International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 3985-3992
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Impact of Blockchain Technology on Nursing Documentation and Patient Privacy

Abdullah Hussen A Alshammari[1]*, Mshaal Qasem Alhazmi[2], Badar Shabikan M Alanazi[3], Abdullah Khalil A Alanazi[4], Khalid Fahad N Alanazi[5], Ahmed Raffaa S Alanazi[6], Hamid Kateb H Alenezi[7], Mansor Mohammed Al Naqzi[8], Metar Sadoh M Alhazmi[9], Marzouq Mohammed Marzouq Alhamad[10]

[1]Health Services and Hospitals Specialist, Women's and Children's Hospital in Arar, Saudi Arabia
* **Corresponding Author Email:** ema30a@gmail.com- **ORCID:** 0000-0002-0047-8850

[2]Health Management and Hospitals Specialist, Women's and Children's Hospital in Arar
Email: meshal_2727@hotmail.com - **ORCID:** 0000-0002-0007-0850

[3]Health Services and Hospitals Management Specialist, Al Shamal Medical Tower
Email: nur4u.b@hotmail.com - **ORCID:** 0000-0002-0017-1850

[4]Hospital and Health Services Management Specialist, Women's and Children's Hospital
Email: Abdallah7000@hotmail.com- **ORCID:** 0000-0002-0027-2850

[5]Health Services and Hospitals Management Specialist, Al Shamal Medical Tower
Email: K0909@hotmail.com - **ORCID:** 0000-0002-0037-3850

[6]Health Management, Al Shamal Medical Tower
Email: someone.ahmed1113@gmaıl.com - **ORCID:** 0000-0002-0057-4850

[7]Health and Hospitals Management Specialist, Women's and Children's Hospital in Arar
Email: hameedkat123@gmail.com - **ORCID:** 0000-0002-0067-5850

[8]Health Informatics, Prince Abdulaziz bin Musaad Hospital
Email: geel-4@hotmail.com- **ORCID:** 0000-0002-0077-6850

[9]Nursing Technician, Prince Abdulaziz bin Musaad Hospital
Email: mt-r20@hotmail.com - **ORCID:** 0000-0002-0087-7850

[10]Nursing Technician, King Abdulaziz Hospital in Sakaka
Email: abonaif1984m@gmail.com - **ORCID:** 0000-0002-0097-9850

Article Info:

DOI: 10.22399/ijcesen.4794
Received : 01 June 2024
Accepted : 30 June 2024

Keywords

Blockchain Technology,
Nursing Documentation,
Patient Privacy,
Health Information Security,
Data Integrity,
Interoperabilit

Abstract:

Blockchain technology presents a transformative paradigm for nursing documentation and patient privacy by addressing critical vulnerabilities in current centralized electronic health record systems. Through its core principles of decentralization, cryptographic hashing, and immutable ledgers, blockchain introduces a framework for creating a single, verifiable source of truth for patient data that is secure from tampering and unauthorized alteration. For nursing documentation, this ensures the integrity and provenance of every entry, streamlines interoperability across care settings, and automates administrative tasks via smart contracts, thereby reducing burdensome workflow and enhancing patient safety. Simultaneously, it fundamentally redefines patient privacy by enabling a model of data sovereignty where patients, through self-sovereign identity and granular consent mechanisms, become the active custodians and permission-grantors of their personal health information. This shift not only fortifies security against breaches but also fosters unprecedented transparency and trust in the patient-provider relationship. While significant challenges in scalability, regulation, and implementation persist, the integration of blockchain holds the potential to create a more resilient, efficient, and patient-centric healthcare ecosystem where nursing documentation evolves from a static administrative record into a dynamic, secure, and collaborative tool for high-quality care.

1. Introduction

The contemporary healthcare landscape is an intricate ecosystem of data generation, exchange, and storage, with nursing documentation constituting its vital, continuous heartbeat. This documentation, encompassing patient assessments, interventions, care plans, progress notes, and outcomes, forms the legal and clinical backbone of patient care, facilitating communication among multidisciplinary teams, supporting clinical decision-making, ensuring continuity of care, and serving as a critical tool for quality improvement, research, and reimbursement [1]. However, the systems underpinning this essential function—primarily centralized Electronic Health Records (EHRs) and hybrid paper-digital models—are beleaguered by profound and interconnected challenges that compromise their efficiency, integrity, and security. These systemic vulnerabilities not only strain nursing workflow, contributing to burnout and administrative burden, but also pose significant, ongoing risks to the very cornerstone of the therapeutic relationship: patient privacy and data sovereignty.

At the heart of these challenges lies the issue of data fragmentation. Patient information is frequently siloed across disparate systems belonging to hospitals, primary care providers, specialist clinics, pharmacies, and laboratories. These systems often lack seamless interoperability, operating on different standards and protocols that hinder the fluid exchange of information [2]. For the nurse at the bedside, this fragmentation translates into an incomplete clinical picture. Critical information, such as a medication list from a primary care physician or a recent diagnostic test from an external lab, may be inaccessible at the point of care, potentially leading to medication errors, duplicated tests, and delayed interventions. The nurse's documentation, in turn, becomes trapped within the institution's EHR, unlikely to follow the patient effortlessly on their healthcare journey beyond those walls, undermining the ideal of longitudinal, patient-centered care.

Compounding the problem of fragmentation are persistent concerns regarding data security and patient privacy. Centralized databases, by their very architecture, present a lucrative and vulnerable target for cyberattacks, such as ransomware and data breaches. A single point of failure can expose the sensitive health information of millions of individuals [3]. Beyond external threats, internal privacy breaches remain a concern, with instances of unauthorized access by healthcare personnel for personal or malicious reasons. The current model often operates on a binary paradigm of access: either a user has broad credentials to view a patient's entire record or they are barred entirely. This lacks the granularity needed for true principle of least privilege, where access is granted on a need-to-know basis. Patients themselves have minimal visibility into who has accessed their data, when, and for what purpose, leaving them with little practical control over their most personal information [4].

Furthermore, the integrity and trustworthiness of documented data are perpetually in question. While EHRs maintain audit logs, these logs are themselves subject to potential alteration or manipulation. Disputes can arise regarding the accuracy or timing of an entry, especially in legal or adverse event contexts. The current system does not provide an immutable, verifiable chain of custody for clinical data. From a nursing perspective, documentation is often perceived as a burdensome administrative task driven by regulatory and billing requirements rather than as a dynamic tool for care. Time spent navigating cumbersome EHR interfaces is time diverted from direct patient care, fueling frustration and contributing to the phenomenon of "note bloat" where the volume of documentation increases without a corresponding enhancement in clinical value or communication clarity [5].

It is within this context of systemic inefficiency, vulnerability, and eroding trust that blockchain technology emerges not merely as a novel IT solution, but as a potential foundational paradigm shift for health information management. Initially conceptualized as the distributed ledger underpinning cryptocurrencies like Bitcoin, blockchain's core attributes—decentralization, immutability, transparency, and cryptographic security—offer a compelling antithesis to the weaknesses of centralized health data architectures [6]. At its essence, a blockchain is a shared, immutable ledger for recording transactions, tracking assets, and building trust. Information is stored in cryptographically linked blocks across a network of computers (nodes), making it nearly impossible to alter historical records without consensus from the network. This technology promises a future where health data is not owned by any single institution but is permissioned by the patient, where every access and entry is permanently and transparently recorded, and where data can flow securely across organizational boundaries without compromising security or privacy [7].

The application of blockchain in nursing documentation and patient privacy is therefore not a mere incremental improvement but a radical reimagining of the information infrastructure of

care. It proposes a model where nurses can contribute to a unified, longitudinal patient record with the confidence that their documentation is secure, tamper-proof, and instantly available to authorized parties across the care continuum. It envisions a system where patients are transformed from passive subjects of data collection to active governors of their health information, with auditable control over access permissions. This transition holds the potential to restore trust, streamline workflow, enhance data quality, and ultimately create a more resilient, patient-empowered healthcare ecosystem [8].

2. Fundamentals of Blockchain Technology:

To appreciate its potential impact, one must first understand the core architectural principles of blockchain technology. A blockchain is a type of Distributed Ledger Technology (DLT) where a record of transactions (or, in healthcare, data events) is maintained across a network of multiple participants (nodes) without the need for a central, trusted authority. Each node holds an identical copy of the ledger, which is updated through a consensus mechanism, ensuring all participants agree on the ledger's state [9]. This decentralization is the first fundamental break from the current client-server model of EHRs.

Data on a blockchain is organized into blocks. Each block contains a batch of transactions, a timestamp, and, crucially, a cryptographic hash of the previous block. A hash is a unique digital fingerprint generated from the block's data; even the smallest alteration to the data changes this fingerprint entirely [10]. By linking each block to the previous one via its hash, a continuous, tamper-evident chain is formed. To alter a single record in a past block, an attacker would need to recalculate the hash for that block and for every subsequent block in the chain, and do so simultaneously on over 51% of the distributed copies of the ledger—a computationally infeasible task for a large, established network. This creates the property of immutability, a permanent and verifiable audit trail for all data entries [11].

Consensus mechanisms are the protocols that enable the decentralized network to agree on the validity of new transactions and the appending of a new block to the chain. Common mechanisms include Proof of Work (PoW), used by Bitcoin, which requires computational effort to solve a complex puzzle, and Proof of Stake (PoS), which assigns validation power based on the stake or ownership of tokens in the network. In healthcare, more energy-efficient and faster consensus models like Practical Byzantine Fault Tolerance (PBFT) or permissioned variants are likely employed, where known, vetted entities (e.g., hospitals, clinics, accrediting bodies) operate the nodes, enhancing transaction speed and compliance with regulations like HIPAA [12].

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They reside on the blockchain and automatically execute predefined actions when specific conditions are met. In a healthcare context, a smart contract could automatically grant emergency access to a patient's allergy information for a treating physician in an ER, revoke access for a consultant after a referral period ends, or trigger a notification to a nurse if a patient's vital signs, as recorded by a wearable device and written to the blockchain, fall outside predetermined parameters [13]. These automations can enforce policy with precision and reduce administrative overhead.

For healthcare, two primary types of blockchains are relevant: public (permissionless) and private/permissioned. Public blockchains are open to anyone, while private blockchains restrict participation to invited members. Consortium blockchains, a subset of permissioned ledgers, are controlled by a group of organizations, making them particularly suited for the multi-institutional nature of healthcare delivery, where a network of trusted providers, payers, and patients can interact [14]. Furthermore, a critical design consideration is what data is stored directly *on-chain*versus *off-chain*. Given the sensitivity and size of medical records (e.g., MRI images, lengthy nursing notes), storing raw data directly on a public ledger is often impractical and undesirable. Instead, the blockchain can store only cryptographic hashes or pointers to the data, which resides securely in off-chain storage (e.g., encrypted in a distributed file system like IPFS or a traditional, secure cloud). The on-chain hash acts as an immutable proof of the data's existence and state at a given time; any tampering with the off-chain data would be immediately detectable because its hash would no longer match the one recorded on the blockchain [15]. This hybrid model balances security, privacy, and scalability.

3. Transforming Nursing Documentation:

The integration of blockchain technology into nursing documentation directly addresses many of the chronic pain points nurses face, fundamentally altering the process from a siloed, retrospective task to an integrated, real-time component of care coordination. The most profound impact lies in establishing an immutable and verifiable chain of custody for clinical data. Every entry a nurse makes—an initial assessment, a medication

administration record (MAR), a vital signs chart, a progress note—can be cryptographically signed with a private key (a digital signature unique to that nurse) and timestamped before being written to the ledger [16]. This creates an indisputable record of who documented what, and when. In cases of legal scrutiny, such as malpractice claims, or during clinical audits, this feature provides a level of evidential integrity currently unattainable with conventional EHRs. It protects the nurse by verifying their actions and protects the patient by ensuring the record cannot be secretly altered. The concept of a single, shared source of truth for a patient's care history, accessible across institutions, can dramatically reduce errors stemming from information gaps or reliance on outdated records [17].

Blockchain also holds immense promise for revolutionizing interoperability, the holy grail of health informatics. Instead of relying on complex, fragile, and expensive point-to-point interfaces between disparate EHR systems, a consortium blockchain can act as a universal, shared layer for health data exchange. Authorized entities can query the blockchain or be notified via smart contracts of relevant events. When a nurse admits a patient transferred from another facility, instead of making frantic phone calls or waiting for faxed records, they could, with the patient's permission, instantly access a verified summary of key data (e.g., problem lists, medications, recent procedures) contributed by the previous providers to the patient's blockchain record [18]. This seamless flow of information enhances safety, reduces duplication, and allows nurses to spend less time hunting for information and more time synthesizing it into effective care.

Smart contracts can automate numerous routine administrative and clinical tasks, streamlining nursing workflow. For instance, a smart contract linked to a pharmacy's blockchain node could automatically verify a patient's medication orders against the drug formulary and insurance coverage rules before the nurse even begins the administration process, flagging potential issues instantly [19]. In care coordination, a smart contract could be programmed so that when a nurse documents the completion of a preoperative checklist, it automatically notifies the operating room team and anesthesiology, updating the patient's status across the care continuum. Furthermore, documentation compliance can be embedded into the system; a smart contract could remind a nurse if a required reassessment for a patient on a high-risk medication is overdue, based on the last documented entry. These automations reduce cognitive load, prevent process breakdowns, and ensure consistent adherence to clinical protocols [20].

The nature of documentation itself could evolve. With a secure, patient-centric ledger, contributions from patients and their families via personal health records (PHRs) or wearable devices can be integrated directly into the shared record with clear provenance. A nurse can view patient-reported outcome measures (PROMs) or glucose readings from a continuous monitor that are cryptographically signed by the device or patient and immutably recorded. This creates a richer, more holistic patient narrative, blending professional clinical observations with lived experience data. For nursing research, blockchain offers a paradigm shift. Researchers could request access to anonymized, aggregated clinical data from the ledger for quality improvement or studies, with patients granting permission via smart contracts and with an immutable audit trail of what data was accessed and for which purpose, enhancing transparency and trust in secondary data use [21].

4. Redefining Patient Privacy and Data Sovereignty:

Perhaps the most radical implication of blockchain in healthcare is its potential to invert the traditional model of data ownership and privacy. Current systems are fundamentally institution-centric: the hospital or clinic owns and controls the EHR database, with patients granted certain rights of access and disclosure under regulations like HIPAA. Blockchain enables a shift toward a genuine patient-centric model, where individuals become the stewards and primary grantors of access to their health data [22]. This concept, often termed "patient data sovereignty" or "self-sovereign identity" in health, is enabled by the cryptographic underpinnings of the technology.

In a blockchain-based health data ecosystem, a patient would have a unique digital identifier (a decentralized identifier, or DID) anchored on the blockchain. This DID is not issued by any institution but is self-owned. Associated with this DID are verifiable credentials—cryptographically signed attestations from trusted entities (e.g., a hospital attesting to a diagnosis, a nurse's employer attesting to their license). The patient stores these credentials in a secure digital wallet on their smartphone [23]. When a nurse at a new clinic needs access to the patient's history, the patient does not simply hand over control. Instead, using their wallet, they can grant granular, time-bound, and purpose-specific access permissions to specific data attributes. For example, a patient could permit

an orthopedic surgeon to view only their musculoskeletal history and imaging results, while withholding unrelated psychiatric or genetic data. This permission transaction is recorded immutably on the blockchain, creating a transparent access log [24].

This granular, consent-on-demand model, enforced by smart contracts, fundamentally enhances privacy. It moves beyond the all-or-nothing access typical in EHRs. Patients can see an immutable history of all entities that have accessed their data, for what reason, and when. If access was granted in an emergency via a "break-glass" smart contract clause, this too is permanently recorded and auditable [25]. This transparency acts as a powerful deterrent against unauthorized "snooping" by healthcare staff, as every access, legitimate or not, leaves a permanent trace that the patient can review. The patient can also revoke access at any time, with the smart contract automatically enforcing this revocation across the network.

Blockchain's security architecture provides robust protection for data integrity and confidentiality. Patient data, when stored off-chain, is encrypted. The keys to decrypt this data can be managed in a decentralized manner. Techniques like sharding (splitting data into fragments) and advanced encryption can be used so that no single node on the network holds a complete, readable copy of a patient's record, mitigating the risk of mass data breaches [26]. Even if an off-chain storage server is compromised, the data remains encrypted, and the hashes on the blockchain would show if the encrypted data was illicitly altered. Furthermore, zero-knowledge proofs (ZKPs), an advanced cryptographic method, could allow a system to verify a specific fact (e.g., "this patient is over 18" or "this lab result is within normal range") without revealing the underlying data itself, enabling privacy-preserving data analytics and eligibility checks [27].

This paradigm empowers patients as active participants in their care. With consolidated access to their own complete, longitudinal record from multiple providers, patients are better informed and can engage more meaningfully in shared decision-making with their nurses and physicians. They can also choose to contribute their data, anonymously or otherwise, to research databases or population health initiatives, potentially receiving micropayments or tokens in return, creating new models for data sharing that respect individual autonomy [28]. For nurses, this changes the dynamic of information gathering; rather than being the sole custodians of data entry, they become partners with patients in curating and interpreting a shared health record, fostering a more collaborative therapeutic relationship.

5. Challenges, Limitations, and Implementation Considerations

Despite its transformative potential, the integration of blockchain into nursing documentation and healthcare at large is fraught with significant technical, regulatory, organizational, and human challenges that must be soberly addressed. Technically, scalability and performance are primary concerns. Most current blockchain platforms, especially those using robust consensus mechanisms like PoW, have limited transaction throughput and can experience latency. Nursing documentation involves a high volume of frequent, small data entries; a system must be able to handle thousands of transactions per second across a large network without delays that could impact care at the point of service [29]. Permissioned blockchains with optimized consensus (e.g., Hyperledger Fabric) offer higher throughput but require careful architectural design. The storage model—storing only hashes on-chain—alleviates some burden, but managing the secure, compliant off-chain storage remains a complex IT undertaking.

Interoperability with legacy systems is arguably the single greatest practical hurdle. Healthcare organizations have invested billions in existing EHR systems. A blockchain network cannot exist in a vacuum; it must have bidirectional interfaces with these legacy EHRs to pull data for on-chain hashing and to push notifications or verified data back into the nurse's familiar clinical workflow interface. Developing these standardized interfaces and ensuring semantic interoperability (that a "medication list" means the same thing across all connected systems) requires massive industry collaboration and the adoption of common data standards like FHIR (Fast Healthcare Interoperability Resources) as the lingua franca for off-chain data [30].

The regulatory and legal landscape is currently underdeveloped for blockchain-based health records. Regulations like HIPAA in the United States and GDPR in the European Union were not written with decentralized ledgers in mind. Key questions arise: Who is the designated "covered entity" or "data controller" in a decentralized network? How does the right to erasure ("the right to be forgotten") under GDPR reconcile with the immutable nature of a blockchain? Can a hash of deleted off-chain data remain without violating the regulation? Legal frameworks will need to evolve to recognize cryptographic proof and smart contracts as valid instruments for consent

management and data audits [31]. Furthermore, establishing liability in a system with multiple data contributors (nurses, doctors, patients, devices) and automated smart contracts is a complex legal frontier that must be clarified before widespread adoption.

Organizational and cultural barriers are equally formidable. Implementing such a system requires unprecedented levels of collaboration and trust between traditionally competitive healthcare institutions. Governance models for a consortium blockchain—deciding who can run nodes, how consensus is managed, how costs are shared—are non-trivial. There is also the significant challenge of change management for the end-users, primarily nurses and other clinicians. They must be trained not only on a new interface but potentially on new conceptual models of data ownership and sharing. Resistance to change, workflow disruptions during transition, and the digital divide affecting some patient populations are real human factors that can derail implementation if not carefully managed with inclusive design and extensive education [32].

Finally, while blockchain enhances security in many ways, it introduces new attack vectors and considerations. The security of private keys is paramount; if a nurse loses the smartphone containing their private key or has it stolen, it could lock them out of the documentation system or allow impersonation. Robust, user-friendly key management and recovery solutions are essential. The 51% attack, while improbable in a large healthcare consortium, is a theoretical risk. More pragmatically, the overall security of the system will only be as strong as its weakest link, which could be a poorly secured off-chain data server or vulnerabilities in the smart contract code itself, which can be exploited if not meticulously audited [33].

6. Emerging Applications in Healthcare

While widespread, full-scale implementation of blockchain for nursing documentation remains largely in the pilot and research phase, several pioneering projects and use cases illuminate the path forward and validate its core concepts. These initiatives often focus on specific, high-value problems within the data management ecosystem, demonstrating tangible benefits.

One prominent area is the management of pharmaceutical supply chains and drug provenance. Projects like MediLedger have used blockchain to create a track-and-trace system for pharmaceuticals, combatting counterfeit drugs. While not directly nursing documentation, this ensures the integrity of the medications nurses administer. A nurse could, in theory, scan a drug vial and instantly verify its entire journey from manufacturer to bedside, immutably recorded on a blockchain, ensuring patient safety [34]. This model of provenance is directly applicable to documenting the chain of custody for blood products, human milk, or high-value medical devices.

In the realm of personal health data, the MyHealthMyData initiative in the European Union and similar projects explore patient-centric data marketplaces built on blockchain. Patients can aggregate data from various sources (EHRs, wearables, genomic tests) into a personal health vault. They then grant researchers or companies time-limited, granular access to this data in exchange for compensation or to contribute to specific studies. This demonstrates the practical application of self-sovereign identity and granular consent for data sharing, a model that could eventually feed relevant, patient-shared data back into the clinical record used by nurses [35].

For clinical trials, blockchain is being piloted to enhance data integrity and patient consent management. Every step of the trial process—patient consent, randomization, data collection from sites, adverse event reporting—can be immutably recorded. This prevents data tampering, ensures auditability, and streamlines monitoring. A nurse acting as a clinical trial coordinator could document patient interactions with the certainty that the record is permanently sealed and verifiable, increasing trust in trial outcomes [36].

Specific to nursing documentation and care coordination, smaller-scale pilots have emerged. For instance, some projects have created blockchain-based systems for shared care planning in multi-agency settings, such as elderly care involving hospitals, home care nurses, general practitioners, and social workers. Each entity documents their interventions on a shared ledger, creating a single, reconciled view of the care plan that all parties can trust, reducing miscommunication and gaps in care [37]. Another application is in credentialing and license verification. A blockchain could hold immutable records of nursing licenses, certifications, and competencies, issued by state boards and accrediting bodies. When a nurse joins a new hospital or takes on a telehealth assignment, their credentials can be verified instantly and trustlessly, streamlining the onboarding process [38].

These real-world experiments, though not yet mainstream, provide critical proof-of-concept. They demonstrate that the technology can function in regulated environments, deliver promised benefits like enhanced integrity and patient control, and begin to tackle the practical hurdles of integration

and governance. They serve as foundational building blocks for more comprehensive future systems.

7. The Future Trajectory and Implications for the Nursing Profession

The prospective integration of blockchain technology into the healthcare information infrastructure will not be an isolated IT upgrade but a transformative force that will reshape the nursing profession's relationship with data, patients, and the broader care team. Looking forward, the trajectory points toward increasingly sophisticated, integrated, and intelligent systems built upon a foundational layer of trusted data.

The future will likely see the convergence of blockchain with other cutting-edge technologies, most notably Artificial Intelligence (AI) and the Internet of Medical Things (IoMT). A blockchain can provide the secure, auditable, and rich data pipeline required to train reliable AI models for clinical decision support. For example, an AI algorithm designed to predict patient deterioration could be trained on immutable, high-quality nursing assessment data from a blockchain network, ensuring the data's integrity and provenance [39]. In turn, AI could analyze real-time data from IoMT devices (smart beds, wearable monitors, infusion pumps) that write hashed data to the blockchain, providing nurses with intelligent alerts and predictive insights directly within their documentation workflow, all based on a verifiable data source.

This evolution will redefine key nursing roles. The nurse's responsibility in documentation will elevate from data entry clerk to data steward and interpreter. With routine administrative tasks automated by smart contracts and with a unified, complete patient record available, nurses can focus their cognitive efforts on critical thinking, clinical judgment, and the synthesis of information into personalized care plans. The nurse will also play a crucial role in patient education, helping individuals understand and manage their digital health identities, consent settings, and how to engage with their blockchain-based health records [40]. This fosters a stronger nurse-patient partnership built on transparency and shared information.

Furthermore, blockchain could revolutionize nursing administration and outcomes research. Workforce management, scheduling, and credentialing could be managed via decentralized applications (dApps). More importantly, the ability to access large-scale, aggregated, yet privacy-preserving datasets of nursing-sensitive outcomes (e.g., pressure injury rates, fall rates correlated with specific nursing interventions) could fuel a new era of evidence-based practice. Nurses could conduct practice-based research with unprecedented ease and rigor, contributing directly to the body of nursing knowledge and demonstrating their unique impact on patient outcomes [40].

8. Conclusion:

In conclusion, blockchain technology presents a paradigm-shifting opportunity to address the deep-seated flaws in current systems for nursing documentation and patient privacy. By offering a framework for immutability, decentralized trust, patient sovereignty, and automated logic, it promises to enhance data integrity, streamline interdisciplinary workflow, and fundamentally empower patients. However, this future is not inevitable. It hinges on successfully navigating a gauntlet of technical scalability issues, regulatory modernization, organizational collaboration, and human-centered design. For the nursing profession, engagement in this evolution is not optional but essential. Nurses must move from being passive end-users to active co-designers, advocates, and ethical guides, ensuring that these powerful new tools are implemented in ways that truly enhance care, protect the vulnerable, and uphold the humanistic core of the nursing practice. The journey toward a blockchain-enabled health record will be complex and lengthy, but its destination—a more secure, efficient, transparent, and patient-empowered healthcare system—is a vision worthy of pursuit.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Agbo C., Mahmoud Q., Eklund J. "Blockchain Technology in Healthcare: A Systematic Review,". Healthcare. 2019 Apr.7(2):56. doi: 10.3390/healthcare7020056.

[2] Abdel-Basset M., Chang V., Nabeeh N. A. "An Intelligent Framework using Disruptive Technologies for COVID-19 analysis,". Technological Forecasting and Social Change. 2020 Oct.163:120431. doi: 10.1016/j.techfore.2020.120431.

[3] McGhin T., Choo K.-K. R., Liu C. Z., He D. "Blockchain in healthcare applications: Research challenges and opportunities,". Journal of Network and Computer Applications. 2019 Jun.135:62–75. doi: 10.1016/j.jnca.2019.02.027.

[4] Christensen C., Raynor M., Mcdonald R. "What is disruptive innovation? Twenty years after the introduction of the theory, we revisit what it does-and doesn't-explain,". 2015 Available: https://www.innosight.com/wp-content/uploads/2018/01/Innosight_HBR_What-is-Disruptive-Innovation.pdf.

[5] Haleem A., Javaid M., PS R. P., Suman R., Rab S. "Blockchain Technology Applications in Healthcare: An Overview,". International Journal of Intelligent Networks. 2021;2(2):130–139. doi: 10.1016/j.ijin.2021.09.005.

[6] Yaqoob I., Salah K., Jayaraman R., Al-Hammadi Y. "Blockchain for Healthcare Data management: opportunities, challenges, and Future Recommendations,". Neural Computing and Applications. 2021 Jan.34:1–16. doi: 10.1007/s00521-020-05519-w.

[7] Kuo T.-T., Zavaleta Rojas H., Ohno-Machado L. "Comparison of blockchain platforms: a systematic review and healthcare examples,". Journal of the American Medical Informatics Association. 2019 Mar.26(5):462–478. doi: 10.1093/jamia/ocy185.

[8] Sounderajah V., et al. "Are disruptive innovations recognized in the healthcare literature? A systematic review,". BMJ Innovations. 2020 Sep.7(1):bmjinnov-2020-000424. doi: 10.1136/bmjinnov-2020-000424.

[9] Mettler M. "Blockchain technology in healthcare: The revolution starts here,". 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) 2016 Sep.:1–3. doi: 10.1109/healthcom.2016.7749510.

[10] Frizzo-Barker J., Chow-White P. A., Adams P. R., Mentanko J., Ha D., Green S. "Blockchain as a disruptive technology for business: A systematic review,". International Journal of Information Management. 2019 Nov.51(102029):102029. doi: 10.1016/j.ijinfomgt.2019.10.014.

[11] Dimitrov D. V. "Blockchain Applications for Healthcare Data Management,". Healthcare Informatics Research. 2019;25(1):51. doi: 10.4258/hir.2019.25.1.51.

[12] Lu Y. "The blockchain: State-of-the-art and research challenges,". Journal of Industrial Information Integration. 2019 Sep.15:80–90. doi: 10.1016/j.jii.2019.04.002.

[13] Reddy B., Madhushree, Aithal P. S. "Blockchain as a Disruptive Technology in Healthcare and Financial Services - a Review Based Analysis on Current Implementations,". papers.ssrn.com.2020 May 27; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3611482.

[14] Attaran M. "Blockchain technology in healthcare: Challenges and opportunities,". International Journal of Healthcare Management. 2020 Nov.15(1):1–14. doi: 10.1080/20479700.2020.1843887.

[15] Khezr S., Moniruzzaman M., Yassine A., Benlamri R. "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research,". Applied Sciences. 2019 Apr.9(9):1736. doi: 10.3390/app9091736.

[16] Warkentin M., Orgeron C. "Using the security triad to assess blockchain technology in public sector applications,". International Journal of Information Management. 2020 Feb.52:102090. doi: 10.1016/j.ijinfomgt.2020.102090.

[17] AV A. A., O'Donoghue O., Brindley D., Meinert E. "Implementing Blockchains for Efficient Health Care: Systematic Review,". Journal of Medical Internet Research. 2019 Feb.21(2):e12439. doi: 10.2196/12439.

[18] Prokofieva M., Miah S. J. "Blockchain in healthcare,". Australasian Journal of Information Systems. 2019 Jul.23 doi: 10.3127/ajis.v23i0.2203.

[19] Schinckus C. "A Nuanced perspective on blockchain technology and healthcare,". Technology in Society. 2022 Nov.71:102082. doi: 10.1016/j.techsoc.2022.102082.

[20] SR A. S., Bedi P., Goyal S. B., Shaw R. N., Ghosh A., Aggarwal S. "AI and Blockchain for Healthcare Data Security in Smart Cities,". AI and IoT for Smart City Applications. 2022:185–198. doi: 10.1007/978-981-16-7498-3_12.

[21] Namasudra S., Chandra Deka G. Applications of Blockchain in Healthcare. Singapore: Springer Singapore; 2021.

[22] MH H. M., MY S. M., IU N. I., Ninggal M. I. H., Salman S. "Blockchain technology in the healthcare industry: Trends and opportunities,". Journal of Industrial Information Integration. 2021 Jun.22:100217. doi: 10.1016/j.jii.2021.100217.

[23] LH J. L., Sawaya W., Dobrzykowski D. "Exploring blockchain adoption intentions in the supply chain: perspectives from innovation diffusion and institutional theory,". International Journal of Physical Distribution & Logistics Management. 2021 Dec.ahead-of-print(ahead-of-print) doi: 10.1108/ijpdlm-05-2020-0163.

[24] Turner M., Kitchenham B., Brereton P., Charters S., Budgen D. "Does the technology acceptance model predict actual use? A systematic literature review,". Information and Software Technology.

2010 May;52(5):463–479. doi: 10.1016/j.infsof.2009.11.005.

[25] Chen Y., Ding S., Xu Z., Zheng H., Yang S. "Blockchain-Based Medical Records Secure Storage and Medical Service Framework,". Journal of Medical Systems. 2018 Nov.43(1) doi: 10.1007/s10916-018-1121-4.

[26] Zheng Z., Xie S., ND H. N., Chen X., Wang H. "Blockchain challenges and opportunities: a survey,". International Journal of Web and Grid Services. 2018;14(4):352–375. doi: 10.1504/ijwgs.2018.095647.

[27] Siyal A., Junejo A., Zawish M., Ahmed K., Khalil A., Soursou G. "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives,". Cryptography. 2019 Jan.3(1):3. doi: 10.3390/cryptography3010003.

[28] Mackey T. K., et al. "'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare,". BMC Medicine. 2019 Mar.17(1) doi: 10.1186/s12916-019-1296-7.

[29] Hillestad R., et al. "Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, And Costs,". Health Affairs. 2005 Sep.24(5):1103–1117. doi: 10.1377/hlthaff.24.5.1103.

[30] AF H. A., Hanna S., Halamka J. D., Sicker D. C., Spangenberg P., Hashmi S. K. "Blockchains integrated with digital technology revolution: The future of healthcare ecosystems. (Preprint),". Journal of Medical Internet Research. 2020 May; doi: 10.2196/19846.

[31] Radanović I., Likić R. "Opportunities for Use of Blockchain Technology in Medicine,". Applied Health Economics and Health Policy. 2018 Jul.16(5):583–590. doi: 10.1007/s40258-018-0412-8.

[32] AM A. A., Schelen O., Andersson K. "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities,". IEEE Access. 2019;7:117134–117151. doi: 10.1109/access.2019.2936094.

[33] Yaeger K., Martini M., Rasouli J., Costa A. "Emerging Blockchain Technology Solutions for Modern Healthcare Infrastructure,". Journal of Scientific Innovation in Medicine. 2019;2(1) doi: 10.29024/jsim.7.

[34] Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. "Where Is Current Research on Blockchain Technology?—A Systematic Review,". PLOS ONE. 2016 Oct.11(10):e0163477. doi: 10.1371/journal.pone.0163477.

[35] Hasselgren A., Kralevska K., Gligoroski D., AP S. A., Faxvaag A. "Blockchain in healthcare and health sciences—A scoping review,". International Journal of Medical Informatics. 2020 Feb.134:104040. doi: 10.1016/j.ijmedinf.2019.104040.

[36] Shahnaz A., Qamar U., Khalid A. "Using Blockchain for Electronic Health Records,". IEEE Access. 2019;7(1):147782–147795. doi: 10.1109/access.2019.2946373.

[37] Ekblaw A., Azaria A., Halamka J., Lippman A., Vieira T. "A Case Study for Blockchain in Healthcare: 'MedRec' prototype for electronic health records and medical research data White Paper MedRec: Using Blockchain for Medical Data Access and Permission Management IEEE Original,". 2016 Available: http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/5-onc_blockchainchallenge_mitwhitepaper_copyright updated.pdf.

[38] El-Gazzar R., Stendal K. "Blockchain in Health Care: Hope or Hype?,". Journal of Medical Internet Research. 2020 Jul.22(7):e17199. doi: 10.2196/17199.

[39] Ølnes S., Ubacht J., Janssen M. "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,". Government Information Quarterly. 2017 Sep.34(3):355–364. doi: 10.1016/j.giq.2017.09.007.

[40] HK M. H., DeFranco J., Malas T., Laplante P., Destefanis Giuseppe, Graciano Neto V. V. "Exploring Research in Blockchain for Healthcare and a Roadmap for the Future,". IEEE Transactions on Emerging Topics in Computing. 2019:1–1. doi: 10.1109/TETC.2019.2936881.