raw file contained 8,408 hourly records spanning January through December 2024. Before analysis, the following quality-control and preprocessing steps were applied in sequence:

1. Records flagged by NOAA as erroneous (coded −9999) were removed, leaving 8,403 valid observations.
2. Temperature values were converted from the source format (tenths of degrees Celsius) to degrees Celsius.
3. Timestamps were parsed and aligned to hourly intervals in Coordinated Universal Time (UTC).

4. Data completeness was assessed against the 8,784 expected hourly observations for the full year (2024 is a leap year), yielding 95.7% completeness.

These steps constitute the data ingestion layer of the framework. In an operational blockchain deployment, each validated observation would generate a SHA-256 cryptographic hash at this stage, prior to commitment to the immutable ledger, ensuring that only quality-controlled records enter the verification pipeline.

Statistical anomaly detection

Data cleaning, aggregation, and statistical analyses were performed using Python 3.11 (Pandas 2.2.2, NumPy 1.26) within a Jupyter Notebook environment. A deterministic global-baseline z-score method was selected for anomaly detection. This approach was chosen over machine-learning alternatives for three reasons: (a) it requires no training data, eliminating dependence on historical datasets that may themselves contain unverified observations; (b) the algorithm is fully deterministic, meaning any user with the same input data and threshold will obtain identical results; and (c) the method is transparent to non-specialists, supporting the framework's goal of end-to-end auditability by stakeholders without advanced statistical expertise.

The global mean and standard deviation were computed across the full dataset:

$$\mathrm{mu} = (1/N) * \mathrm{sum}(x\_i) \text{ for } i = 1 \text{ to } N \tag{1}$$

$$\mathrm{sigma} = \mathrm{sqrt}[(1/(N-1)) * \mathrm{sum}((x\_i - \mathrm{mu})\hat{}2)] \text{ for } i = 1 \text{ to } N \tag{2}$$

where x_i denotes the observed temperature at hour i and N is the total number of valid observations. The standardized anomaly score for each observation was then computed as:

$$z\_i = (x\_i - \mathrm{mu}) / \mathrm{sigma} \tag{3}$$

Observations with $|z\_i| > 3.0$ were classified as statistically extreme. The threshold of 3.0 standard deviations was selected because it corresponds to the conventional criterion for identifying outliers in approximately normal distributions, flagging values expected to occur less than 0.3% of the time under stationary conditions. To assess sensitivity, the analysis was repeated at thresholds of $|z| > 2.5$ and $|z| > 3.5$. At $|z| > 2.5$, the number of flagged observations increased to 122, introducing detections from 10 additional months—including both high- and low-temperature extremes—that did not correspond exclusively to documented heat events. At $|z| > 3.5$, no observations were flagged. The threshold of 3.0 isolated 33 anomalies exclusively within the April–May heat wave period, providing the best balance between sensitivity and specificity for this dataset. The modular design permits users to substitute alternative thresholds or detection methods without altering the surrounding verification architecture.

Detected anomalies were cross-checked against contemporaneous meteorological reports, confirming the April–May 2024 regional heat events in the Philippines [28]. Output tables include timestamps, z-scores, and absolute temperature values.

Conceptual blockchain verification model

A proof-of-stake architecture was modeled conceptually to demonstrate how verified climate observations could be cryptographically secured. The framework is parameterized using Ethereum PoS as a reference model, which provides a well-documented reference implementation with established performance characteristics [23]. Key design parameters are as follows. Each validated observation generates a SHA-256 cryptographic hash, which is stored on-chain, while the complete observation record is stored off-chain in distributed storage such as the InterPlanetary

File System (IPFS), a peer-to-peer network that enables content-addressed, verifiable data storage. Under the Ethereum PoS model, block time averages approximately 12 seconds, with transaction finality achieved within approximately 13 minutes (two epochs of 32 slots), meaning that once committed, observation records cannot be retroactively altered without controlling a supermajority of staked validators [29]. For a pilot climate-data network, a small set of geographically distributed validator nodes operated by independent institutions—such as meteorological agencies, universities, or civil society organizations—could provide an initial level of decentralization, with the network expandable to a larger consortium as participation grows.

Energy efficiency estimates were derived from published Ethereum PoS data. Following the September 2022 transition from proof of work, Ethereum's annual energy consumption fell from approximately 78 terawatt-hours to approximately 0.0026 terawatt-hours, a reduction of 99.95% [23]. For the present framework, estimated energy consumption for a 90-day deployment processing 2,160 observations is approximately 0.06 kilowatt-hours, based on published Ethereum proof-of-stake benchmarks.

Because blockchain ledgers are append-only, data points committed to the chain cannot be deleted or overwritten. If a sensor malfunction or quality-control failure is identified after commitment, the framework addresses this through a correction-by-amendment protocol rather than data deletion. A new transaction is appended to the chain containing: (a) a reference to the original observation hash, (b) the corrected value or a retraction flag, and (c) a cryptographic signature from the correcting authority. The original record remains on-chain as a permanent audit trail, while the framework would be designed so that downstream queries and analyses resolve to the most recent valid version. This approach preserves the immutability guarantee — no historical record is altered — while providing a transparent, auditable mechanism for error correction that mirrors the retraction and correction practices standard in scientific publishing.

Performance assessment

Analytical performance was measured by the number and temporal clustering of detected anomalies, as well as by computational efficiency. For a representative 90-day dataset, total storage requirements were approximately 2.1 MB, and analyses were executed in under one minute on a standard desktop computer.

Ethics statement

This research used publicly available environmental data and involved no human participants, animals, or identifiable information. Large language models (Claude, Anthropic) were used for language editing, formatting, and coding assistance; the author reviewed, verified, and is fully responsible for all content.

Results

Dataset characteristics (NOAA Station 984290, Manila)

From 1 January to 31 December 2024, the file contained 8,408 hourly records, of which 8,403 included valid temperature values (5 entries were flagged −9999). Relative to the 8,784 expected hours (2024 is a leap year), completeness was 95.7%. Temperatures (converted from tenths of °C) ranged from 22.0 to 38.0 °C (mean 29.17 °C, SD 2.56 °C).

Anomaly detection

A deterministic global baseline z-score method was used to flag statistical extremes ($|z| > 3$). The results provided in the project output file (anomalies.csv) list 33 hourly anomalies between 36.9 and 38.0 °C (Fig 2). These were temporally clustered in April ($n = 21$) and May ($n = 12$) 2024, consistent with regional heat episodes [28]. Independent recomputation using the archived dataset confirmed all dates, temperatures, and z-scores listed in the project output file (anomalies.csv). The blockchain verification layer was modeled but not executed in code; the repository reflects the statistical analysis only.

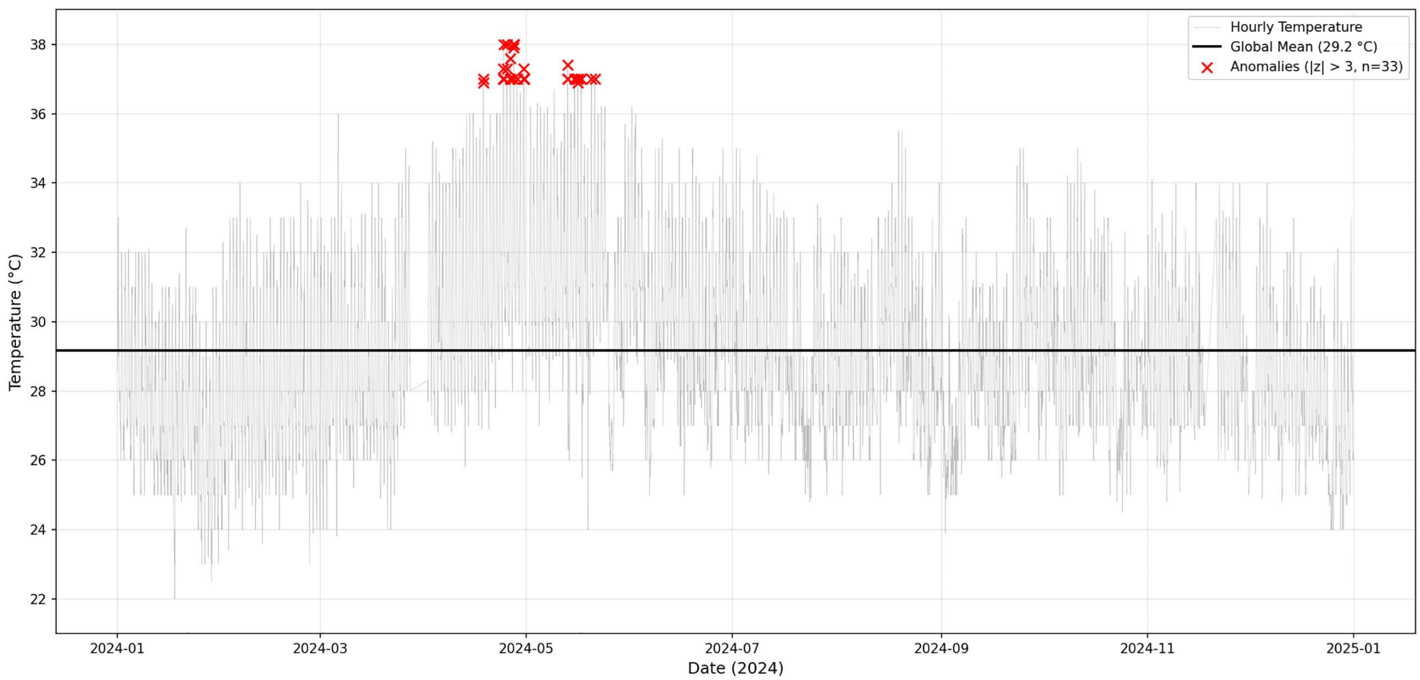

Fig 2. Hourly temperature and flagged anomalies, Manila Station 984290 (Jan–Dec 2024). Hourly temperatures (°C) are shown as a thin line; the global mean is shown as a thick line. Points indicate hours flagged as statistical extremes using a global-baseline z-score threshold of $|z| > 3$. Anomalies cluster in April–May. Data: NOAA Integrated Surface Database, Station 984290 (Manila, Philippines).

https://doi.org/10.1371/journal.pclm.0000764.g002

Conceptual performance estimates (architecture feasibility)

To assess the feasibility of a verification layer, we modeled a proof-of-stake design using on-chain content hashes with off-chain storage. Under this design, a representative 90-day deployment would require on the order of ~138 kB on-chain metadata and ~2.1 MB off-chain data, with second-scale ingestion latency and substantially lower energy use than proof-of-work systems. These are model-based estimates, not measurements from a live chain (Table 2).

Discussion

This study demonstrates that a proof-of-stake blockchain architecture can provide transparent, energy-efficient verification of climate data while maintaining full analytical reproducibility. The verification layer described here was evaluated conceptually using modeled blockchain specifications rather than being operated on a live network. Applied to 8,403 hours of operational temperature observations from Manila, Philippines, the framework successfully detected 33 genuine heat extremes (36.9–38.0 °C) during documented April–May 2024 heat waves using deterministic statistical methods. The modeled blockchain layer—using on-chain cryptographic hashes with off-chain data storage—would require only ~0.06 kilowatt-hours for a 90-day deployment, representing a 97–99% reduction in energy consumption compared to proof-of-work systems. These results establish technical feasibility for distributed verification of climate observations without compromising environmental sustainability.

Proof-of-Stake consensus and environmental sustainability

The energy efficiency estimates presented here rely fundamentally on proof-of-stake (PoS) consensus, which differs categorically from proof-of-work (PoW) mechanisms. PoW systems like Bitcoin require massive computational competition to

Table 2. Estimated storage requirements for a 90-day climate dataset (2,160 observations).

Storage location	Data type	Total size	Size per observation
On-chain (Ethereum)	Cryptographic hashes + metadata	138 KB	64 bytes
Off-chain (IPFS)	Complete observation records	2.1 MB	972 bytes
Total	Combined	2.24 MB	1036 bytes

The hybrid blockchain design stores only cryptographic hashes on-chain, while complete observation records are stored off-chain, providing about a 15-fold reduction in on-chain storage compared with direct on-chain storage.

https://doi.org/10.1371/journal.pclm.0000764.t002

validate transactions, consuming ~120 terawatt-hours annually—equivalent to the electricity use of entire nations [31]. In contrast, PoS validators are selected based on staked assets rather than computational power, eliminating energy-intensive mining. Ethereum's transition from PoW to PoS in September 2022 reduced network energy consumption by 99.95%, demonstrating that blockchain verification need not conflict with climate mitigation goals [23].

For climate data applications, this distinction is non-negotiable. A PoW-based climate verification system would consume more energy than the monitoring infrastructure it seeks to secure, creating an unacceptable environmental cost. PoS architectures avoid this paradox entirely while maintaining cryptographic security [29,32]. Moreover, modern PoS platforms such as Ethereum support smart contracts—self-executing code that can automate data validation, dispute resolution, and governance mechanisms directly on-chain [33]. This programmability enables the framework to enforce quality control protocols, trigger alerts for anomalies, and manage multi-institutional data contributions without centralized administration [34].

Comparison with Centralized and Alternative Verification Systems

Current climate data management relies primarily on institutional repositories such as the National Oceanic and Atmospheric Administration's (NOAA) Integrated Surface Database, the European Centre for Medium-Range Weather Forecasts' (ECMWF) ERA5 reanalysis, and national meteorological archives [35,36]. These systems employ rigorous internal quality control but lack mechanisms for external stakeholders to verify data integrity or reproduce analytical workflows independently [37]. Recent initiatives promoting FAIR principles (Findable, Accessible, Interoperable, Reusable) have improved metadata standards and data accessibility, but do not address immutability or tamper-evidence [20].

Alternative approaches to building trust include data citation standards, digital object identifiers (DOIs), and version-control systems such as Git [22]. While valuable for attribution and reproducibility, these tools do not prevent retrospective alteration of archived data. Cryptographic checksums (e.g., SHA-256 hashes) can detect tampering but require trusted third parties to maintain hash registries [21]. Distributed ledger technology eliminates this single point of failure by distributing verification across independent validators.

Prior blockchain applications in climate domains have focused primarily on carbon credit tracking [17], renewable energy certificates [38], and supply chain transparency [39]. Several projects have explored blockchain for environmental sensor networks [24], but these typically verify sensor metadata rather than integrating statistical analysis into the verification layer. The framework presented here uniquely combines immutable data storage with on-chain or verifiable off-chain computation of anomaly detection, creating an end-to-end auditable pipeline from observation to interpretation. Table 3 compares these approaches across eight verification features relevant to climate data systems.

Interpretation in context

The results show that simple, well-documented statistics (global mean, standard deviation, and z-scores) can yield reproducible flags that non-specialists can audit. This transparency is critical: if only experts can verify analytical

Table 3. Comparison of verification approaches for climate data systems.

Feature	Centralized archives (NOAA, ECMWF)	FAIR principles	Checksums / DOIs / Git	Prior blockchain applications	Present framework
Data immutability	No; administrators can alter records	No	Partial; checksums detect but do not prevent alteration	Yes; distributed ledger prevents retrospective changes	Yes; on-chain cryptographic hashes
Tamper evidence	Internal logs only	No	Yes, if hash registry is maintained by trusted third party	Yes; distributed across validators	Yes; no single point of failure
External auditability	Limited; requires institutional access	Improved metadata access	Partial; requires access to hash registry	Yes, for metadata and transactions	Yes; end-to-end from observation to analysis
Analytical reproducibility	Varies by institution	Encouraged but not enforced	Version control supports code reproducibility	Not typically integrated	Yes; deterministic algorithms with published code
Statistical analysis integration	Separate from verification layer	Not addressed	Not addressed	Not integrated; metadata provenance only	Yes; anomaly detection within verification pipeline
Energy efficiency	N/A (centralized servers)	N/A	N/A	Varies; PoW systems consume high energy	PoS design; estimated 97–99% reduction vs. PoW
Decentralized governance	No; single institutional authority	No	No	Partial; depends on implementation	Designed for multi-stakeholder validator consortia
Public accessibility	Varies; often restricted	Improved	Requires technical expertise	Varies by platform	Designed for non-specialist audit capability

Comparison of verification approaches for climate data systems. NOAA = National Oceanic and Atmospheric Administration; ECMWF = European Centre for Medium-Range Weather Forecasts; FAIR = Findable, Accessible, Interoperable, Reusable; DOI = digital object identifier; PoW = proof of work; PoS = proof of stake.

https://doi.org/10.1371/journal.pclm.0000764.t003

methods, the trust gap persists. By using deterministic algorithms with published code [30], any stakeholder with basic programming skills can independently reproduce the anomaly flags and confirm that the results were not selectively reported or post-hoc manipulated. A blockchain-based verification layer—if implemented as modeled—could add tamper-evident provenance to these same observations without altering the analytical logic, thereby addressing the trust gap between collection, curation, and interpretation. The approach is designed to complement, not replace, conventional archives by adding independent verifiability and public audit trails.

Effective implementation requires governance frameworks that define data admission criteria, validator responsibilities, and dispute resolution processes [40]. Multi-stakeholder consortia—including meteorological agencies, academic institutions, and civil society organizations—could operate validator nodes, distributing authority and preventing capture by any single entity. Smart contracts could encode quality standards, automatically flagging observations that deviate from sensor specifications or fail cross-validation checks [41]. Such mechanisms would operationalize the technical verification layer demonstrated in this study.

Implications for climate policy and communication

The framework addresses a specific dimension of the climate trust deficit: concerns about data manipulation and institutional opacity. While transparent verification alone cannot overcome ideological resistance or misinformation campaigns [42], it removes a technical barrier that legitimizes skepticism. When data integrity is independently auditable, debates can shift from questioning whether data were altered to interpreting what verified observations mean [43].

For policymakers, verifiable climate data strengthens the evidentiary basis for mitigation and adaptation decisions [44]. Regulatory frameworks increasingly demand traceable, auditable environmental data—particularly for carbon markets, emissions reporting, and climate finance mechanisms [45]. A distributed verification infrastructure could serve as trusted input for these systems, reducing compliance costs and fraud risks [46].

Limitations

Several limitations merit consideration. The NOAA record covers January through December 2024 and is 95.7% complete, which could influence the global baseline and the number of flagged extremes; however, the pipeline explicitly handles missing values and is fully reproducible, allowing seamless reruns as additional hours become available. The analysis focuses on a single station and a single variable, limiting generalizability. Yet, this single, high-frequency, operational record provides a clean testbed that avoids cross-site confounding and demonstrates end-to-end reproducibility on real data. Multi-station networks would require coordination protocols to ensure data standardization and synchronized timestamping across nodes [47], but the core verification architecture scales naturally through blockchain's peer-to-peer design [48].

The anomaly rule ($|z| > 3$ using a global baseline) is intentionally simple and may miss regime shifts; its simplicity is also a strength because the threshold is deterministic, transparent to non-specialists, and can be easily swapped for seasonal baselines or robust alternatives in future work without changing the surrounding workflow. More sophisticated anomaly detection methods—including machine learning approaches—could be integrated as smart contract modules, allowing the framework to evolve while maintaining full audit trails of methodological changes [49].

The blockchain layer was modeled rather than deployed, so storage, latency, and energy values are estimates. This choice deliberately isolates the analytical layer, prevents unnecessary environmental cost during method development, and still yields concrete implementation targets for a subsequent pilot. Live deployment would enable empirical measurement of network performance under realistic conditions, including transaction throughput during high-frequency observation ingestion and resilience to validator node failures [50].

Finally, governance mechanics (admission rules, dispute resolution, versioning) were not exercised on a live network; even so, the design articulates how these elements would operate and provides a practical blueprint for testing them in controlled pilots. Game-theoretic analysis of validator incentives and adversarial scenarios would be necessary before operational deployment to ensure long-term system integrity [51].

Implementation Pathways and Future Work

Pilot deployments at multiple stations and variables (e.g., humidity, wind, precipitation) with live, low-energy chains would allow empirical measurement of throughput, costs, and validator behavior. Methodologically, daily or seasonal baselines and multi-metric anomaly scoring (e.g., heat index) could be compared with the present global baseline method. Governance specifications (data admission rules, dispute resolution, versioning) should be operationalized and tested. The primary intended users of this framework fall into three categories: meteorological agencies and data producers, who would operate validator nodes and contribute quality-controlled observations; researchers and policymakers, who would query verified datasets and reproduce analyses; and civil society organizations and the public, who would audit data provenance and analytical outputs without requiring specialized expertise.

Successful adoption requires addressing technical, institutional, and social barriers [52]. Meteorological agencies may resist ceding control over data validation to distributed networks, requiring a phased integration in which blockchain verification complements rather than replaces existing workflows. Validator node operation must be economically sustainable, either through public funding models or tokenized incentive mechanisms that reward data contributions [53].

Socio-economic barriers also warrant consideration. Deploying and maintaining validator nodes requires computational infrastructure, stable internet connectivity, and technical personnel — resources that are unevenly distributed across institutions and regions. Low-income countries and smaller meteorological agencies may lack the capacity to participate without external support, risking a digital divide in which verification infrastructure mirrors existing inequalities in data access [8]. Addressing this requires tiered participation models in which institutions contribute according to capacity — for example, as data providers, light-client verifiers, or full validator nodes — alongside targeted funding from international climate finance mechanisms or multilateral organizations. The framework's low energy requirements (approximately 0.06 kilowatt-hours per 90-day deployment) substantially reduce the infrastructure threshold compared with proof-of-work systems, but connectivity and training costs remain nontrivial for resource-constrained settings.

Interoperability with legacy systems is essential. Application programming interfaces (APIs) can enable traditional databases to cross-reference blockchain-verified records, allowing gradual migration without disrupting operational forecasting and research pipelines [54]. Educational initiatives must target both data producers (meteorological technicians, sensor operators) and data users (researchers, policymakers) to build capacity for distributed verification literacy.

International coordination presents both opportunities and challenges. A global climate data blockchain could transcend national boundaries, enabling cross-border verification and reducing duplication of monitoring infrastructure. However, geopolitical tensions and differing regulatory frameworks complicate consensus on governance structures [55]. Regional pilots—such as networks covering specific climate zones or transboundary watersheds—may provide tractable proving grounds before scaling globally [56].

Conclusions

A transparent pipeline using deterministic statistics detected 33 high-temperature hours in Manila during April–May 2024, consistent with known heat conditions and demonstrating reproducible anomaly identification from operational data. While the blockchain component was modeled rather than deployed, a proof-of-stake design with on-chain hashes and off-chain storage appears technically feasible and well aligned with the goal of verifiable climate records. The 97–99% energy reduction compared to proof-of-work systems demonstrates that distributed verification can support, rather than undermine, climate mitigation objectives. Together, these elements outline a practical path toward trustworthy, energy-efficient climate information systems that non-experts can audit end-to-end. Future work should prioritize multi-station pilot deployments with live proof-of-stake chains, empirical measurement of validator behavior and network performance, and development of tiered participation models that enable resource-constrained institutions to contribute to decentralized verification. By providing a technical foundation for independently auditable climate data, this framework addresses one dimension of the trust deficit that has hindered evidence-based climate policy and public engagement.

Acknowledgments

The author thanks the University of Washington School of Medicine and Washington State University Elson S. Floyd College of Medicine for institutional support.

Author contributions

Conceptualization: Thomas F. Heston.

Data curation: Thomas F. Heston.

Formal analysis: Thomas F. Heston.

Investigation: Thomas F. Heston.

Methodology: Thomas F. Heston.

Software: Thomas F. Heston.

Validation: Thomas F. Heston.

Writing – original draft: Thomas F. Heston.

Writing – review & editing: Thomas F. Heston.

References

1. Fage-Butler A, Ledderer L, Nielsen KH. Public trust and mistrust of climate science: A meta-narrative review. Public Underst Sci. 2022;31(7):832–46. https://doi.org/10.1177/09636625221110028 PMID: 35946959
2. Cologna V, Kotcher J, Mede NG, Besley J, Maibach EW, Oreskes N. Trust in climate science and climate scientists: A narrative review. PLOS Clim. 2024;3(5):e0000400. https://doi.org/10.1371/journal.pclm.0000400
3. Sarathchandra D, Haltinner K. Trust/distrust judgments and perceptions of climate science: A research note on skeptics' rationalizations. Public Underst Sci. 2020;29(1):53–60. https://doi.org/10.1177/0963662519886089 PMID: 31691642
4. Leka J, Furnham A. Correlates of climate change skepticism. Front Psychol. 2024;15:1328307. https://doi.org/10.3389/fpsyg.2024.1328307 PMID: 38721315
5. Vera LA, Walker D, Murphy M, Mansfield B, Siad LM, Ogden J, et al. When Data Justice and Environmental Justice Meet: Formulating a Response to Extractive Logic through Environmental Data Justice. Inf Commun Soc. 2019;22(7):1012–28. https://doi.org/10.1080/1369118X.2019.1596293 PMID: 31787840
6. Costa C, Pezzetta R, Toffalini E, Grassi M, Cona G, Miniussi C, et al. Enhancing the quality and reproducibility of research: Preferred Evaluation of Cognitive and Neuropsychological Studies - The PECANS statement for human studies. Behav Res Methods. 2025;57(7):182. https://doi.org/10.3758/s13428-025-02705-3 PMID: 40447861
7. Mollakuqe E, Dimitrova V. Comparative analysis of identity management, access control, and authorization practices in public and private universities. Open Res Eur. 2024;4:23. https://doi.org/10.12688/openreseurope.16634.2 PMID: 39100072
8. Maeda EE, Torres JA. Open Environmental Data in Developing Countries: Who Benefits? Ambio. 2012;41: 410–2. https://doi.org/10.1007/s13280-012-0283-4
9. Gortan M, Testa L, Fagiolo G, Lamperti F. A unified dataset for pre-processed climate indicators weighted by gridded economic activity. Sci Data. 2024;11(1):533. https://doi.org/10.1038/s41597-024-03304-1 PMID: 38789504
10. Mikhailov D, Chunara R, Cucunubá Z, Lamarque J-F, Lennard C, Stewart U. Bridging climate and health data for decision making. BMC Proc. 2025;19(Suppl 4):36. https://doi.org/10.1186/s12919-025-00348-y PMID: 41121136
11. Ullah F, He J, Zhu N, Wajahat A, Nazir A, Qureshi S, et al. Blockchain-enabled EHR access auditing: Enhancing healthcare data security. Heliyon. 2024;10(16):e34407. https://doi.org/10.1016/j.heliyon.2024.e34407 PMID: 39253236
12. Adeniyi JK, Ajagbe SA, Adeniyi AE, Adeyanju KI, Afolorunso AA, Adigun MO, et al. A blockchain-based smart healthcare system for data protection. iScience. 2025;28(4):112109. https://doi.org/10.1016/j.isci.2025.112109 PMID: 40201127
13. Ichikawa D, Kashiyama M, Ueno T. Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR Mhealth Uhealth. 2017;5(7):e111. https://doi.org/10.2196/mhealth.7938 PMID: 28747296
14. Lima V, Bernardi F, Rijo R, Ueyama J, Alves D. A Mechanism for Verifying the Integrity and Immutability of Tuberculosis Data Using IOTA Distributed Ledger Technology. Stud Health Technol Inform. 2021;279:130–5. https://doi.org/10.3233/SHTI210099 PMID: 33965929
15. Shaikh M, Ebrahimi A, Wiil UK. A Novel Blockchain-Based Model for Secure Genomic Data Management. Stud Health Technol Inform. 2025;328:302–7. https://doi.org/10.3233/SHTI250724 PMID: 40588931
16. Ni E, Tang X, Zhou X, Lee D, Elhussein A, Knight E, et al. Recent advances and future prospects for blockchain in biomedicine. Cell Rep Methods. 2025;5(8):101114. https://doi.org/10.1016/j.crmeth.2025.101114 PMID: 40714006
17. Saeed N, Wen F, Afzal MZ. A unified FLC-blockchain framework for optimized carbon credit trading in multi-microgrid systems. Sci Rep. 2025;15(1):30081. https://doi.org/10.1038/s41598-025-12562-x PMID: 40820094
18. Haryani I, Aditya IA, Nuraini AH, Widiyanesti S, Alamsyah A, Nurhazizah E, et al. Blockchain-based renewable energy certificate system in Indonesia. Heliyon. 2025;11(3):e42364. https://doi.org/10.1016/j.heliyon.2025.e42364 PMID: 39991208
19. Pradhan NR, Singh AP, Verma SK, Wozniak M, Shafi J, et al. A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. Sci Rep. 2022;12(1):14523. https://doi.org/10.1038/s41598-022-18603-z PMID: 36008545
20. Boeckhout M, Zielhuis GA, Bredenoord AL. The FAIR guiding principles for data stewardship: fair enough?. Eur J Hum Genet. 2018;26(7):931–6. https://doi.org/10.1038/s41431-018-0160-0 PMID: 29777206
21. Imran M, Hlavacs H, Haq IU, Jan B, Khan FA, Ahmad A. Provenance based data integrity checking and verification in cloud environments. PLoS One. 2017;12(5):e0177576. https://doi.org/10.1371/journal.pone.0177576 PMID: 28545151
22. González-Cebrián A, Bradford M, Chis AE, González-Vélez H. Standardised Versioning of Datasets: a FAIR-compliant Proposal. Sci Data. 2024;11(1):358. https://doi.org/10.1038/s41597-024-03153-y PMID: 38594314
23. De Vries A. Cryptocurrencies on the road to sustainability: Ethereum paving the way for Bitcoin. Patterns (N Y). 2022;4(1):100633. https://doi.org/10.1016/j.patter.2022.100633 PMID: 36699742
24. F S, Li N, Sohail S. A blockchain based secure IoT system using device identity management. Sensors. 2022;22:7535. https://doi.org/10.3390/s22197535
25. Benaich R, El Mendili S, Gahi Y. Advancing Healthcare Security: A Cutting-Edge Zero-Trust Blockchain Solution for Protecting Electronic Health Records. HighTech Innov J. 2023;4(3):630–52. https://doi.org/10.28991/hij-2023-04-03-012

26. Niesya N, Sayeed MS. Adoption of Blockchain Technology in Healthcare Supply Chain Management: A Review. HighTech Innov J. 2024;5(4):1154–69. https://doi.org/10.28991/hij-2024-05-04-019
27. Global Hourly - Integrated Surface Database (ISD). National Centers for Environmental Information (NCEI). https://www.ncei.noaa.gov/products/land-based-station/integrated-surface-database 2021. 2025 October 31.
28. Sandford C, Dunn R, Killick R, Palmer M, Titchner H, Rayner N. Global and regional climate in 2024. Weather. 2025;80:401–10. https://doi.org/10.1002/wea.7776
29. Hafid A, Hafid AS, Makrakis D. Sharding-Based Proof-of-Stake Blockchain Protocols: Key Components & Probabilistic Security Analysis. Sensors (Basel). 2023;23(5):2819. https://doi.org/10.3390/s23052819 PMID: 36905022
30. Heston TF. Tomheston/blockchain-ai-climate-framework: Blockchain AI Study. Zenodo. 2025. https://doi.org/10.5281/zenodo.17429218
31. Erdogan S, Ahmed MY, Sarkodie SA. Analyzing asymmetric effects of cryptocurrency demand on environmental sustainability. Environ Sci Pollut Res Int. 2022;29(21):31723–33. https://doi.org/10.1007/s11356-021-17998-y PMID: 35013947
32. Shi S, He D, Li L, Kumar N, Khan MK, Choo K-KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Comput Secur. 2020;97:101966. https://doi.org/10.1016/j.cose.2020.101966 PMID: 32834254
33. Han P. AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication. Sci Rep. 2025;15(1):37327. https://doi.org/10.1038/s41598-025-21313-x PMID: 41136499
34. Omar IA, Jayaraman R, Salah K, Simsekler MCE, Yaqoob I, Ellahham S. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. BMC Med Res Methodol. 2020;20(1):224. https://doi.org/10.1186/s12874-020-01109-5 PMID: 32894068
35. Soci C, Hersbach H, Simmons A, Poli P, Bell B, Berrisford P, et al. The ERA5 global reanalysis from 1940 to 2022. Quart J Royal Meteoro Soc. 2024;150(764):4014–48. https://doi.org/10.1002/qj.4803
36. Hersbach H, Bell B, Berrisford P, Hirahara S, Horányi A, Muñoz-Sabater J, et al. The ERA5 global reanalysis. Q J R Meteorol Soc. 2020;146:1999–2049. https://doi.org/10.1002/qj.3803
37. Glade O. QA/QC and verification reporting requirements and their application. 2019. https://unfccc.int/sites/default/files/resource/QAQC%20and%20verification_refresher%20seminar%202019_0.pdf
38. Rejeb A, Rejeb K, Zrelli I, Süle E, Iranmanesh M. Blockchain technology in the renewable energy sector: A co-word analysis of academic discourse. Heliyon. 2024;10(8):e29600. https://doi.org/10.1016/j.heliyon.2024.e29600 PMID: 38660260
39. Yadav N, Luthra S, Garg D. Blockchain technology for sustainable supply chains: a network cluster analysis and future research propositions. Environ Sci Pollut Res Int. 2023;30(24):64779–99. https://doi.org/10.1007/s11356-023-27049-3 PMID: 37086323
40. Ullah I, Havinga PJM. Governance of a Blockchain-Enabled IoT Ecosystem: A Variable Geometry Approach. Sensors (Basel). 2023;23(22):9031. https://doi.org/10.3390/s23229031 PMID: 38005419
41. Ahmed M, Taconet C, Ould M, Chabridon S, Bouzeghoub A. IoT Data Qualification for a Logistic Chain Traceability Smart Contract. Sensors (Basel). 2021;21(6):2239. https://doi.org/10.3390/s21062239 PMID: 33806832
42. Gertrudix M, Carbonell-Alcocer A, Arcos R, Arribas CM, Codesido-Linares V, Benítez-Aranda N. Disinformation as an obstructionist strategy in climate change mitigation: a review of the scientific literature for a systemic understanding of the phenomenon. Open Res Eur. 2024;4:169. https://doi.org/10.12688/openreseurope.18180.2 PMID: 39399659
43. Rosman T, Bosnjak M, Silber H, Koßmann J, Heycke T. Open science and public trust in science: Results from two studies. Public Underst Sci. 2022;31(8):1046–62. https://doi.org/10.1177/09636625221100686 PMID: 35699352
44. Perugini L, Pellis G, Grassi G, Ciais P, Dolman H, House JI, et al. Emerging reporting and verification needs under the Paris Agreement: How can the research community effectively contribute?. Environ Sci Policy. 2021;122:116–26. https://doi.org/10.1016/j.envsci.2021.04.012 PMID: 34345221
45. Milanés Montero P, Pérez Calderón E, Lourenço Dias AI. Transparency of financial reporting on greenhouse gas emission allowances: The influence of regulation. Int J Environ Res Public Health. 2020;17:893. https://doi.org/10.3390/ijerph17030893
46. Gao L. Enterprise internal audit data encryption based on blockchain technology. PLoS One. 2025;20(1):e0315759. https://doi.org/10.1371/journal.pone.0315759 PMID: 39792931
47. Yamakawa Y, Matsui Y, Noda A, Ishikawa M, Shimojo M. Development of a Sensor Network System with High Sampling Rate Based on Highly Accurate Simultaneous Synchronization of Clock and Data Acquisition and Experimental Verification †. Micromachines (Basel). 2018;9(7):325. https://doi.org/10.3390/mi9070325 PMID: 30424258
48. Maftei AA, Petrariu AI, Popa V, Lavric A. A Blockchain Framework for Scalable, High-Density IoT Networks of the Future. Sensors (Basel). 2025;25(9):2886. https://doi.org/10.3390/s25092886 PMID: 40363323
49. Antonini M, Pincheira M, Vecchio M, Antonelli F. An Adaptable and Unsupervised TinyML Anomaly Detection System for Extreme Industrial Environments. Sensors (Basel). 2023;23(4):2344. https://doi.org/10.3390/s23042344 PMID: 36850940
50. Haque EU, Abbasi W, Almogren A, Choi J, Altameem A, Rehman AU, et al. Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. Sci Rep. 2024;14(1):26561. https://doi.org/10.1038/s41598-024-77706-x PMID: 39489789
51. Zhu D, Li Y, Zhou Z, Zhao Z, Kong L, Wu J, et al. Blockchain-Based Incentive Mechanism for Electronic Medical Record Sharing Platform: An Evolutionary Game Approach. Sensors (Basel). 2025;25(6):1904. https://doi.org/10.3390/s25061904 PMID: 40293072

52. Chan CKY, Burton K, Flower RL. Facilitators and barriers of technology adoption and social connectedness among rural older adults: a qualitative study. Health Psychol Behav Med. 2024;12(1):2398167. https://doi.org/10.1080/21642850.2024.2398167 PMID: 39234572

53. Smajgl A, Schweik CM. Advancing sustainability with blockchain-based incentives and institutions. Front Blockchain. 2022;5. https://doi.org/10.3389/fbloc.2022.963766

54. Anthony Jnr B. Enabling interoperable distributed ledger technology with legacy platforms for enterprise digitalization. Enterprise Information Systems. 2024;18:2255979. https://doi.org/10.1080/17517575.2023.2255979

55. Bernier A, Molnár-Gábor F, Knoppers BM. The international data governance landscape. J Law Biosci. 2022;9(1):lsac005. https://doi.org/10.1093/jlb/lsac005 PMID: 35382430

56. Armitage D, de Loë RC, Morris M, Edwards TWD, Gerlak AK, Hall RI, et al. Science-policy processes for transboundary water governance. Ambio. 2015;44(5):353–66. https://doi.org/10.1007/s13280-015-0644-x PMID: 25773532