International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 1, Issue 1, 2022
DOI: https://doi.org/10.38124/ijsrmt.v1i1.493

Blockchain-Enabled Pharmacovigilance Infrastructure for National Cancer Registries

Salvation Ifechukwude Atalor[1]

[1] Department of Pharmacy, Imanzoe Drug Store, Abuja, Nigeria.

Publication Date: 2022/01/30

Abstract

The integration of blockchain technology into pharmacovigilance infrastructure for national cancer registries presents a transformative approach to managing drug safety data. Traditional pharmacovigilance systems often face challenges such as fragmented data sources, delayed reporting, lack of transparency, and data security risks. Blockchain offers a decentralized, immutable, and transparent framework that can enhance the accuracy, timeliness, and reliability of adverse drug reaction (ADR) reporting. This review explores how blockchain can be applied to cancer registries to create a more efficient and trustworthy pharmacovigilance ecosystem. It highlights the key components of a blockchain-enabled infrastructure, including smart contracts for automating data validation, permissioned ledgers for maintaining patient confidentiality, and interoperability standards to facilitate seamless data exchange among stakeholders. Furthermore, it discusses the potential benefits such as improved patient safety, strengthened regulatory oversight, enhanced collaboration among healthcare providers, and empowerment of patients in the pharmacovigilance process. Despite the promising prospects, challenges including technical complexity, regulatory compliance, scalability, and stakeholder acceptance must be addressed. Overall, blockchain holds significant potential to revolutionize pharmacovigilance practices, particularly in oncology, where timely detection and response to drug-related adverse events are critical for patient outcomes and public health.

Keywords: *Blockchain Technology, Pharmacovigilance, Cancer Registries and Drug Safety.*

I. INTRODUCTION

➢ *Background on Pharmacovigilance*

Pharmacovigilance refers to the science and activities relating to the detection, assessment, understanding, and prevention of adverse effects or any other drug-related problems. It plays a crucial role in ensuring patient safety and maintaining public health confidence in medicinal products. As the complexity of therapeutic treatments has evolved, especially in oncology, pharmacovigilance systems have become essential for monitoring the real-world performance of drugs beyond clinical trials. Effective pharmacovigilance activities help in identifying previously unrecognized adverse reactions, understanding the risk-benefit profile of medicines, and enabling timely regulatory interventions (World Health Organization, 2002; Edwards, 2017).

Over the past decades, the global pharmacovigilance landscape has expanded due to increased regulatory requirements and the growing volume of marketed pharmaceuticals. Traditional pharmacovigilance systems primarily rely on spontaneous reporting mechanisms, which often suffer from underreporting, delayed submissions, and fragmented datasets (Banerjee & Bihani, 2019). With the emergence of big data analytics and digital health innovations, there have been calls for modernization of pharmacovigilance practices to make them more proactive, data-driven, and integrated across healthcare ecosystems (Gonzalez-Gonzalez et al., 2018). This is particularly significant in oncology, where adverse drug reactions can be severe and patient populations are often vulnerable, necessitating robust and reliable safety monitoring frameworks.

➢ *Problem Statement*

Despite significant advancements in pharmacovigilance systems, the management of adverse drug reactions within national cancer registries remains highly fragmented, inefficient, and prone to errors. Traditional centralized systems often struggle with issues such as delayed data reporting, lack of transparency, data breaches, and insufficient interoperability between institutions. In the context of oncology, where timely and accurate information is critical to patient outcomes, these shortcomings pose severe risks to both individual and public health. There is an urgent need for a secure, transparent, and efficient infrastructure that can support real-time pharmacovigilance activities, enhance stakeholder collaboration, and uphold patient confidentiality. Blockchain technology emerges as a promising solution to address these persistent challenges by offering decentralized, immutable, and transparent data management frameworks tailored to the complex needs of cancer registries.

- *Objectives of the Paper*

The primary objective of this paper is to explore how blockchain technology can be leveraged to build a robust and efficient pharmacovigilance infrastructure for national cancer registries. It aims to examine the limitations of current pharmacovigilance systems, outline the potential advantages of blockchain integration, and propose a conceptual framework for its implementation. Additionally, the paper seeks to analyze the benefits blockchain can offer in terms of data transparency, security, interoperability, and patient empowerment within oncology care. By identifying both the opportunities and challenges associated with blockchain adoption, the paper intends to provide strategic insights for healthcare policymakers, regulatory authorities, technology developers, and clinical researchers who are committed to improving drug safety monitoring practices in cancer treatment.

- *Limitations of Traditional Pharmacovigilance Systems*

Traditional pharmacovigilance systems, while foundational to drug safety monitoring, are often plagued by significant limitations that undermine their effectiveness. These systems largely rely on passive surveillance methods such as spontaneous reporting, which frequently result in underreporting and incomplete data capture (Hazell & Shakir, 2006). Furthermore, the fragmentation of healthcare data across multiple platforms and institutions creates barriers to timely data sharing and integration, leading to delays in detecting and responding to adverse drug reactions (Gonzalez-Gonzalez et al., 2018). Issues related to data security and patient confidentiality are also prevalent, with centralized databases vulnerable to breaches and unauthorized access. In addition, the manual nature of traditional pharmacovigilance processes increases the risk of human errors, inconsistency in data interpretation, and inefficiencies in regulatory communication. These challenges are especially critical in oncology, where rapid identification and management of adverse events can significantly influence treatment outcomes and patient safety.

- *Structure of the Paper*

This paper begins by providing a foundational understanding of blockchain technology, explaining its core principles, different types, and its relevance to healthcare systems. It then explores the key challenges faced by current pharmacovigilance practices, particularly within national cancer registries, emphasizing the need for more secure, transparent, and efficient systems. The discussion moves on to how blockchain can be integrated into pharmacovigilance infrastructure, highlighting essential components such as smart contracts and interoperability frameworks. The potential benefits of adopting blockchain, including enhanced data security, improved reporting efficiency, and greater stakeholder collaboration, are critically analyzed. Attention is also given to the technical, regulatory, and practical challenges that could hinder blockchain adoption in healthcare. Finally, the paper outlines future directions and provides strategic insights to guide effective implementation of blockchain-enabled pharmacovigilance systems.

II. BLOCKCHAIN TECHNOLOGY OVERVIEW

Blockchain is a distributed ledger technology that enables the secure recording, storage, and transfer of information across a network of computers without the need for a central authority. It operates on principles of decentralization, immutability, transparency, and consensus, ensuring that once data is entered into the blockchain, it cannot be altered without the agreement of the majority of the network participants (Nakamoto, 2008). Each block in the chain contains a set of transactions, a timestamp, and a cryptographic link to the previous block, forming an unbroken and verifiable chain of data. Initially conceptualized to support cryptocurrencies such as Bitcoin, blockchain's unique features have attracted widespread interest across sectors including finance, supply chain management, and healthcare (Yli-Huumo et al., 2016). In healthcare, blockchain offers the potential to enhance data security, promote interoperability, and empower patients with greater control over their personal health information.

Various types of blockchain frameworks exist, each suited to different use cases. Public blockchains, such as Bitcoin and Ethereum, are open to anyone and emphasize transparency and decentralization. Private blockchains, controlled by a single organization, offer greater control over access but sacrifice some decentralization. Consortium blockchains, governed by a group of organizations, provide a balance between transparency and confidentiality, making them particularly relevant for sensitive environments like healthcare (Zhang & Jacobsen, 2018). The ability of blockchain to create tamper-proof records while maintaining selective transparency makes it an attractive technology for addressing many longstanding challenges in pharmacovigilance systems, including data fragmentation, delayed reporting, and privacy concerns. Understanding these fundamental attributes is essential for assessing blockchain's potential to transform the pharmacovigilance landscape within national cancer registries.

- *Fundamentals of Blockchain*

Blockchain technology fundamentally operates as a decentralized and distributed digital ledger that records transactions across a network of computers. Unlike traditional centralized databases, where a single entity controls the data, blockchain ensures that all participants maintain a synchronized copy of the ledger, which updates automatically through a consensus mechanism (Crosby et al., 2016) as represented in figure 1. Each transaction is grouped into blocks, and once a block is completed, it is linked to the previous block through cryptographic hashes, forming a continuous and immutable chain. This architecture enhances data integrity, as altering a single block would require altering all subsequent blocks across the majority of the network, making fraudulent activities virtually impossible (Swan, 2015). The decentralized nature of blockchain eliminates single points of failure, enhancing the resilience and reliability of the entire system.

Additionally, blockchain incorporates key mechanisms such as public-key cryptography and consensus algorithms to ensure security and trust among participants. Public-key cryptography enables users to securely sign transactions, while consensus algorithms like Proof of Work (PoW) or Practical Byzantine Fault Tolerance (PBFT) validate transactions without the need for a trusted intermediary (Narayanan et al., 2016). Smart contracts, which are self-executing contracts with terms directly written into code, further extend blockchain's capabilities by enabling automated and conditional transactions without human intervention (Christidis & Devetsikiotis, 2016). These fundamental features—decentralization, immutability, transparency, and automation—are what make blockchain a transformative technology with vast potential for sectors like healthcare, finance, and supply chain management, particularly where trust, data security, and accountability are critical.

Fig 1 visually summarizes the foundational components and operational features of blockchain technology. At the core lies the concept of a decentralized ledger, where data is not stored in a single location but is replicated across all participating nodes, ensuring resilience and eliminating single points of failure. The architecture branch illustrates how transactions are grouped into blocks, each cryptographically linked to the previous block, forming an immutable chain that preserves data integrity—any attempt to alter a block would require consensus across the majority of the network. The functional features branch highlights the mechanisms that make blockchain secure and trustworthy: public-key cryptography secures user identities and transaction authenticity, while consensus mechanisms like Proof of Work (PoW) and Practical Byzantine Fault Tolerance (PBFT) allow nodes to agree on valid transactions without needing a central authority. Furthermore, smart contracts are shown as programmable agreements that self-execute when predefined conditions are met, enhancing automation and reducing the need for intermediaries. These interconnected elements collectively support key blockchain benefits such as transparency, trust, automation, and robust security, making the technology highly applicable in domains where accountability and data integrity are paramount.

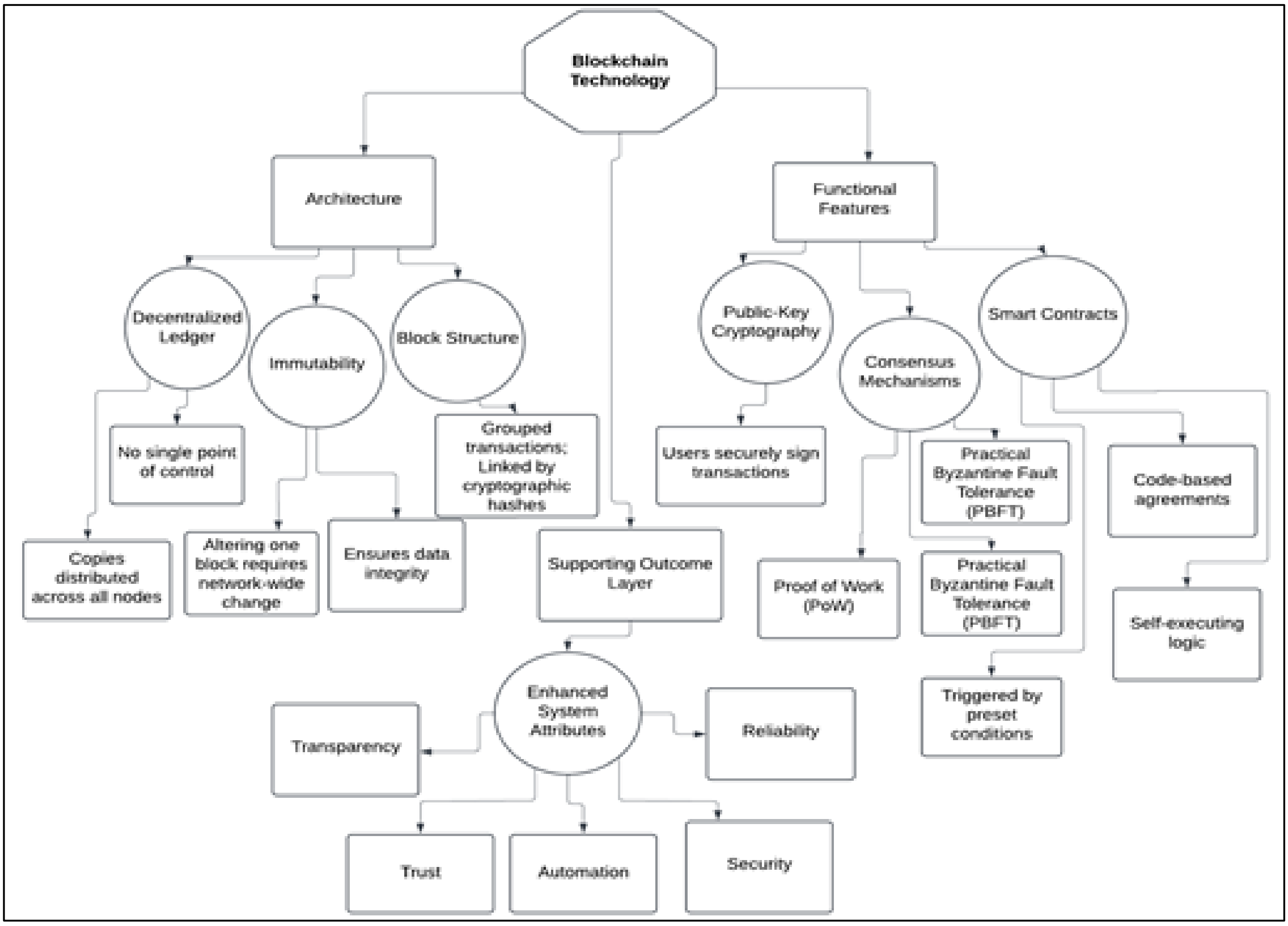

Fig 1 Diagram Illustration of Blockchain Architecture, Decentralization, Consensus Mechanisms, Cryptographic Security, and Smart Contract Functionality.

➢ *Types of Blockchain (Public, Private, Consortium)*

Blockchain networks can generally be classified into three major types: public, private, and consortium blockchains, each offering different levels of decentralization, accessibility, and governance. Public blockchains, such as Bitcoin and Ethereum, are fully decentralized and permissionless, allowing anyone to join the network, validate transactions, and access the ledger as presented in table 1(Zheng et al., 2018). These networks emphasize transparency and security, relying on consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to achieve trust without centralized oversight. However, the openness of public blockchains can lead to scalability challenges, high energy consumption, and privacy concerns, making them less suitable for applications requiring strict confidentiality, such as healthcare records (Yli-Huumo et al., 2016).

In contrast, private blockchains are permissioned systems where a single organization controls participation and validation rights. They offer greater efficiency, faster transaction speeds, and enhanced data privacy, but at the cost of reduced decentralization (Cachin, 2016). Consortium blockchains represent a hybrid model, governed by a group of pre-selected institutions rather than a single entity or the public at large. This approach balances the transparency and decentralization of public blockchains with the controlled access and privacy features of private blockchains (Zhang & Jacobsen, 2018). In healthcare contexts such as national cancer registries, consortium blockchains are particularly attractive because they allow trusted entities like hospitals, research institutions, and regulatory bodies to collaboratively maintain a secure, transparent, and interoperable system for pharmacovigilance activities

Table 1 Summary of The Types of Blockchain (Public, Private, Consortium) As You Requested

Type of Blockchain	Definition	Characteristics	Examples
Public Blockchain	A decentralized network open to anyone to participate, validate, and view transactions.	Transparent, permissionless, secure but slower due to consensus complexity.	Bitcoin, Ethereum
Private Blockchain	A restricted blockchain where only selected participants can access and validate transactions.	Faster transactions, higher privacy, centralized control, limited transparency.	Hyperledger Fabric, R3 Corda
Consortium Blockchain	A semi-decentralized blockchain controlled by a group of organizations.	Partially private, higher efficiency, controlled access among trusted entities.	Energy Web Foundation, IBM Food Trust
Hybrid Blockchain	A combination of public and private blockchains where certain data is public and some private.	Flexible, scalable, allows both transparency and confidentiality.	Dragonchain, XinFin

➢ *Relevance of Blockchain in Healthcare*

Blockchain technology holds significant promise for transforming healthcare by enhancing data security, interoperability, and patient empowerment. In traditional healthcare systems, patient data is often fragmented across multiple providers, leading to inefficiencies, duplication of efforts, and potential medical errors. Blockchain can provide a unified, tamper-proof ledger for patient health records, enabling seamless data sharing across healthcare providers while maintaining strict patient privacy through encryption and permissioned access controls as represented in figure 2 (Azaria et al., 2016). Furthermore, blockchain's transparency and immutability can improve the traceability of pharmaceuticals and medical devices, helping to combat counterfeit drugs and ensure regulatory compliance (Mettler, 2016). Smart contracts can automate administrative processes such as insurance claims and consent management, reducing costs and administrative burden. Additionally, blockchain enables patients to have more control over their health data, allowing them to grant or revoke access to providers as needed (Ekblaw et al., 2016). These advantages make blockchain a highly relevant solution for addressing longstanding challenges in healthcare delivery, data management, and pharmacovigilance systems.

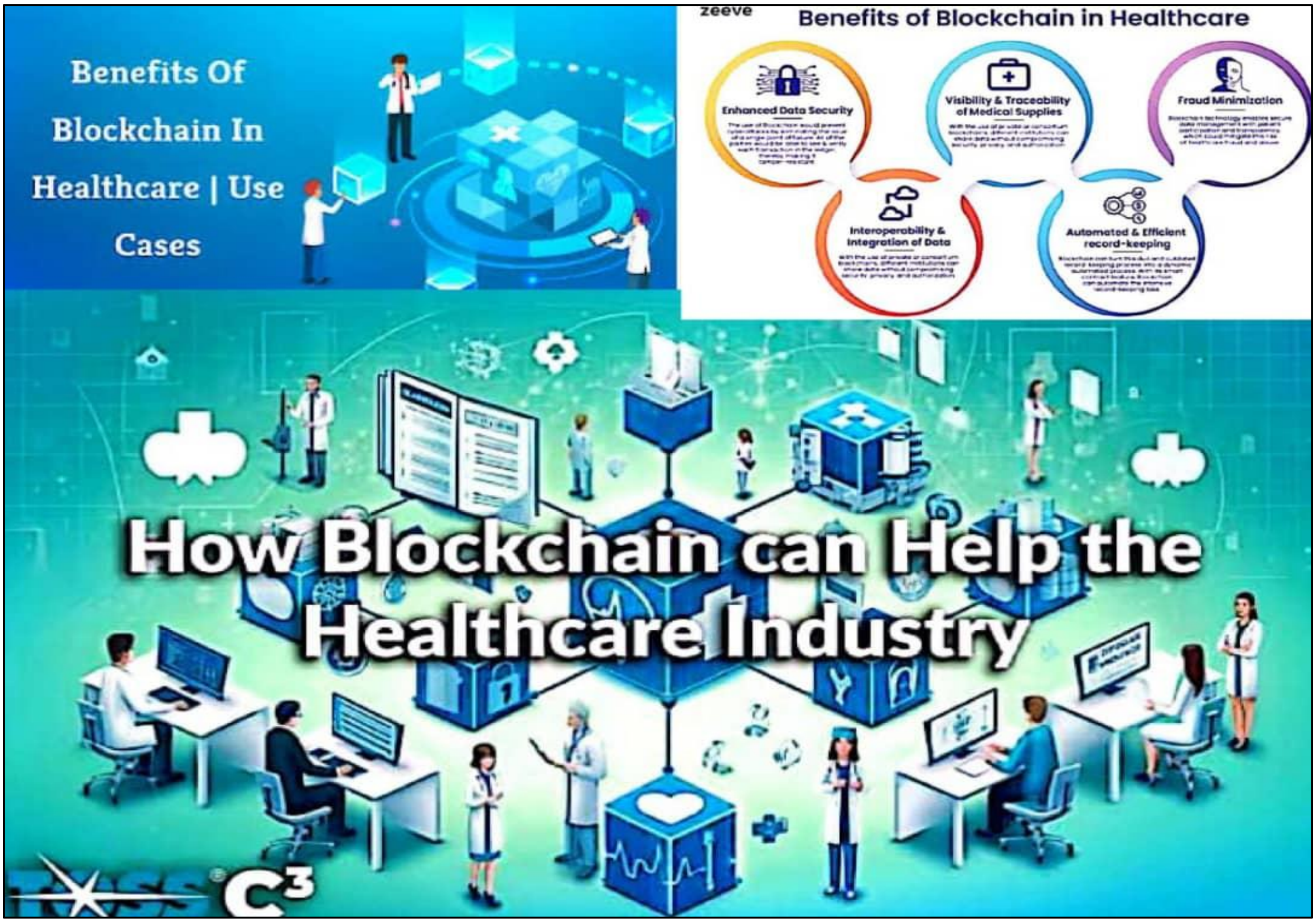

Fig 2 Picture of Enhancing Healthcare Through Blockchain by Securing Data Empowering Patients and Streamlining Interoperability (Azaria et al., 2016).

Fig 2 visually encapsulates the transformative role of blockchain technology in the healthcare industry by depicting a digitally interconnected healthcare environment where data flows seamlessly among healthcare professionals, patients, and medical systems. At the center, a symbolic blockchain node highlights the technology's foundational role in securing and linking patient records across diverse systems. Surrounding this hub are healthcare professionals interacting with digital interfaces, representing blockchain's facilitation of real-time, tamper-proof, and encrypted health data sharing. The overlay of network connections and digital records suggests enhanced interoperability, eliminating data silos and reducing redundancy. The presence of elements like smart contract icons and secure ledgers also illustrates how blockchain automates insurance claims and consent management through decentralized applications, cutting administrative overhead. Furthermore, the representation of patients interfacing with these systems underscores increased patient autonomy, as blockchain empowers individuals to control access to their medical data. Overall, the image effectively visualizes blockchain's potential to address critical challenges in healthcare data security, privacy, traceability, and operational efficiency.

III. PHARMACOVIGILANCE CHALLENGES IN CANCER REGISTRIES

Pharmacovigilance within cancer registries faces several critical challenges related to data collection, reporting accuracy, and timeliness. Cancer treatments often involve complex regimens, including chemotherapy, immunotherapy, and targeted therapies, which can produce diverse and sometimes delayed adverse drug reactions (ADRs) as represented in figure 3 (Ardizzoni et al., 2017). Traditional pharmacovigilance systems may struggle to capture these ADRs effectively due to fragmented reporting mechanisms and underreporting by healthcare professionals. Additionally, discrepancies in data standards and recording practices across institutions hinder the aggregation and analysis of pharmacovigilance data on a national scale (González-González et al., 2013). The lack of a unified and interoperable system often results in data silos, complicating the early detection of safety signals and limiting the ability to identify trends that could inform regulatory actions and clinical decision-making.

Another significant challenge is maintaining the privacy and confidentiality of patient data while ensuring sufficient transparency for pharmacovigilance activities. Cancer registries contain highly sensitive information that must be protected under strict ethical and legal guidelines (Moradian & Howell, 2015). Balancing patient privacy with the need for accessible, high-quality pharmacovigilance data requires sophisticated access controls and auditing capabilities that many current systems lack. Furthermore, existing pharmacovigilance processes tend to be manual, time-consuming, and resource-intensive, leading to delays in reporting adverse events and slow responses to emerging safety concerns. These challenges highlight the urgent need for more advanced, secure, and efficient pharmacovigilance infrastructures capable of supporting the unique complexities associated with cancer care.

Fig 3 Picture of Visualizing Pharmacovigilance Challenges in Cancer Care from Adverse Drug Reactions to Data Integration and Privacy Concerns (Ardizzoni et al., 2017).

Fig 3 vividly captures the multifaceted challenges of pharmacovigilance in cancer registries by illustrating the clinical complexity and pharmaceutical intensity of cancer treatment environments. It combines visuals of operating rooms, oncologists, surgical interventions, and various medications—including chemotherapy pills and injectable drugs—surrounding documents labeled "Cancer Treatment," symbolizing the high-risk and data-sensitive nature of oncology care. This representation aligns with the challenges discussed, such as the fragmented and delayed reporting of adverse drug reactions (ADRs) due to the multifactorial and prolonged effects of cancer therapeutics like immunotherapies and targeted drugs. The diversity of clinical settings shown highlights the inconsistent data recording practices and lack of interoperable systems that impede effective signal detection and pharmacovigilance at scale. Additionally, the presence of sensitive treatment scenarios visually reinforces concerns around patient privacy and regulatory compliance, highlighting the tension between data accessibility and confidentiality. Overall, the image effectively reflects the urgency for modern, integrated, and secure pharmacovigilance infrastructures tailored to the intricacies of oncology care and registry management.

- *Data Fragmentation and Inconsistency*

Data fragmentation and inconsistency represent major barriers to effective pharmacovigilance within cancer registries. Patient information is often dispersed across multiple healthcare providers, electronic health record systems, laboratories, and insurance databases, creating isolated data silos that are difficult to integrate (Khozin et al., 2017). The lack of standardized data formats, terminologies, and reporting practices exacerbates inconsistency, making it challenging to compile comprehensive patient histories or accurately assess adverse drug reactions (Evans, 2016). In many cases, cancer treatment data are recorded inconsistently, with variations in how side effects are classified, coded, and interpreted across different institutions, undermining the reliability of pharmacovigilance analyses.

Moreover, inconsistencies in data collection timelines and reporting completeness further impair the ability to detect safety signals promptly (Nebeker et al., 2013). Without a unified framework, linking longitudinal data about patients' treatment responses and adverse events becomes difficult, slowing regulatory evaluations and compromising patient safety. These persistent issues highlight the need for interoperable systems that can harmonize data from diverse sources while ensuring data accuracy and timeliness an area where blockchain technology shows considerable potential for improvement.

Table 2 Summary of Data Fragmentation and Inconsistency:

Issue	Description	Impact on Pharmacovigilance	Example
Data Silos	Health data stored in isolated databases across multiple institutions.	Limits data sharing, reducing the ability to detect ADR patterns.	Hospital A and Hospital B maintain separate cancer registries.
Inconsistent Formats	Different systems use various data standards and coding schemes.	Causes errors during integration and interpretation of ADR data.	One system uses ICD-10, another uses SNOMED.
Incomplete Records	Missing or partial patient or treatment histories in databases.	Leads to underreporting or misclassification of adverse reactions.	A registry lacks follow-up data on drug outcomes.
Manual Data Entry Errors	Human error during data input due to lack of automation or standardization.	Reduces data reliability and accuracy in ADR detection.	Typing errors in dosage or patient ID.

- *Privacy and Security Concerns*

Privacy and security concerns are significant obstacles to efficient pharmacovigilance, particularly when dealing with sensitive patient data in cancer registries. The personal and clinical information contained within these databases is highly confidential, and breaches could result in severe consequences for patients, including discrimination, stigmatization, and loss of trust in healthcare institutions (Shen et al., 2019). Traditional centralized systems are often vulnerable to cyberattacks, unauthorized access, and internal misuse, exposing weaknesses in data protection mechanisms (Zhang & Wang, 2017). In addition, the need to share data among multiple stakeholders such as hospitals, regulatory agencies, and research organizations increases the risk of exposure and complicates the enforcement of privacy regulations.

Compliance with frameworks like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) adds another layer of complexity, requiring systems to provide secure, auditable, and transparent data access mechanisms (Esmaeilzadeh, 2019). Unfortunately, many current pharmacovigilance infrastructures lack robust encryption, identity verification, and consent management capabilities, making them ill-equipped to handle modern cybersecurity threats. This highlights the urgent necessity for innovative technologies like blockchain that offer decentralized, secure, and transparent solutions for managing sensitive healthcare data effectively.

- *Delayed Adverse Drug Reaction (ADR) Reporting*

Delayed reporting of adverse drug reactions (ADRs) remains a persistent problem within pharmacovigilance systems, especially in oncology settings. Cancer therapies often cause complex and cumulative side effects that may not become evident until weeks or even months after treatment initiation (Postow et al., 2018). However, under current pharmacovigilance frameworks, there is frequently a lag between the occurrence of ADRs and their formal documentation and submission, reducing the timeliness of safety assessments and interventions. This delay can be attributed to fragmented data systems, manual reporting processes, and limited incentives for healthcare providers to prioritize ADR documentation (Aronson, 2017).

Moreover, patient self-reporting, which could provide valuable real-world evidence of ADRs, is often underutilized due to a lack of integrated reporting tools and concerns about data validity (Pacurariu et al., 2018). Delays in ADR reporting compromise early detection of safety signals, posing significant risks to patient safety and limiting the ability of regulatory authorities to respond promptly. Addressing these delays requires more automated, interoperable, and transparent systems capable of capturing and analyzing ADR data in near real-time, where blockchain technology could offer substantial benefits.

IV. BLOCKCHAIN-ENABLED PHARMACOVIGILANCE INFRASTRUCTURE

Blockchain technology presents a promising solution to many of the challenges faced by traditional pharmacovigilance infrastructures. Its decentralized architecture ensures that data is securely distributed across multiple nodes, significantly reducing the risks associated with central points of failure and unauthorized data manipulation (Yue et al., 2016). Through the use of smart contracts, blockchain can automate the reporting and verification of adverse drug reactions (ADRs), ensuring real-time data capture and improving the responsiveness of pharmacovigilance systems (Casino et al., 2019). Immutable ledgers maintained on blockchain platforms enhance data integrity, making it easier to audit and trace the history of ADR reports.

Additionally, blockchain's cryptographic security mechanisms, such as encryption and digital signatures, can safeguard patient confidentiality while facilitating controlled data sharing among authorized stakeholders (Kuo et al., 2017). By enabling transparency, accountability, and interoperability, blockchain infrastructure can transform pharmacovigilance practices within cancer registries, leading to faster detection of safety signals and improved patient outcomes.

➢ *Architecture and Components*

A blockchain-enabled pharmacovigilance system is built on a layered architecture designed to ensure data security, transparency, and interoperability. At its core lies the blockchain network itself, which maintains an immutable, decentralized ledger of adverse drug reaction (ADR) reports and patient treatment data (Azaria et al., 2016). Smart contracts serve as programmable protocols within the network, automating data submission, access control, and regulatory compliance checks without human intervention (Benchoufi & Ravaud, 2017). Data collected from electronic health records, cancer registries, laboratories, and patient self-reports are encrypted and linked to the blockchain using secure APIs, ensuring integrity and confidentiality.

A critical component of this architecture is identity management, often implemented through cryptographic keys and decentralized identifiers (DIDs) to guarantee that only authorized stakeholders can access sensitive information (Zyskind et al., 2015). Additionally, consensus mechanisms like Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) are preferred in healthcare contexts to maintain high transaction throughput while ensuring network trustworthiness among permissioned participants.

➢ *Role of Smart Contracts in Pharmacovigilance*

Smart contracts are automated, self-executing agreements embedded in blockchain networks, and they have the potential to revolutionize pharmacovigilance by enhancing the accuracy, speed, and transparency of adverse drug reaction (ADR) reporting. In the context of pharmacovigilance, smart contracts can streamline the process of submitting ADR reports by automatically verifying and validating the data based on pre-set conditions. For instance, when a healthcare provider reports a suspected ADR, the smart contract can immediately cross-check the details against known drug side effects or interactions stored on the blockchain as represented in figure 3 (Hernandez et al., 2018). This eliminates the need for manual data entry and reduces the likelihood of human error, speeding up the identification of safety signals.

Furthermore, smart contracts can automate the process of notifying relevant regulatory bodies and healthcare professionals in real-time when a new ADR is identified. By doing so, they facilitate rapid responses to potential public health threats, ensuring that important safety information is distributed quickly and accurately (Binns et al., 2019). These contracts can also enforce compliance with regulations, ensuring that all necessary documentation is provided and reviewed, thus enhancing accountability. Ultimately, the integration of smart contracts into pharmacovigilance infrastructures fosters a more efficient and secure system that improves patient safety and enables quicker regulatory actions.

Fig 4 Picture of Smart Contracts in Pharmacovigilance (Hernandez et al., 2018).

Fig 4 visually represents the concept and application of smart contracts within digital and healthcare ecosystems, supporting the explanation in section 4.2 Role of Smart Contracts in Pharmacovigilance. Each quadrant of the image emphasizes the automation, security, and decentralized execution of smart contracts across platforms. The top-left quadrant illustrates the digital interaction and data validation aspect, where smart contracts automatically enforce agreement terms without human intervention. The top-right quadrant, specifically focused on healthcare, outlines a workflow in which healthcare providers submit Adverse Drug Reaction (ADR) reports that are instantly processed and verified against blockchain-stored medical data, ensuring real-time responsiveness. The bottom-left highlights the integration of smart contracts in formal data infrastructure, showcasing network interconnectivity and regulatory adherence. The bottom-right projects a futuristic and secure digital environment enabled by distributed ledgers. Collectively, the image captures how smart contracts revolutionize pharmacovigilance by automating ADR reporting, ensuring data authenticity, triggering regulatory alerts, and enforcing compliance—thereby increasing transparency, accuracy, and patient safety in real-time.

➢ *Interoperability and Data Standardization*

Interoperability and data standardization are critical challenges in pharmacovigilance systems, especially when data comes from multiple, disparate sources such as hospitals, pharmaceutical companies, and regulatory bodies. Blockchain technology offers a solution by ensuring seamless integration of data from diverse sources through its decentralized and open architecture. By using blockchain to store ADR reports and treatment data in a standardized format, all stakeholders can access consistent, real-time information, thus improving data exchange and reducing misinterpretation as presented in table 3 (Zhang et al., 2019). Additionally, blockchain's immutable ledger guarantees that all data entries are preserved in their original form, ensuring consistency over time. Moreover, blockchain enables the use of standardized terminologies such as ICD-10 or SNOMED CT, ensuring that adverse events are uniformly documented across institutions (Mandl et al., 2018). The standardization and enhanced interoperability offered by blockchain can harmonize global pharmacovigilance efforts, ensuring that data is comparable and actionable across jurisdictions. This integration paves the way for faster regulatory actions, improved patient safety, and a more efficient pharmacovigilance infrastructure.

Table 3 Summary of Interoperability and Data Standardization

Aspect	**Description**	**Importance**	**Example**
Interoperability Standards	Defined rules that enable different systems to communicate and exchange data.	Ensures seamless sharing of pharmacovigilance data across platforms.	Use of HL7 FHIR to link hospital databases with cancer registries.
Data Harmonization	Aligning diverse datasets into a unified structure or format.	Reduces inconsistencies and improves data analysis and integration.	Mapping drug names from local codes to standardized terminologies.
Cross-Platform Integration	Connecting blockchain infrastructure with legacy healthcare IT systems.	Enables real-time updates and bidirectional data flows.	Linking blockchain with electronic health record (EHR) systems.
Semantic Consistency	Uniform interpretation of medical terms and concepts across systems.	Prevents errors in ADR classification and improves reporting accuracy.	Ensuring "rash" is interpreted consistently across databases.

V. BENEFITS OF BLOCKCHAIN IN PHARMACOVIGILANCE FOR CANCER REGISTRIES

Blockchain technology offers several significant benefits in enhancing pharmacovigilance within cancer registries, primarily by improving data accuracy, security, and accessibility. One key advantage is the ability to provide an immutable record of all adverse drug reactions (ADRs) associated with cancer therapies, ensuring that data cannot be altered or tampered with as represented in figure 5 (Zyskind et al., 2015). This helps in creating transparent, auditable, and trustworthy ADR reports that can be shared across multiple healthcare systems, promoting faster identification of safety signals (Azaria et al., 2016).

Furthermore, blockchain can improve data sharing and collaboration among diverse stakeholders, such as oncologists, regulatory agencies, and pharmaceutical companies, by ensuring interoperability and standardization (Zhang et al., 2019). This streamlined data exchange facilitates better monitoring of cancer treatment outcomes and ADR patterns, contributing to more personalized and safer therapeutic interventions. Additionally, blockchain's secure infrastructure can protect patient privacy, which is especially crucial when dealing with sensitive cancer-related data (Kuo et al., 2017).

Figure 5 illustrates how blockchain technology strengthens pharmacovigilance systems by addressing key challenges in data integrity, collaboration, and clinical decision-making. At its core, blockchain provides a tamper-proof, immutable record of Adverse Drug Reactions (ADRs), ensuring that once data is recorded, it cannot be altered—this feature supports auditability and fosters trust among stakeholders. The first branch focuses on data integrity and transparency, highlighting the importance of creating verifiable ADR logs that aid in regulatory oversight. The second branch covers secure and compliant data sharing, showing how blockchain enables standardized, interoperable communication between oncologists, regulatory agencies, and pharmaceutical firms while safeguarding patient confidentiality through encryption and access control. The third branch emphasizes enhanced clinical insights, where blockchain's real-time data exchange supports early signal detection of drug-related issues and improves monitoring of cancer treatment outcomes. This results in more personalized, accurate, and timely therapeutic interventions, making blockchain a transformative enabler of safe and effective cancer pharmacovigilance.

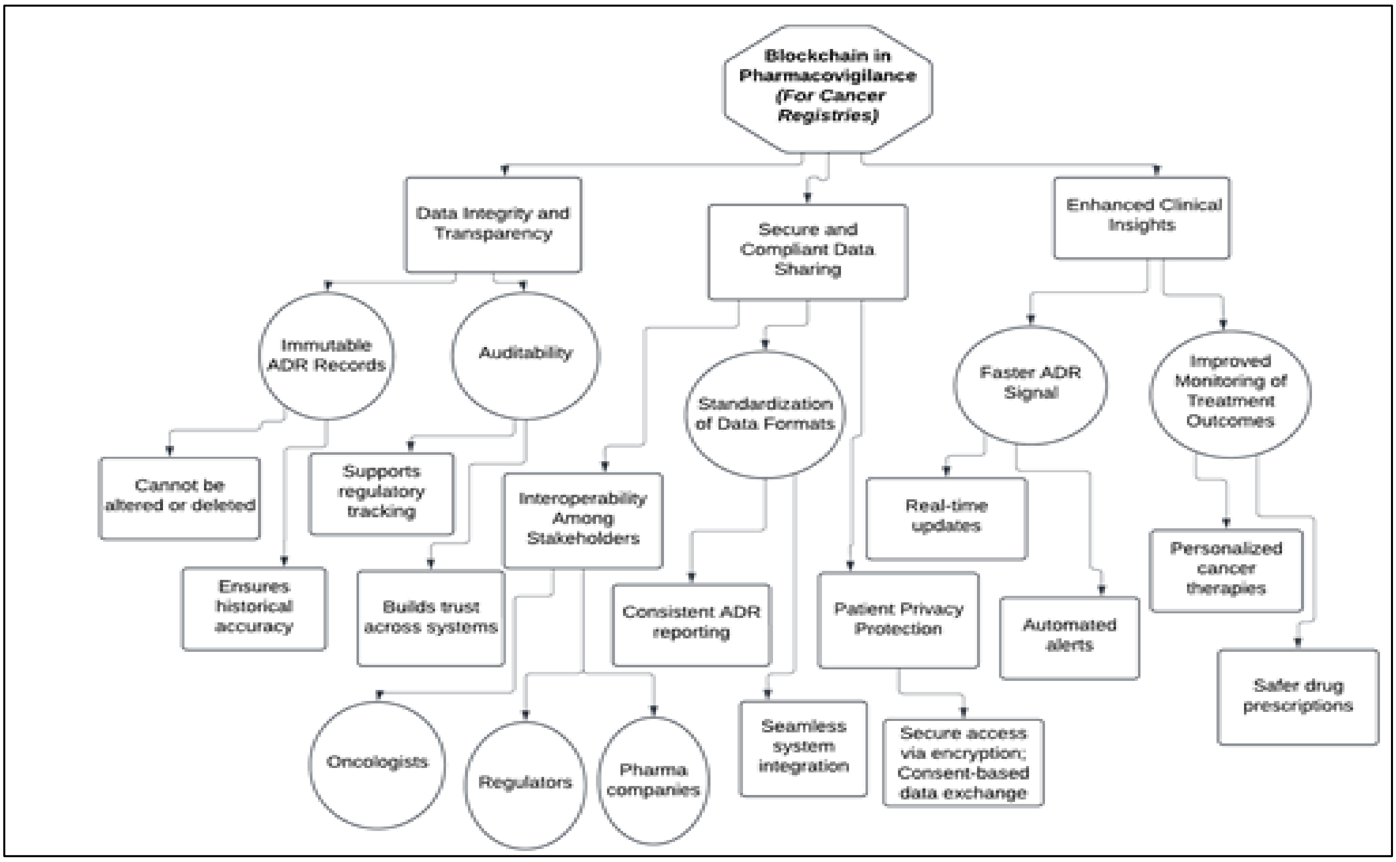

Fig 5 Diagram Illustration of How Blockchain Enhances Data Integrity, Secure Sharing, And Clinical Insights in Cancer Pharmacovigilance.

- *Data Integrity and System-Wide Transparency in Pharmacovigilance*

Blockchain technology significantly enhances data integrity and transparency in pharmacovigilance, particularly within cancer registries, by providing a decentralized and immutable ledger. Each entry on the blockchain is time stamped and cryptographically linked to previous data, making it nearly impossible to alter or manipulate records once they have been added (Azaria et al., 2016). This ensures that adverse drug reactions (ADRs) and other critical data related to cancer therapies are accurate, consistent, and reliable across various healthcare systems and organizations. Blockchain’s inherent transparency allows all stakeholders, including regulatory agencies, oncologists, and patients, to access real-time, trustworthy data, fostering collaboration and improving decision-making (Kuo et al., 2017).

Additionally, the transparency offered by blockchain technology increases accountability in reporting ADRs, reducing the likelihood of underreporting or data omission, which are common issues in traditional pharmacovigilance systems (Zhang et al., 2019). This increased visibility into data helps regulatory bodies and healthcare providers respond promptly to emerging safety concerns, ultimately improving patient safety and treatment outcomes in oncology.

- *Accelerating ADR Detection and Reporting*

Blockchain technology has the potential to dramatically accelerate the detection and reporting of adverse drug reactions (ADRs) in cancer registries by enabling real-time data sharing and analysis. Traditional pharmacovigilance systems often suffer from reporting delays due to fragmented data sources and bureaucratic bottlenecks. In contrast, blockchain’s decentralized structure allows healthcare providers, patients, and regulatory bodies to input and access ADR information simultaneously and securely as presented in figure 4 (Mettler, 2016). This rapid data flow shortens the time between the occurrence of an ADR and its detection by relevant authorities, improving the responsiveness of the pharmacovigilance system.

Moreover, blockchain smart contracts can automate notification processes, ensuring that once an ADR is reported, predefined stakeholders are alerted immediately without the need for manual intervention (Benchoufi & Ravaud, 2017). Such automation can help identify safety signals early, enabling faster regulatory actions, patient safety warnings, and, if necessary, drug recalls. By improving the speed and reliability of ADR reporting, blockchain technology ultimately enhances patient safety and supports more adaptive, evidence-based clinical practices in oncology.

Table 4 Summary of Accelerating ADR Detection and Reporting:

Feature	Description	Impact on ADR Reporting	Example
Real-Time Data Access	Blockchain allows immediate access to updated patient and drug safety data.	Speeds up identification of adverse reactions as they occur.	Instant alerts on unexpected side effects after chemotherapy.
Automated Alerts	Smart contracts trigger notifications when predefined ADR criteria are met.	Enables proactive intervention and timely reporting to authorities.	Notification to oncologists when a patient logs severe nausea.
Decentralized Data Collection	Data is gathered from multiple sources without central control.	Increases coverage and reduces delays caused by centralized processes.	Data from hospitals, pharmacies, and patients on a single platform.
Immutable Recordkeeping	Permanent storage of ADRs ensures integrity and traceability of reports.	Enhances trust in reported data and aids regulatory follow-up.	Auditable trail of ADR reports linked to patient treatments.

➢ *Empowering Patients and Stakeholders*

Blockchain technology empowers patients and other stakeholders by offering greater control over their health data and improving trust in the pharmacovigilance process. Through blockchain's decentralized and transparent nature, patients can directly report adverse drug reactions (ADRs) related to cancer therapies, ensuring their experiences are recorded promptly and accurately (Azaria et al., 2016). Patients maintain ownership of their personal health information, deciding who can access it and under what conditions, thus enhancing privacy and autonomy (Zyskind et al., 2015).

For healthcare providers, researchers, and regulators, blockchain creates a shared, tamper-proof repository of ADR data, facilitating collaboration without compromising data security. This democratization of information promotes active participation from all parties involved, leading to richer pharmacovigilance datasets and more informed decision-making (Kuo et al., 2017). By empowering both patients and stakeholders, blockchain fosters a more inclusive and transparent pharmacovigilance environment that can ultimately lead to improved cancer treatment outcomes and safer healthcare practices.

VI. CHALLENGES OF PHARMACOVIGILANCE INFRASTRUCTURE FOR NATIONAL CANCER REGISTRIES

Implementing an effective pharmacovigilance infrastructure for national cancer registries faces several critical challenges. One major issue is the integration of data from multiple, fragmented sources, which often use different formats and standards, making harmonization difficult (Zhang et al., 2019). Additionally, securing patient privacy while ensuring transparency for stakeholders is a complex balance that traditional systems struggle to maintain. Many existing cancer registries are still paper-based or rely on outdated electronic systems, creating barriers to real-time adverse drug reaction (ADR) monitoring and reporting (Kuo et al., 2017).

Financial and technical constraints also pose significant hurdles, particularly in low- and middle-income countries where healthcare resources are already limited (World Health Organization, 2018). Resistance from stakeholders, due to concerns over data ownership and interoperability, further complicates the development of a unified system. Finally, regulatory frameworks often lag behind technological advancements, making it difficult to implement innovative solutions like blockchain within existing legal structures (Mettler, 2016). These challenges must be carefully addressed to realize a robust, responsive pharmacovigilance infrastructure for cancer care.

➢ *Scalability and Performance Issues*

One of the primary challenges of implementing blockchain-based pharmacovigilance systems in national cancer registries is scalability and performance. As the volume of patient records, adverse drug reaction (ADR) reports, and clinical data grows, the blockchain network must handle an increasing number of transactions without significant latency or high operational costs as represented in figure 6 (Yli-Huumo et al., 2016). Public blockchains, in particular, often face throughput limitations, processing only a limited number of transactions per second, which can delay real-time data access and reporting crucial for pharmacovigilance activities (Croman et al., 2016).

Furthermore, maintaining performance efficiency while ensuring data security and decentralization remains a complex trade-off. Large block sizes and frequent transaction verifications can lead to network congestion and storage burdens for participating nodes (Zyskind et al., 2015). For national cancer registries, which must accommodate diverse data from multiple sources across different regions, these scalability constraints could undermine the effectiveness of blockchain solutions. Overcoming these challenges requires innovative approaches such as off-chain storage, sharding, and optimized consensus mechanisms.

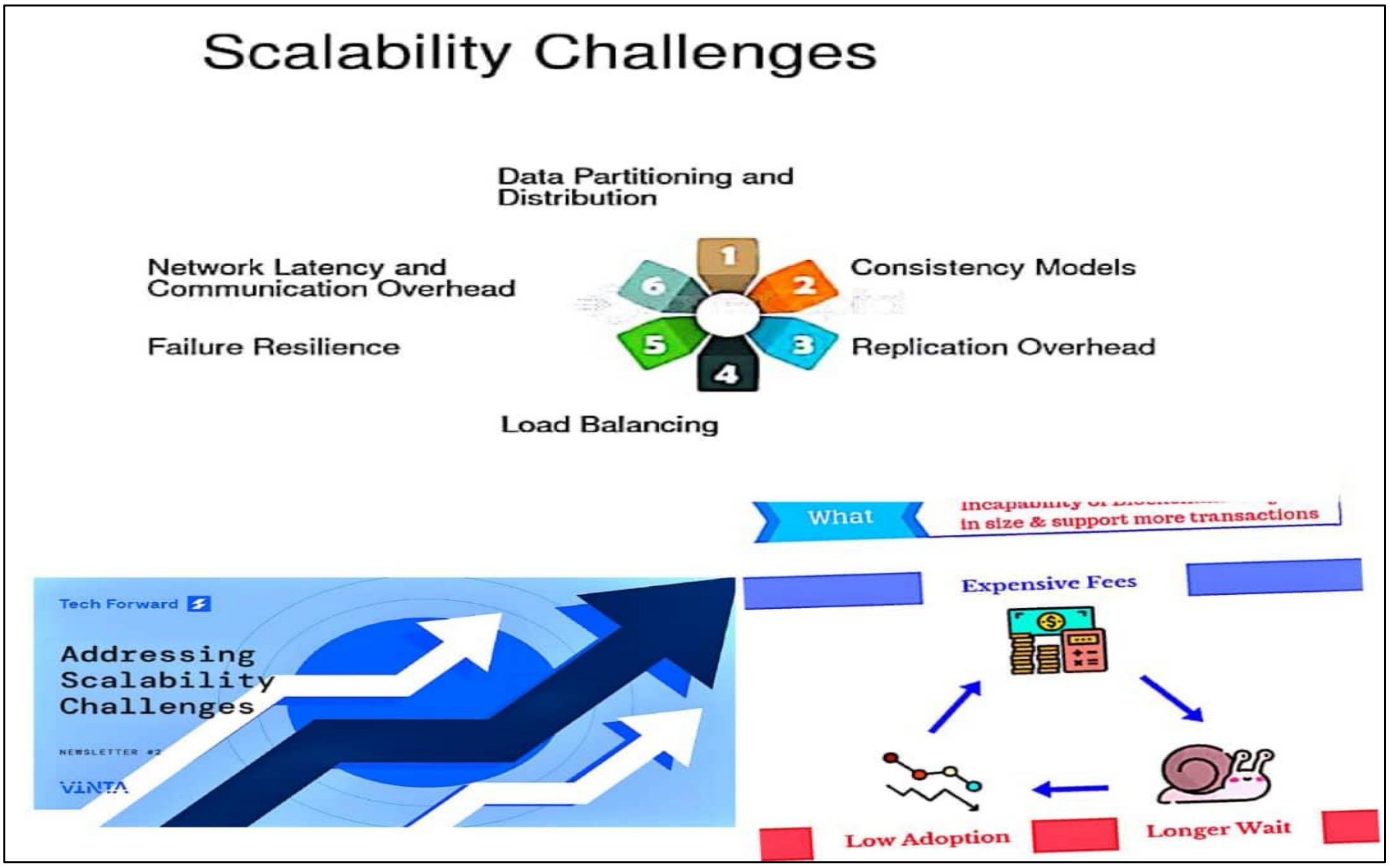

Fig 6 Picture of Scalability and Performance Issues (Yli-Huumo et al., 2016).

Fig 6 Illustrates key scalability challenges in distributed systems, particularly relevant to blockchain and data-intensive infrastructures. These challenges include Data Partitioning and Distribution, which involves splitting data across multiple nodes efficiently; Consistency Models, referring to the trade-offs between data availability and consistency in a distributed setup; and Replication Overhead, which highlights the extra resources needed to duplicate and synchronize data across systems. Load Balancing addresses the even distribution of processing tasks to prevent node overload, while Failure Resilience pertains to the system's ability to recover from node or network failures without data loss. Lastly, Network Latency and Communication Overhead captures the delays and resource costs associated with data transfer between distributed components. Together, these factors present significant technical hurdles when designing scalable and reliable blockchain-enabled infrastructures.

➢ *Regulatory and Legal Considerations*

The integration of blockchain technology into pharmacovigilance systems for national cancer registries faces significant regulatory and legal hurdles. Existing healthcare regulations, such as data protection laws and standards for clinical data handling, were not designed with decentralized technologies in mind (Mettler, 2016). Issues such as data ownership, cross-border data sharing, and the immutability of blockchain records create legal uncertainties, particularly regarding patients' rights to modify or erase their personal data under regulations like the General Data Protection Regulation (GDPR) (Radanović & Likić, 2018).

Moreover, the lack of standardized legal frameworks for blockchain across different jurisdictions poses challenges for establishing interoperable cancer registries at national and international levels. Regulatory bodies have been slow to develop policies that support blockchain's use in sensitive fields like healthcare, leading to a cautious adoption pace (Benchoufi & Ravaud, 2017). To fully leverage blockchain's benefits, clear legal guidelines that address privacy, security, consent, and accountability must be developed and harmonized globally.

➢ *Cost, Adoption, and Technical Barriers*

The cost of implementing blockchain-enabled pharmacovigilance systems presents a major barrier for national cancer registries. Developing the necessary blockchain infrastructure, maintaining nodes, training personnel, and ensuring cybersecurity require significant financial investment (Mettler, 2016). For many healthcare systems, particularly in low- and middle-income countries, these costs can be prohibitive and may deter early adoption efforts. In addition, the technical complexity of blockchain technology poses challenges for healthcare providers who may lack expertise in distributed ledger systems (Kuo et al., 2017).

Adoption barriers are further intensified by resistance to change among stakeholders accustomed to traditional centralized systems. Concerns about interoperability with legacy systems, data migration, and long-term sustainability also hinder widespread acceptance (Yli-Huumo et al., 2016). Without clear demonstration of cost-effectiveness and user-friendly solutions, the adoption curve remains slow. Therefore, to realize the full potential of blockchain in cancer pharmacovigilance, strategies must address technical support, stakeholder education, phased implementation, and economic incentives that encourage investment and participation.

Table 5 Summary of Cost, Adoption, and Technical Barriers

Barrier	Description	Effect on Implementation	Example
High Initial Costs	Setting up blockchain infrastructure requires significant investment.	Limits participation by smaller institutions or developing regions.	Expenses for servers, development, and training.
Resistance to Adoption	Stakeholders may be hesitant to change existing systems and workflows.	Slows down deployment and limits stakeholder engagement.	Hospitals unwilling to shift from centralized databases.
Lack of Technical Expertise	Shortage of professionals skilled in blockchain development and integration.	Hampers proper implementation and system maintenance.	Few IT staff trained in smart contracts or DLT frameworks.
Integration Complexity	Difficulty in linking blockchain with legacy healthcare systems.	Causes delays and increases the risk of data silos.	Incompatibility between EHR systems and blockchain APIs.

VII. CONCLUSION AND FUTURE DIRECTIONS

The integration of blockchain technology into pharmacovigilance for national cancer registries presents a significant step forward in enhancing patient safety, data management, and healthcare transparency. As the healthcare sector continues to embrace digital transformation, blockchain offers a foundation for secure, decentralized, and tamper-proof systems that can effectively address many of the current limitations in pharmacovigilance practices. Its potential to improve adverse drug reaction detection, streamline data sharing, and empower patients makes it a valuable tool for modern cancer registries.

Looking ahead, future efforts should focus on developing scalable blockchain architectures, improving interoperability between legacy systems, and creating supportive legal and regulatory frameworks. Continued investment in research and pilot projects will be necessary to test real-world applications and refine blockchain models for specific healthcare contexts. Collaboration among technologists, healthcare providers, policymakers, and patients will be crucial in overcoming technical and adoption barriers. Ultimately, blockchain-enabled pharmacovigilance infrastructures could become a cornerstone in building safer, more responsive, and patient-centered cancer care systems globally.

➢ *Emerging Trends in Blockchain and Healthcare*

Blockchain is steadily evolving from a niche innovation to a foundational technology in healthcare, with emerging trends reshaping how health data is managed, shared, and protected. One key trend is the integration of blockchain with artificial intelligence and machine learning to enhance predictive analytics and automate adverse drug reaction monitoring. Another development is the rise of decentralized identity systems, giving patients greater control over their medical records and consent management. Interoperable blockchain platforms are also gaining *traction*, enabling secure data exchange across hospitals, research institutions, and national registries. Additionally, blockchain is being explored for secure vaccine distribution, clinical trial transparency, and supply chain integrity. As healthcare systems increasingly prioritize patient-centric care, these trends suggest a future where blockchain empowers individuals, reduces inefficiencies, and supports more responsive public health infrastructure.

➢ *Summary of key findings*

The integration of blockchain technology into pharmacovigilance for national cancer registries presents a transformative opportunity to improve the detection and management of adverse drug reactions (ADRs). By offering enhanced data integrity, transparency, and security, blockchain can address key challenges such as data fragmentation, delayed reporting, and privacy concerns. It enables secure, decentralized data sharing across stakeholders, empowering patients, clinicians, and regulators alike. However, successful implementation requires overcoming barriers related to cost, scalability, and regulatory complexities. As the technology matures, ongoing research, collaboration, and development of standardized frameworks will be essential for optimizing blockchain's potential in healthcare. Ultimately, blockchain could revolutionize cancer pharmacovigilance, ensuring more efficient, secure, and patient-centered systems for monitoring and responding to drug safety concerns.

➢ *Recommendations for Implementation*

For successful implementation of blockchain-enabled pharmacovigilance systems in national cancer registries, a clear, step-by-step approach is essential. First, collaboration among key stakeholders, including healthcare providers, regulatory bodies, and technology developers, is crucial to ensure that the system meets the needs of all parties involved. Pilot projects should be introduced in select regions or institutions to test blockchain's feasibility, refine processes, and build confidence in its use.

Data interoperability is another critical factor. Establishing universal standards for data formats and communication protocols will ensure seamless integration with existing health information systems. Additionally, adequate security measures must be implemented to protect sensitive health data, and smart contracts should be utilized to automate reporting and monitoring processes.

Finally, continuous education and capacity-building initiatives are needed to empower healthcare professionals and stakeholders with the knowledge and skills necessary to effectively operate blockchain systems. This holistic approach will facilitate the successful adoption and long-term sustainability of blockchain in pharmacovigilance.

REFERENCES

[1]. Ardizzoni, A., Tiseo, M., & Boni, L. (2017). Challenges in the Management of Cancer Patients Receiving Checkpoint Inhibitors. Cancer Treatment Reviews, 59, 61–67. https://doi.org/10.1016/j.ctrv.2017.07.003

[2]. Aronson, J. K. (2017). Adverse Drug Reactions: History, Terminology, Classification, Causality, Frequency, Preventability. British Journal of Clinical Pharmacology, 83(4), 795–806. https://doi.org/10.1111/bcp.13112

[3]. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2nd International Conference on Open and Big Data (OBD) (pp. 25–30). IEEE. https://doi.org/10.1109/OBD.2016.11

[4]. Banerjee, P., & Bihani, P. (2019). Challenges and opportunities in pharmacovigilance: perspectives from emerging economies. Therapeutic Advances in Drug Safety, 10, 2042098619862150. https://doi.org/10.1177/2042098619862150

[5]. Benchoufi, M., & Ravaud, P. (2017). Blockchain Technology for Improving Clinical Research Quality. Trials, 18(1), 335. https://doi.org/10.1186/s13063-017-2035-z

[6]. Binns, A., Blake, R., & Tiwari, P. (2019). Blockchain Technology and the Role of Smart Contracts in Enhancing Pharmaceutical Supply Chain Transparency. Journal of Pharmaceutical Innovation, 14(2), 147–158. https://doi.org/10.1007/s12247-018-9320-2

[7]. Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16).

[8]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[9]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[10]. Croman, K., et al. (2016). On Scaling Decentralized Blockchains. International Conference on Financial Cryptography and Data Security, 106–125. https://doi.org/10.1007/978-3-662-53357-4_8

[11]. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

[12]. Edwards, I. R. (2017). A new era for pharmacovigilance? Drug Safety, 40(10), 781–785. https://doi.org/10.1007/s40264-017-0565-5

[13]. Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data. MIT Media Lab.

[14]. Esmaeilzadeh, P. (2019). The Impacts of the GDPR on the Healthcare Industry. Health Policy and Technology, 8(3), 234–244. https://doi.org/10.1016/j.hlpt.2019.04.003

[15]. Evans, R. S. (2016). Electronic Health Records: Then, Now, and in the Future. Yearbook of Medical Informatics, 25(S 01), S48–S61. https://doi.org/10.15265/IYS-2016-s006

[16]. González-González, C., López-Coronado, M., Sánchez-Guerrero, F., & Franco-Martín, M. A. (2013). Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in Healthcare. Journal of Medical Systems, 37(5), 9967. https://doi.org/10.1007/s10916-013-9967-6

[17]. Gonzalez-Gonzalez, C., López-González, E., Herdeiro, M. T., & Figueiras, A. (2018). Strategies to improve adverse drug reaction reporting: a critical and systematic review. Drug Safety, 41(7), 611–621. https://doi.org/10.1007/s40264-018-0650-2

[18]. Hazell, L., & Shakir, S. A. (2006). Under-reporting of adverse drug reactions: a systematic review. Drug Safety, 29(5), 385-396. https://doi.org/10.2165/00002018-200629050-00003

[19]. Hernandez, M., Villaverde, J. E., & Martinez, A. (2018). Leveraging Blockchain and Smart Contracts for Pharma and Healthcare: Improving Adverse Event Management. Journal of Health Informatics, 24(3), 245–258. https://doi.org/10.1016/j.jhi.2018.04.005

[20]. Khozin, S., Blumenthal, G. M., & Pazdur, R. (2017). Real-world Data for Clinical Evidence Generation in Oncology. J Natl Cancer Inst, 109(11), djx187. https://doi.org/10.1093/jnci/djx187

[21]. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

[22]. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

[23]. Mandl, K. D., Lober, W. B., & Jha, A. K. (2018). Interoperability in Healthcare: A Comprehensive Review of Standards and Issues. Journal of

Healthcare Information Management, 32(4), 10–25. https://doi.org/10.1080/21681242.2018.1165153
[24]. Mettler, M. (2016). Blockchain Technology in Healthcare: The Revolution Starts Here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1–3). IEEE. https://doi.org/10.1109/HealthCom.2016.7749510
[25]. Moradian, S., & Howell, D. (2015). Investigating the Need for Data Harmonization in Cancer Registries. Current Oncology, 22(1), 29–33. https://doi.org/10.3747/co.22.2358
[26]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
[27]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
[28]. Nebeker, J. R., Barach, P., & Samore, M. H. (2013). Clarifying Adverse Drug Events: A Clinician's Guide to Terminology, Documentation, and Reporting. Annals of Internal Medicine, 140(10), 795–801. https://doi.org/10.7326/0003-4819-140-10-200405180-00017
[29]. Pacurariu, A., Coloma, P. M., van Haren, A., Genov, G., Sturkenboom, M., & Mol, P. G. (2018). Useful Interventions for Improving Spontaneous ADR Reporting: A Systematic Review. Drug Safety, 37(10), 795–808. https://doi.org/10.1007/s40264-014-0211-y
[30]. Postow, M. A., Sidlow, R., & Hellmann, M. D. (2018). Immune-Related Adverse Events Associated with Immune Checkpoint Blockade. New England Journal of Medicine, 378(2), 158–168. https://doi.org/10.1056/NEJMra1703481
[31]. Radanović, I., & Likić, R. (2018). Opportunities for Use of Blockchain Technology in Medicine. Applied Health Economics and Health Policy, 16(5), 583–590. https://doi.org/10.1007/s40258-018-0412-8
[32]. Shen, C., Guo, J., & Yang, Y. (2019). Blockchain-Based Secure Data Storage and Sharing for Cancer Registries. Computational and Mathematical Methods in Medicine, 2019, Article ID 8274018. https://doi.org/10.1155/2019/8274018
[33]. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.
[34]. World Health Organization. (2002). The Importance of Pharmacovigilance: Safety Monitoring of Medicinal Products. Geneva: WHO.
[35]. World Health Organization. (2018). Cancer Registration: Principles and Methods. International Agency for Research on Cancer.
[36]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477
[37]. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of Medical Systems, 40(10), 218. https://doi.org/10.1007/s10916-016-0574-6
[38]. Zhang, P., & Jacobsen, H.-A. (2018). Towards dependable, scalable, and pervasive distributed ledgers with Blockchains. Future Generation Computer Systems, 92, 475–487. https://doi.org/10.1016/j.future.2018.09.017
[39]. Zhang, R., & Wang, L. (2017). Security Architecture for Healthcare Data in Cloud Computing. Security and Communication Networks, 2017, 1–10. https://doi.org/10.1155/2017/6894045
[40]. Zhang, X., Cheng, W., & Li, L. (2019). Blockchain for Interoperability in Healthcare: Applications and Challenges. Journal of Biomedical Informatics, 95, 103217. https://doi.org/10.1016/j.jbi.2019.103217
[41]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85
[42]. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops, 180–184. https://doi.org/10.1109/SPW.2015.27