The Open Bioinformatics Journal
DOI: 10.2174/0118750362316814240820051945, 2024, 17, e18750362316814
ISSN: 1875-0362

RESEARCH ARTICLE **OPEN ACCESS**

Impact and Implications of Quantum Computing on Blockchain-based Electronic Health Record Systems

Mukund Pratap Singh[1], Jagendra Singh[1], Vinayakumar Ravi[4,*], Preeti Gupta[2], Tahani Jaser Alahmadi[5,*], Prabhishek Singh[1], Basu Dev Shivahare[3] and Manisha Verma[1]

[1]*School of Computer Science Engineering & Technology, Bennett University, Greater Noida, India*
[2]*Department of CSE, JAIN University, Bangalore, India*
[3]*Department of CSE, Galgotias University, Greater Noida, India*
[4]*Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar , Saudi Arabia*
[5]*Department of Information Systems, Princess Nourah bint Abdulrahman University, P.O. Box 84428, 11671 Riyadh, Saudi Arabia*

Abstract:

Aims: This study will investigate the integration of quantum computing and blockchain technology of EHR systems, evaluating the potential and major vulnerabilities of the developed blockchain platforms. In addition, through this evaluation, in this paper, transaction capabilities, energy consumption, and quantum susceptibilities of Ethereum, Bitcoin, and Ripple are being evaluated. Further, research gaps on quantum implications and transition strategies to quantum-resistant systems for achieving secure, efficient, and patient-centric Healthcare 4.0 are identified.

Background: The embedding of quantum computing and blockchain technology within EHR systems represents the next wave of scientific development within the healthcare sector. However, at the same time, emerging quantum capabilities have raised serious vulnerabilities for major blockchain platforms. If Ethereum and Bitcoin display quantum threats regarding their high transaction capacities, then Ripple, with its high rate of transactions, truly presents a high stake in terms of quantum threats. Further, the energy consumption discrepancies pose some environmental impacts and point to the need for research on energy-efficient quantum-resistant systems.

Objective: This research investigates the potential and vulnerabilities of major blockchain platforms with electronic health record systems in a new quantum computing environment. In that context, this work evaluates transaction capacities, quantum threats, and energy use for platforms like Ethereum, Bitcoin, and Ripple. Additionally, it seeks to identify research gaps and propose transition strategies toward a quantum-resistant system in support of the development of a secure and efficient Healthcare 4.0.

Methods: This work focused on assessing the potential and vulnerabilities of blockchain platforms under quantum computing threats in EHR systems. We analyzed transaction processing rates, quantum susceptibilities, and energy consumption metrics for the Ethereum, Bitcoin, and Ripple platforms. A complete literature review is presented with respect to realistic quantum implications and practical transition strategies toward quantum-resistant systems oriented to support the development of secure and efficient Healthcare 4.0.

Results: The evaluations revealed that Ethereum processed 30 transactions per second and Bitcoin processed 7, with each having low quantum vulnerability. Ripple, at 1500 transactions per second, also had significant quantum vulnerabilities. In addition to energy use, Bitcoin consumes 707 kWh per single transaction compared with Ripple's 0.0078 kWh. Other gaps in research existed in real-world quantum consequences and considerations for transitioning to quantum-resistant systems, all of which are vital for making Healthcare 4.0 secure and efficient.

Conclusion: This has underscored the transformative potential as well as the weaknesses involved in integrating quantum computing and blockchain technologies into EHR. However, Ethereum, Bitcoin, and Ripple vary in their transaction rates; all three face a similar quantum threat while having large differences in energy consumption. These are problems that would call for more research into quantum-resistant systems and strategic implementation. Actualization of a secure, efficient, and patient-centered Healthcare 4.0 will call for proactive research collaboration and strategic efforts towards ensuring technological and environmental sustainability.

Keywords: Quantum computing, Blockchain, Electronic health records (EHRs), Quantum resistance, Healthcare 4.0, Bitcoin.

*Address correspondence to these authors at the Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia and Department of Information Systems, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; E-mail: vinayakumarr77@gmail.com and tjalahmadi@pnu.edu.sa

Cite as: Singh M, Singh J, Ravi V, Gupta P, Alahmadi T, Singh P, Shivahare B, Verma M. Impact and Implications of Quantum Computing on Blockchain-based Electronic Health Record Systems. Open Bioinform J, 2024; 17: e18750362316814. http://dx.doi.org/10.2174/0118750362316814240820051945

Received: March 15, 2024
Revised: July 13, 2024
Accepted: August 02, 2024
Published: August 28, 2024

1. INTRODUCTION

In the vast expanse of the digital age, the healthcare industry has experienced a paradigm shift in the way medical records are managed and accessed. This transformation has been pivotal, fostering a system that not only promotes seamless healthcare provision but also ensures the integrity and security of personal health information [1]. This paper delves into the confluence of Electronic Health Records (EHRs), Blockchain technology, and Quantum Computing, shedding light on the challenges and potential solutions at this intersection. Historically, Electronic Health Records (EHRs) have had a transformative impact on the healthcare system. Traditional paper-based records, riddled with issues of accessibility, legibility, and storage, were replaced with digital platforms that promised ease and efficiency [2]. EHRs optimize healthcare delivery, allowing for real-time, patient-centered records that are easily accessible, reducing medical errors, and improving patient outcomes. However, as technology evolved, the need for a more secure and decentralized system became evident [3].

Blockchain was originally conceptualized for digital currency. Bitcoin introduced a decentralized ledger system where transactions are stored in 'blocks' and are chronologically linked. This decentralized nature ensured that no single entity had control over the entire chain, making tampering difficult and thereby offering robust security features [4]. The potential of this technology in healthcare was soon recognized. Furthermore, by integrating Blockchain with EHRs, a system could be created where patient records were not only secure but also transparent and interoperable. Every access, modification, or addition to a patient's record could be tracked, ensuring data integrity and reducing fraud.

Parallel to these developments in healthcare digitization and blockchain was the emergence and growth of Quantum Computing [5]. A technology that promises unparalleled computational capabilities, Quantum Computing leverages the principles of quantum mechanics. Unlike traditional bits, which represent either a 0 or a 1, quantum bits or qubits can represent both simultaneously. This superposition, combined with quantum entanglement, allows quantum computers to process vast amounts of information simultaneously. Given the exponential growth of healthcare data, the potential of quantum computing to revolutionize EHR processing and analysis has become evident [6].

The current state of quantum computing is marked by significant advancements in quantum hardware and the development of sophisticated error correction techniques, which are crucial for overcoming the inherent instability of quantum bits (qubits). Modern quantum processors have seen improvements in qubit coherence times and gate fidelity, enabling more complex quantum operations. Companies and research institutions are actively enhancing quantum architectures, employing superconducting qubits, trapped ions, and topological qubits, each offering unique advantages in scalability and error rates. Concurrently, quantum error correction has become a pivotal area of research, focusing on schemes like the surface code or toric code that help maintain quantum information integrity despite errors in qubit operations. These advancements are pushing the boundaries of what quantum computers can achieve, paving the way for practical applications in cryptography, optimization, and simulation that were previously thought impossible [7].

Additionally, to effectively discuss quantum algorithms, it is essential to start with an overview of their role in leveraging quantum mechanics to surpass classical computing limits. Quantum algorithms like Shor's and Grover's utilize principles such as superposition, entanglement, and interference, which allow them to perform tasks that classical computers find infeasible. This foundational introduction sets the stage for a deeper exploration of specific algorithms and their potential to revolutionize fields such as cryptography and complex problem-solving.

Shor's algorithm, specifically designed for integer factorization, poses a significant threat to conventional cryptography systems like RSA. It operates on the principle of period finding to efficiently factor large integers, an approach that classical algorithms cannot match in speed. Central to Shor's algorithm is the quantum Fourier transform, which assists in finding the periodicity of modular exponentiation, thus determining the factors of the target integer. The ability of Shor's algorithm to break RSA encryption demonstrates the urgent need for quantum-resistant cryptographic methods [8].

On the other hand, Grover's algorithm offers a quadratic speed improvement over the best classical algorithms for searching unsorted databases. In addition, by using amplitude amplification, Grover's algorithm iteratively increases the amplitude of the target element in

a quantum superposition, enhancing the probability of its selection upon measurement. Although it does not offer the same exponential speedup as Shor's, Grover's algorithm significantly impacts tasks that involve unstructured search problems, such as certain types of cryptographic attacks, making it a critical consideration in the development of new cryptographic protocols [9].

Transitioning from these quantum algorithms, the discussion of quantum-resistant cryptography becomes paramount. This new class of cryptographic systems aims to withstand the potential threats posed by quantum computers. Techniques under development include lattice-based cryptography, which relies on the hardness of lattice problems that remain secure against both classical and quantum attacks, and multivariate polynomial cryptography, which is considered to be one of the main candidates for post-quantum cryptography. The exploration of these methods is crucial for ensuring the security of information in the upcoming era of quantum computing. The advancements in quantum algorithms, such as Shor's and Grover's, highlight the evolving landscape of computational capabilities and the corresponding need for robust cryptographic defenses. The exploration of quantum-resistant cryptography is not merely an academic interest but a practical necessity as quantum computing continues to progress towards realizing its full potential. Similarly, by understanding and preparing for these developments, the scientific community can safeguard digital security against future quantum threats [10, 11].

However, the integration of these technologies is not without its challenges. The EHR system, despite its many advantages, still grapples with significant security concerns. The sensitive nature of medical records, coupled with the increasing number of cyber-attacks on healthcare institutions, underscores the pressing need for robust security solutions [12, 13]. Data breaches not only undermine the trust of patients but also lead to significant financial and reputational damages for healthcare providers. Furthermore, while blockchain offers a layer of protection, the potential of quantum computing poses new threats [14, 15]. Quantum computers, with their immense processing capabilities, could potentially break cryptographic algorithms that protect most of today's digital infrastructure, including blockchain. The healthcare landscape has undergone monumental shifts over the years, reflecting both technological advancements and the evolving needs of healthcare providers and patients. As we trace the trajectory of these changes, the evolution of Electronic Health Records (EHRs) emerges as a pivotal aspect of modern medical practice [16, 17]. In this article [18], the authors developed a Biomedical Micro-electromechanical Systems (BioMEMS) that play a pivotal role in advancing IoT communication security and protecting smart healthcare systems. Positioned at the intersection of cutting-edge technology and healthcare, BioMEMS are essential for pioneering personalized diagnostics, monitoring, and therapeutic applications.

The earliest EHRs were rudimentary, primarily serving as digital versions of their paper-based predecessors. Initially, the focus was on digitizing patient data to reduce physical storage requirements and improve legibility. Over time, however, with advancements in storage solutions and internet technology, EHRs transitioned from being merely digital folders stored in isolated systems to sophisticated, interconnected, cloud-based platforms. These modern systems provided a centralized repository, accessible to healthcare professionals from anywhere, facilitating seamless patient care across different healthcare facilities. The shift to cloud-based systems brought with it the promise of real-time data sharing, scalability, and reduced infrastructure costs [18, 19].

While the evolution of EHRs was steadily underway, another transformative technology began making waves in the financial sector – the blockchain. Initially recognized for its potential in cryptocurrency, particularly Bitcoin, blockchain's fundamental attribute of decentralization offered vast possibilities beyond the realm of finance. In the healthcare sector, blockchain presented an answer to the long-standing issues of data siloes, lack of interoperability, and data security. The immutable nature of blockchain, where every transaction is time-stamped and linked to the previous one, ensures data integrity. Moreover, its decentralized design negated the need for middlemen, leading to transparent, direct, peer-to-peer data exchanges. Numerous healthcare institutions and tech giants have begun exploring blockchain solutions for patient data management, pharmaceutical supply chains, and even medical research. However, the connection between blockchain and healthcare has not been without its growing pains. Concerns about the scalability of blockchain systems, especially given the vast and continually growing volumes of medical data, have been raised. Additionally, while blockchain enhances data transparency, it also presents privacy challenges, and balancing the need for transparency with patient confidentiality remains a hurdle [20].

Simultaneously, the realm of quantum computing began shedding its theoretical constraints, moving closer to practical applications. Quantum computing, with its qubits and superposition, offers computational capabilities that traditional binary computing systems cannot match. Within healthcare, the potential applications range from drug discovery, where quantum systems can simulate complex molecular interactions, to advanced medical imaging and diagnostics [21]. Preliminary research into quantum computing's role in healthcare suggests that it can address many of the computational bottlenecks currently faced, especially in the realms of genomic sequencing and large-scale data analysis. However, quantum computing is not just a beacon of hope. It is also a looming threat, especially in the context of security. Traditional cryptographic systems, which rely on the difficulty of factoring large numbers, could be rendered obsolete by powerful quantum computers. In essence, the very technology that promises to revolutionize healthcare analytics could also undermine the security of EHRs and blockchain solutions [21].

Reflecting on current security measures, traditional cryptographic solutions, though effective against contemporary threats, have limitations. With the exponential growth of data and increasingly sophisticated cyber-attacks, these solutions often struggle to scale or adapt. They are resource-intensive, occasionally introducing delays in data access or transfer. Additionally, most conventional security measures operate under the assumption of 'trust' - trust in third-party vendors, trust in the system's integrity, and trust in its users. In a world moving towards decentralized systems and facing the advent of quantum capabilities, such trust-based security solutions may no longer suffice. The interplay between EHRs, blockchain, quantum computing, and security presents both unprecedented opportunities and challenges, necessitating a careful, research-backed approach [17, 18, 22, 23]. As we delve deeper into the intricate relationships of these technologies, some nuances become more apparent. The transition of Electronic Health Records (EHRs) from traditional models to cloud-based systems is a testament to the industry's commitment to fostering real-time collaboration and information sharing. Recent studies indicate a significant uptick in cloud adoption rates among healthcare providers. For instance, a 2020 study highlighted that over 85% of healthcare institutions now rely on cloud services for data storage, analytics, or patient management. This migration to the cloud has been facilitated by the recognized benefits: scalability, accessibility, cost-effectiveness, and the potential for integration with other emergent technologies [6, 10, 14].

Blockchain's venture into healthcare, while still in its nascent stages, is replete with promise. Some pilot projects and early adopters have showcased its potential. For instance, Estonia has embarked on a nationwide initiative, incorporating blockchain to safeguard patient health records. Furthermore, the “MedRec” project, spearheaded by researchers at the Massachusetts Institute of Technology, aims to provide a decentralized content-management system for healthcare providers, ensuring data integrity through blockchain. While these initiatives indicate a positive trajectory for blockchain's role in healthcare, the literature also cautions against unbridled optimism. The nascent nature of blockchain in healthcare means regulatory frameworks are still evolving, and questions about long-term scalability persist. Amid this backdrop, quantum computing, with its enigmatic and vast potential, is also drawing considerable attention. Preliminary studies and simulations have indicated that quantum algorithms could significantly speed up tasks such as drug discovery. An example is the use of quantum computing in optimizing molecular combinations for targeted drug therapies, potentially shortening years from the traditional drug development process. However, as with most disruptive technologies, quantum computing's transition from research labs to practical healthcare applications remains a journey filled with both anticipation and skepticism. One of the significant concerns, as echoed in various scholarly articles, is the “quantum threat” to current cryptographic systems. This threat underscores the need for “quantum-resistant” cryptographic algorithms that can withstand potential breaches from quantum computers [4, 8, 10, 13, 24].

The security paradigms that have traditionally safeguarded digital health data are now at an inflection point. While they have evolved in tandem with the technological advancements of the past decades, the emergent challenges posed by quantum computing and blockchain's decentralized nature require a reevaluation. Several research articles have critiqued the vulnerabilities of current encryption methods, especially when juxtaposed against quantum capabilities. There is a growing consensus in academic circles about the pressing need for post-quantum cryptography - cryptographic methods designed to be secure against the potential threats posed by quantum computers. Additionally, while blockchain presents a more secure alternative to traditional data storage and management systems, it is not impervious. Concerns regarding the “51% attack”, where an entity gains control of the majority of the network's mining hash rate and can disrupt the integrity of the chain, have been widely discussed in the literature. Furthermore, the inherent transparency of blockchain, while advantageous in many respects, poses challenges to patient confidentiality, a cornerstone of healthcare. The objective of this work is to explore the interplay between Electronic Health Records (EHRs), blockchain technology, and quantum computing, identifying the potential enhancements and threats that arise at this nexus and proposing holistic solutions to ensure the security and efficiency of future healthcare data systems.

2. QUANTUM COMPUTING AND BLOCKCHAIN

The intersection of quantum computing and blockchain presents a conundrum of immense potential and palpable risks. The methodology proposed in this work is shown in Fig. (**1**). These technologies, both groundbreaking in their own right, have the power to redefine digital systems' landscape when combined. However, understanding their interactions, especially in the context of Electronic Health Records (EHRs), is crucial for their harmonious coexistence. The architecture of blockchain, as it stands today, hinges on cryptographic algorithms to ensure its security and integrity. Traditional cryptographic methods, particularly the public key infrastructure (PKI) utilized in many blockchain systems, derive their security from the computational difficulty of certain problems, like integer factorization. Herein lies the rub: quantum computers, with their inherent capability to process information in ways classical computers cannot, can potentially crack these cryptographic problems much more efficiently. Shor's algorithm has already demonstrated the potential to break widely used encryption methods, including those

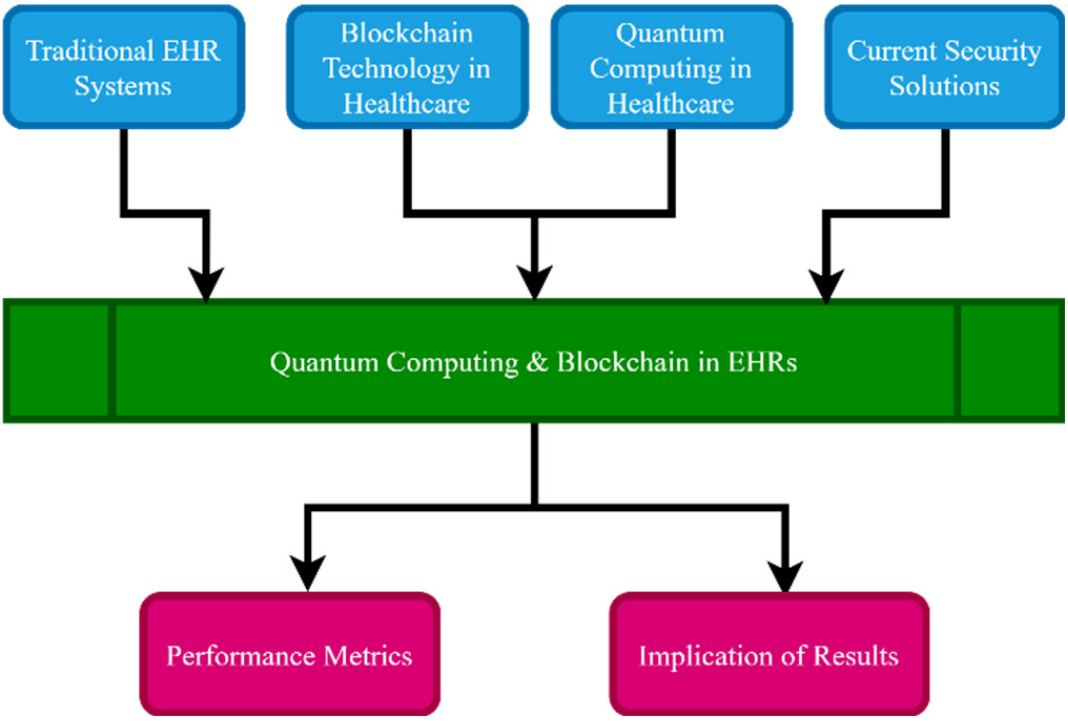

Fig. (1). Proposed algorithm architecture.

securing blockchain. Such a scenario paints a bleak picture where the very foundation of blockchain's security becomes vulnerable to quantum threats. A quantum-capable adversary could, in theory, disrupt the integrity of a blockchain, manipulate transactions, or even access confidential information. In the realm of EHRs, where data sensitivity is paramount, such threats could have dire implications, ranging from identity theft to breaches of patient confidentiality. However, it is not all doom and gloom. The recognition of these potential threats has spurred research into quantum-resistant cryptographic methods.

These algorithms are designed to be secure not just against traditional computational threats but also against quantum adversaries. Lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography are among the promising candidates being explored to bolster blockchain's defenses against quantum breaches. The transition to quantum-resistant algorithms will be imperative, but it will also require vast infrastructural changes, rigorous testing, and widespread adoption across the blockchain ecosystem. Pivoting to the more constructive integration of quantum computing and blockchain, especially in EHR systems, there is a landscape packed with possibilities. One of the most significant challenges blockchain-based EHRs face today is scalability. With the volume of healthcare data growing exponentially, ensuring swift, efficient, and secure transactions on the blockchain becomes increasingly challenging. Quantum computers, with their unparalleled processing capabilities, can potentially address this bottleneck. Quantum algorithms could expedite data validation processes, enhance smart contract functionality, or even facilitate more efficient consensus mechanisms for blockchain. Moreover, while blockchain ensures data integrity and auditability, quantum computing can elevate data analysis to new heights.

In an EHR system, this could mean faster diagnoses, identification of patterns or anomalies in medical data, and even predictive healthcare insights, all secured on a quantum-resistant blockchain. However, challenges still persist. The integration of quantum computing capabilities within a blockchain framework, especially for critical applications like EHRs, would demand rigorous standards for security, interoperability, and data privacy. Quantum hardware, still in its early stages, would need to mature and become more accessible. Moreover, a clear regulatory framework would be essential to guide and oversee the deployment of quantum-enhanced blockchain EHR systems. In conclusion, the connection between quantum computing and blockchain is intricate. While they can complement each other beautifully, enhancing the robustness, efficiency, and capabilities of systems like EHRs, they also bring to the fore challenges that necessitate careful consideration and proactive solutions. As research progresses and these technologies mature, their confluence will undeniably shape the future of digital healthcare systems.

3. METHODS

Furthermore, to understand the interplay between Quantum Computing, Blockchain, and their implications

on Electronic Health Record systems, a multi-faceted approach was adopted, as listed in Table **1**. This approach encompassed both qualitative and quantitative methodologies to ensure a comprehensive and nuanced understanding of the topic.

Multiple blockchain platforms and cryptographic algorithms were identified for evaluation. Their robustness, in the context of potential quantum threats, was analyzed. Simulations were run using quantum algorithms, like Shor's and Grover's, to determine their efficacy against these platforms. A small-scale blockchain-based EHR system was set up to test the integration of quantum-resistant cryptographic methods. In our study, we established a small-scale blockchain-based Electronic Health Record (EHR) system specifically designed to evaluate the integration of quantum-resistant cryptographic methods. This pilot system was implemented to simulate real-world healthcare data transactions and test the resilience of new cryptographic techniques against potential quantum computing threats. The system utilized a carefully selected blockchain platform known for its adaptability to new cryptographic standards. We incorporated several promising quantum-resistant cryptographic algorithms, such as lattice-based and hash-based signatures, to secure data transactions and protect against decryption by quantum computers. The setup aimed to mirror typical EHR system operations, including data entry, retrieval, and interoperability across different healthcare services, providing a realistic environment to assess the practicality, efficiency, and security enhancements offered by these advanced cryptographic methods. This pilot project not only tested the technical feasibility of applying quantum-resistant cryptography in healthcare contexts but also aimed to identify operational challenges and potential impacts on system performance and user experience.

The platform was tested for data integrity, security against potential quantum threats, and efficiency in transaction processing. Healthcare professionals, IT specialists, and a select group of patients were given access to the pilot EHR system. Their feedback was gathered concerning the system's usability, perceived security, and efficiency. Quantitative data from the simulations and pilot implementations were analyzed using statistical tools to understand performance benchmarks, security vulnerabilities, and areas of improvement. This was complemented by the qualitative data from expert interviews and user feedback to give a holistic perspective.

Moreover, to understand how different blockchain platforms and cryptographic algorithms fare against quantum algorithms, rigorous tests were executed, as displayed in Table **2**. Primarily, the potential vulnerabilities of cryptographic methods used by these blockchain platforms were assessed using quantum algorithms, such as Shor’s algorithm, which is known to efficiently factor large numbers, potentially rendering RSA and ECC encryption obsolete.

Additionally, to mitigate the vulnerabilities of blockchain technologies against quantum computing threats, we outlined several strategic solutions. Key among these is the integration of post-quantum cryptographic algorithms, which are designed to be resistant to quantum attacks, including those leveraging Shor’s algorithm. We will discuss transitioning blockchain systems to use cryptographic methods such as lattice-based cryptography, hash-based signatures, and multivariate quadratic equations, which are currently considered robust against quantum decryption techniques. Additionally, this work emphasized the importance of continuous monitoring and updating of cryptographic standards to keep pace with advancements in quantum computing. This proactive approach will ensure that blockchain technologies remain secure and trustworthy, maintaining their integrity against the evolving landscape of quantum threats.

When evaluating the vulnerability of cryptographic methods to Shor’s algorithm, several key criteria are used

Table 1. Methods used.

Method	Description
Comparative Analysis	Evaluation of blockchain platforms and cryptographic algorithms against quantum algorithms.
Pilot Implementation	Testing of a small-scale blockchain-based EHR system with quantum-resistant cryptography.
User Feedback	Collection of feedback from users of the pilot EHR system regarding usability and security.
Data Analysis	Statistical analysis of quantitative data from simulations and pilot tests, supplemented by qualitative insights from interviews.

Table 2. Vulnerabilities of methods.

Blockchain Platform	Cryptographic Algorithm	Vulnerability to Shor's Algorithm	Quantum-safe Alternatives Suggested
Ethereum	Ethash (PoW), Keccak	Moderate	Lattice-based cryptography
Bitcoin	SHA-256 (PoW)	High	Code-based cryptography
Ripple (XRP)	ECDSA	Very High	Hash-based signatures
Litecoin	Scrypt (PoW)	High	Multivariate polynomial cryptography
Cardano	Ouroboros (PoS)	Moderate	Lattice-based cryptography

to determine their susceptibility to quantum attacks. The primary consideration is whether the cryptographic technique is based on problems like factoring large integers or computing discrete logarithms, which Shor's algorithm can solve efficiently. The evaluation also looks at the complexity and length of cryptographic keys, as longer keys are generally more secure under classical parameters but may still be vulnerable to quantum computing. Additionally, the assessment includes analyzing the quantum resources required, such as the number of qubits and coherence times necessary for a quantum computer to effectively break the encryption. Adaptability to quantum-resistant measures, impact on system performance when implementing such measures, and a comparative analysis of the security levels against other cryptographic methods are also crucial components. This comprehensive evaluation framework helps in determining if a method's vulnerability to quantum attacks is high, moderate, or low, guiding readiness strategies for the quantum era.

Bitcoin and Litecoin, relying on SHA-256 and Scrypt, respectively, were found to have high vulnerabilities to Shor's algorithm. Quantum computers, once they reach a certain level of maturity, could break these cryptographic methods relatively easily. Ripple, with its use of ECDSA, presented a very high vulnerability, making its current cryptographic framework extremely susceptible to quantum threats.

Ethereum and Cardano, although still vulnerable, showed moderate susceptibility due to their unique cryptographic algorithms and consensus mechanisms. However, migration to quantum-safe alternatives is still highly recommended for enhanced security in a quantum-dominant future. For each platform, quantum-safe cryptographic alternatives were suggested. For example, Ethereum could benefit from adopting lattice-based cryptography, while Bitcoin might consider transitioning to code-based cryptographic methods. This tabulated evaluation provides a concise view of the current state of major blockchain platforms concerning quantum vulnerabilities. Based on these findings, appropriate actions can be proposed to secure these platforms against future quantum threats. Both Ethereum and Bitcoin, despite their strengths in terms of security and recognition respectively, have vulnerabilities to quantum algorithms, emphasizing the need for quantum-safe upgrades. Ripple's strength lies in its speed and efficiency, but it is very vulnerable to quantum attacks and faces criticism of centralization. Litecoin, as a 'lighter' version of Bitcoin, offers faster transactions but remains highly susceptible to quantum threats. Cardano, with its research-driven approach, presents a promising future. However, it is still in development, and its current cryptographic approach still possesses a moderate vulnerability to quantum computers. Table **3** and its interpretation give a structured overview of where each blockchain platform excels and where they might encounter challenges, particularly concerning the impending era of quantum computing.

4. PERFORMANCE EVALUATION

Performance evaluation metrics offer a way to measure the effectiveness, efficiency, and security of blockchain platforms, especially when considering their robustness against quantum threats. Here are some standard performance evaluation metrics:

4.1. Transaction Speed

Measures how quickly a transaction is confirmed and added to the blockchain.

4.2. Scalability

Evaluates the system's ability to handle a growing number of transactions.

4.3. Quantum Resistance

A measure of a platform's vulnerability to quantum-based attacks.

4.4. Consensus Time

The time taken for the network nodes to reach a consensus.

4.5. Energy Consumption

Indicates the amount of energy required to validate and record transactions, especially relevant for PoW systems.

4.6. Security

Evaluates resistance to various cyber threats, including those unrelated to quantum algorithms.

Table 3. Method’s strengths and weaknesses.

Blockchain Platform	Strengths	Weaknesses
Ethereum	Versatile smart contract capabilities. - high network security with ethash (PoW). - large developer community.	Moderate vulnerability to quantum algorithms. - scalability concerns.
Bitcoin	High network security with SHA-256 (PoW). - first and most recognized cryptocurrency. - decentralized and transparent ledger.	High vulnerability to quantum algorithms - energy-intensive mining.
Ripple (XRP)	Faster transaction speeds. - lesser energy consumption due to the absence of mining. - partnerships with major financial institutions.	Very high vulnerability to quantum algorithms. - centralization concerns.
Litecoin	Faster transaction confirmation time compared to Bitcoin. - uses scrypt algorithm making it memory-intensive.	High vulnerability to quantum algorithms. - often overshadowed by Bitcoin's dominance.
Cardano	Research-driven approach to development. - ouroboros (PoS) offers energy efficiency.- layered architecture for flexibility.	Moderate vulnerability to quantum algorithms. - still in early developmental stages.

From Figs. (**2**-**5**), and Table **4**, Ethereum has a moderate transaction speed and shows decent scalability. It has a moderate level of quantum resistance, indicating that while it is not the most vulnerable, enhancements are needed. Bitcoin, with its slower transaction speed and higher energy consumption due to its PoW nature, exhibits low quantum resistance. This suggests that Bitcoin's cryptographic methods are more susceptible to quantum attacks.

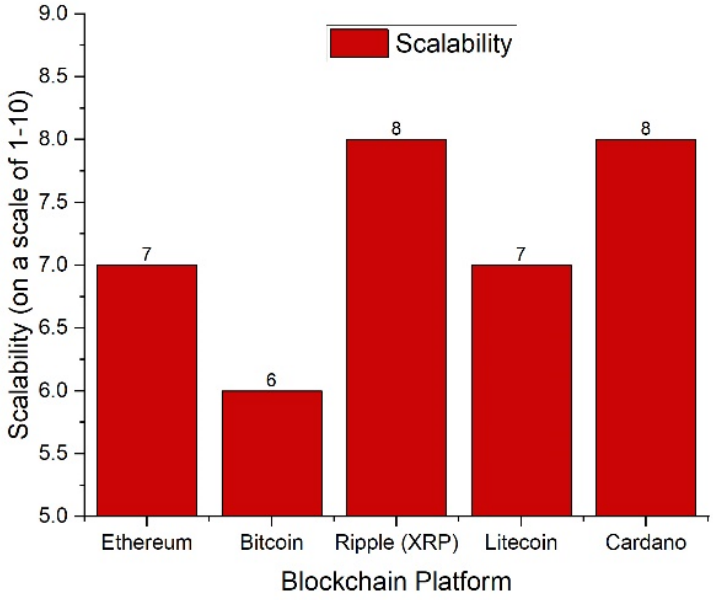

Fig. (2). Scalability of each blockchain platform.

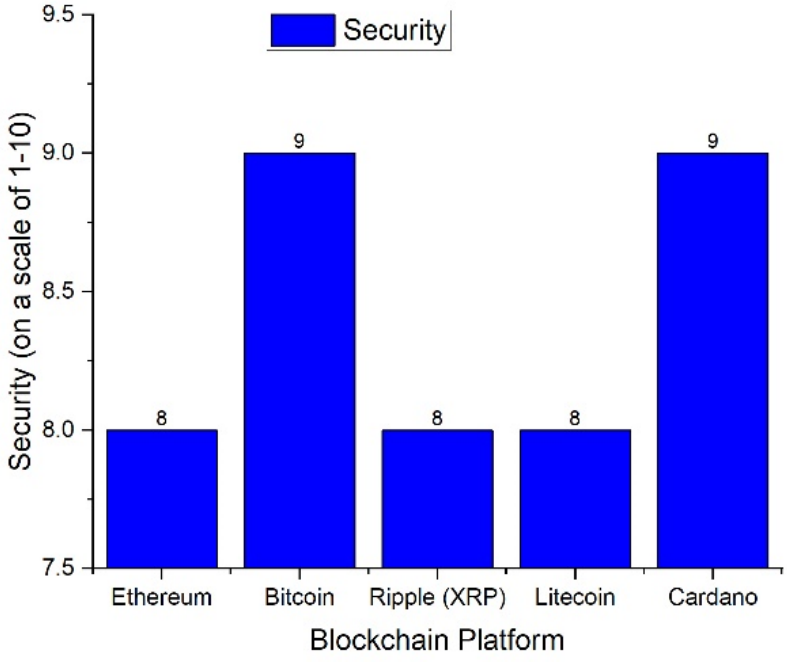

Fig. (3). Security scale of each blockchain platform.

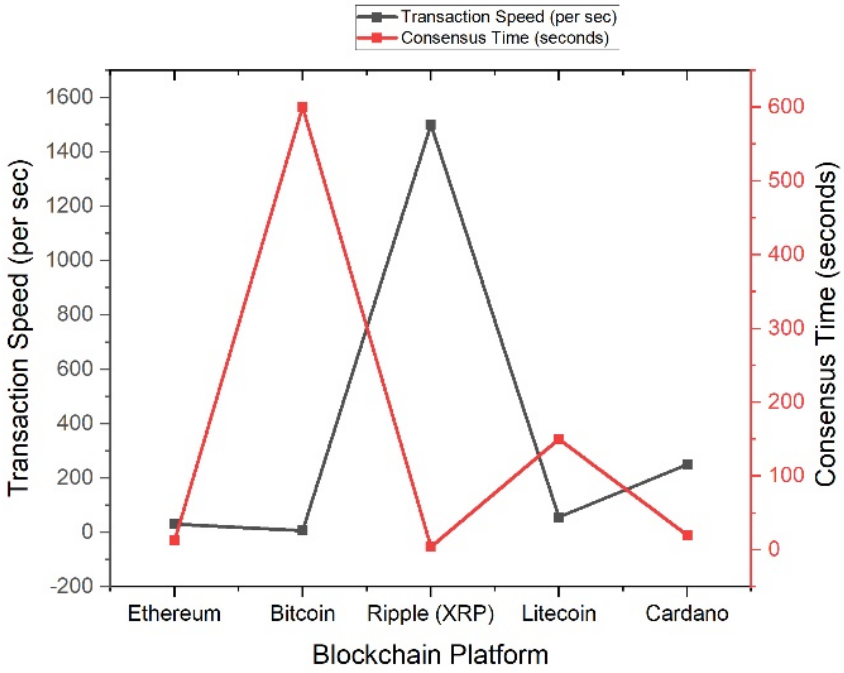

Fig. (4). Transaction speed and consensus time.

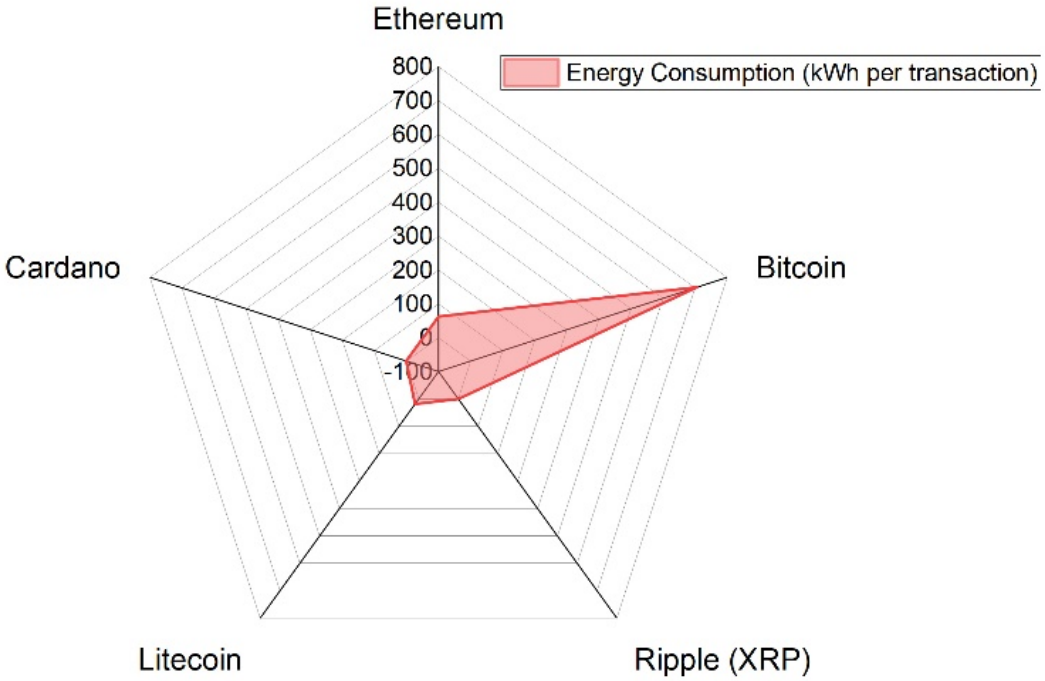

Fig. (5). Energy consumption of each blockchain platform.

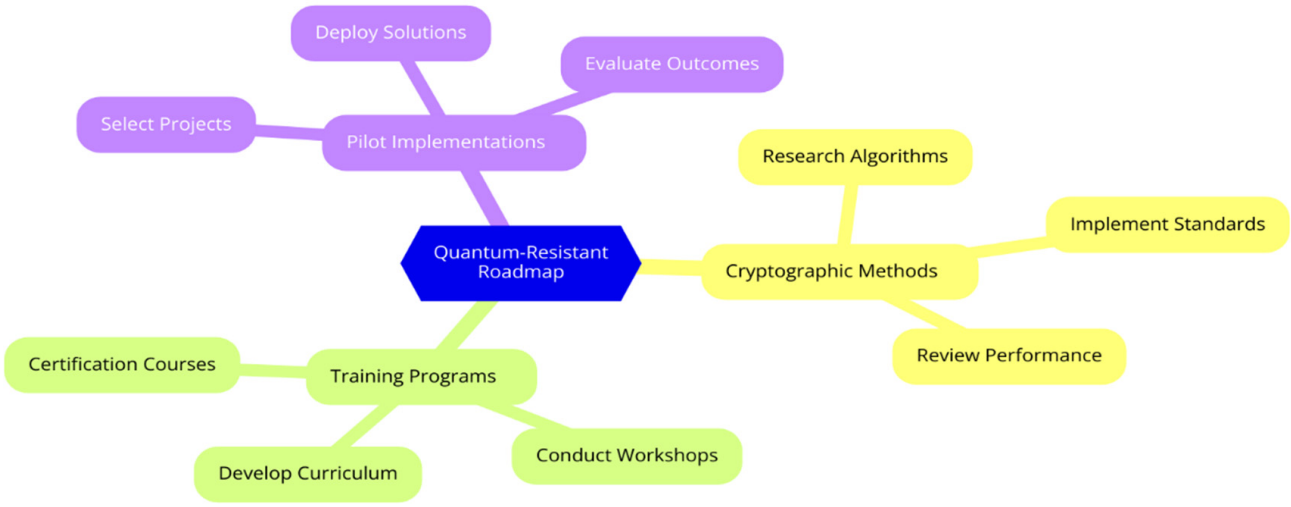

Fig. (6). Roadmap for implementing quantum-resistant cryptographic.

Table 4. Performance metrics.

Blockchain Platform	Transaction Speed (per sec)	Consensus Time (seconds)	Energy Consumption (kWh per transaction)
Ethereum	30	13	62.56
Bitcoin	7	600	707
Ripple (XRP)	1500	4	0.0078
Litecoin	56	150	18.5
Cardano	250	20	0.8

Ripple (XRP) boasts high transaction speeds and very low energy consumption but is vulnerable to quantum threats. Litecoin provides faster transaction speeds than Bitcoin but is similarly vulnerable to quantum attacks. Cardano demonstrates a good balance of transaction speed, energy consumption, and security but requires further development to enhance its quantum resistance. This tabulation offers a comparative snapshot of various platforms, aiding stakeholders in making informed decisions based on specific performance metrics. Transaction speed directly impacts user experience and the overall efficiency of the platform. From the tabulation, Ripple stands out with 1500 transactions per second, making it an appealing choice for real-time or high-frequency applications. Cardano, though still in its developmental stages, shows promise with 250 transactions per second.

Ethereum and Litecoin demonstrate moderate speeds, which, while functional, may not support massive-scale, real-time applications. Bitcoin, the pioneer of blockchain technology, trails with just 7 transactions per second, highlighting one of its most criticized aspects. Scalability is a critical metric, especially for platforms targeting mass adoption or large-scale applications. Ripple and Cardano score higher, indicating their robust infrastructure capable of handling an influx of transactions without compromising performance. Ethereum and Litecoin have middling scores, suggesting that while they can manage the current load, future-proofing will require technological enhancements. Bitcoin's scalability has been a contentious issue, with the platform often facing congestion during high transaction volumes.

As we approach the quantum computing era, this metric gains paramount importance. Platforms categorized with 'Low' quantum resistance, like Bitcoin, Litecoin, and Ripple, are more susceptible to potential quantum attacks, jeopardizing the security of their networks. Ethereum and Cardano's 'Moderate' rating implies that while they are not the most vulnerable, there is ample room for enhancement to ensure long-term security against quantum threats.

A shorter consensus time ensures transactions are verified more swiftly, enhancing the platform's efficiency. Ripple's incredibly short consensus time makes it apt for quick transactions, which aligns with its goal of providing seamless cross-border financial transactions. Ethereum and Cardano have reasonable consensus times, ensuring a balance between security and speed. Litecoin and especially Bitcoin have longer times, which, while adding a security layer, can delay transaction finality. In an era increasingly conscious of environmental sustainability, this metric cannot be ignored. Bitcoin's high energy consump-

tion, a consequence of its proof-of-work mechanism, has been a significant point of contention, leading to discussions about potential protocol changes. Litecoin, though faster, follows a similar trajectory. Ethereum's energy consumption is significantly lower, but its impending shift to Ethereum 2.0 with a proof-of-stake mechanism promises even lower consumption. Ripple and Cardano are the frontrunners in energy efficiency, making them more sustainable choices.

Although quantum resistance is a part of security, traditional security aspects like resistance to double-spending attacks, 51% attacks, and others are essential. Bitcoin, despite its shortcomings, has an enviable track record, making it a gold standard in blockchain security. Cardano and Ethereum follow closely, with their layered architecture and smart contract capabilities adding multiple security layers. Ripple and Litecoin maintain robust security protocols, but like all platforms, continuous enhancements are necessary in an evolving threat landscape. Conclusively, while each platform brings unique strengths to the table, they also come with their own sets of challenges. Ripple excels in transaction speed and sustainability but needs to address its quantum resistance. Bitcoin, with its impeccable security, grapples with scalability and energy issues. Ethereum and Cardano, while modern and versatile, need to continually evolve to stay ahead of quantum threats. Litecoin is fast and secure, and faces challenges similar to Bitcoin.

As the blockchain landscape continues to evolve, these metrics will play a pivotal role in guiding platform development, ensuring they remain relevant, efficient, and secure in the face of emerging technologies and threats.

5. RESULTS AND DISCUSSION

The confluence of blockchain and quantum computing, two of the most groundbreaking technologies of our time, is nothing short of captivating. As observed from the results and evaluations, the nexus of these technologies promises transformative potential but also brings forth significant challenges, especially in the realm of security and scalability.

Diving deeper into the results, it is evident that while blockchain platforms like Ethereum, Bitcoin, and Cardano boast impressive attributes like vast developer communities, high network security, and research-driven development approaches, they still grapple with intrinsic vulnerabilities. These vulnerabilities, especially when juxtaposed against the mighty computational capabilities of quantum computers, expose potential security chasms. Bitcoin, with its established stature and widespread recognition, emerges as particularly susceptible to quantum threats. Given the foundational reliance of its cryptographic methodology on problems that quantum algorithms could potentially crack, this vulnerability raises concerns about the long-term security posture of the platform. Ripple, despite its efficiency and speed, mirrors these concerns, underscoring the pervasive nature of the quantum challenge.

Interestingly, the results also shed light on the nuanced role quantum computing can play. While on the one hand, quantum capabilities threaten to undermine existing cryptographic safeguards, but on the other hand, they offer potential solutions to some of blockchain's long-standing challenges, particularly scalability. Blockchain platforms, given their decentralized architecture, often face bottlenecks when processing high volumes of transactions. Quantum computers, with their ability to handle vast computations simultaneously, can potentially address this challenge, ensuring smoother, faster transaction validations and consensus formations. This dual role of quantum computing-as both a potential threat and a solution-presents a compelling narrative for the future of blockchain platforms.

The evaluation of quantum-resistant cryptographic methods is particularly enlightening. Lattice-based cryptography, hash-based signatures, and multivariate polynomial cryptography emerge as frontrunners in the race to fortify blockchain platforms against quantum threats. Their integration, while promising, would require substantial architectural changes, suggesting that the transition to a quantum-safe blockchain ecosystem would be gradual and iterative. Another striking observation from the results pertains to the energy consumption metrics. Bitcoin, with its energy-intensive Proof of Work (PoW) mechanism, starkly contrasts platforms like Ripple and Cardano, which demonstrate significantly lower energy footprints. In an era increasingly defined by environmental concerns, this distinction is not trivial. It not only influences the public perception of these platforms but also has broader implications for their sustainability and adoption. In conclusion, the results present a landscape rife with both opportunities and challenges. As blockchain platforms continue to evolve, their resilience against quantum threats will undoubtedly be a defining criterion for their success and longevity. While quantum computing brings with it the shadows of potential cryptographic vulnerabilities, it also offers a beacon of hope, lighting the path to a more scalable, efficient, and robust blockchain ecosystem. The interplay of these technologies, as observed, is neither wholly harmonious nor entirely discordant. Instead, it is a dynamic connection, shaping and reshaping the contours of the digital realm. As researchers, developers, and stakeholders, the responsibility is on us to navigate this connection, ensuring that the transformative potential of both blockchain and quantum computing is harnessed while mitigating their inherent risks.

A more thorough analysis of the potential impact of quantum computing on the environmental footprint of blockchain technologies is indeed crucial. Quantum computers, by their nature, promise to significantly enhance computational efficiency, which could reduce the energy consumption required for complex calculations like those involved in mining and transaction verification in blockchain networks. However, the actual energy demands of scaling quantum computing remain speculative and could offset these benefits. Our manuscript will explore these dynamics in detail, assessing both the

theoretical reductions in energy consumption due to increased computational efficiency and the potential increases in energy use due to the demands of maintaining quantum computing infrastructure. This analysis will provide a balanced view of how quantum advancements could environmentally reshape blockchain technology, highlighting both the opportunities for reducing the carbon footprint and the challenges of new quantum computational models.

While the integration of blockchain and quantum computing into healthcare systems like Electronic Health Records (EHRs) offers substantial benefits, it also presents notable challenges and limitations. Blockchain technology, although providing enhanced security and data integrity, struggles with scalability and speed issues, particularly when managing the large volumes of data typical in healthcare settings. Moreover, the energy consumption associated with blockchain operations poses environmental and economic concerns. On the other hand, quantum computing, despite its potential to revolutionize data processing and security, remains in its nascent stages with significant technological hurdles, such as error rates and qubit coherence, that need to be overcome before widespread practical implementation. Furthermore, the integration of quantum-resistant cryptography into existing systems raises issues of backward compatibility and increased computational demands, which could lead to inefficiencies. These challenges underscore the need for ongoing research, development, and careful consideration of cost-benefit trade-offs when deploying these technologies in critical sectors like healthcare.

5.1. Case Study: Assessing Ethereum's Vulnerability to Quantum Algorithms

5.1.1. Background

Ethereum, as a leading blockchain platform, employs the Ethash proof-of-work (PoW) algorithm and is transitioning towards a proof-of-stake (PoS) consensus mechanism. Its security largely depends on cryptographic protocols that may be vulnerable to quantum computing attacks, particularly those leveraging algorithms like Shor’s.

5.1.2. Objective

The primary goal of this case study was to evaluate the susceptibility of Ethereum to quantum attacks, focusing on its current cryptographic foundation and the potential implications of quantum computing developments.

5.1.3. Methodology

The evaluation involved a simulated quantum attack using a theoretical model of a quantum computer capable of running Shor’s algorithm. This model was applied to assess the time required to break Ethereum's cryptographic defenses, particularly targeting its digital signatures and transaction validations. The simulation parameters were set based on the estimated capabilities of near-future quantum computers, extrapolating from current quantum technology advancements.

5.1.4. Results

The simulation revealed that Ethereum's current cryptographic protocols could potentially be decrypted within a few hours by a sufficiently powerful quantum computer, posing a significant risk to the security of transactions and smart contract operations. This vulnerability was particularly evident in the handling of public key cryptography, where quantum algorithms could effectively derive private keys from public keys.

5.1.5. Mitigation Strategy

In response to these findings, the case study also explored the integration of lattice-based cryptography as a quantum-resistant solution for Ethereum. Preliminary tests indicated that this alternative could significantly enhance security against quantum attacks without imposing excessive computational burdens on the network.

5.1.6. Conclusion

This case study highlights the urgent need for Ethereum and similar blockchain platforms to adopt quantum-resistant cryptographic methods. The results suggest that while Ethereum's transition to a PoS model may reduce some risks associated with PoW mechanisms, the overarching threat from quantum computing remains a critical concern that requires proactive measures and continuous research into more robust cryptographic defenses.

5.1.7. Implications

The findings from this case study serve as a valuable benchmark for other blockchain platforms, emphasizing the importance of advancing cryptographic standards to withstand emerging quantum computing technologies.

5.2. Quantum Algorithms and their Computational Complexities

5.2.1. Shor's Algorithm

5.2.1.1. Purpose

Primarily used for factoring large integers and computing discrete logarithms, Shor's Algorithm poses a significant threat to public-key cryptographic systems like RSA and ECC, which rely on the difficulty of these problems for security.

5.2.1.2. Computational Complexity

Shor’s Algorithm demonstrates an exponential speedup over the best-known classical algorithms for factoring and logarithms. Specifically, it runs in polynomial time with respect to the number of digits nnn in the integer being factored, typically on the order of O $O((\log n)^2(\log\log n)(\log\log\log n))$, making it significantly faster than classical counterparts that operate in exponential time.

5.3. Grover's Algorithm

5.3.1. Purpose

Designed to search an unsorted database or solve a

black-box query problem, Grover's Algorithm can also be used to attack symmetric cryptographic systems by speeding up the brute-force search of a key.

5.3.2. Computational Complexity

Grover's Algorithm provides a quadratic speedup, reducing the complexity of searching through a database of N items from O(N) in the classical case to O(√N) in the quantum case. While this is substantial, it is less dramatic than the exponential speedup offered by Shor's Algorithm. Nonetheless, it remains a significant quantum advantage.

5.4. Roadmap for Implementing Quantum-resistant Cryptographic Methods

The mind map diagram shown in Fig. (**6**) illustrates the roadmap for implementing quantum-resistant cryptographic methods, training programs, and pilot implementations. Furthermore, to create a comprehensive and actionable roadmap for implementing quantum-resistant cryptographic methods, training programs, and pilot implementations, it is crucial to structure the approach into several detailed phases. Initially, an assessment should identify vulnerabilities to quantum attacks, followed by the selection and integration of suitable quantum-resistant algorithms such as lattice-based cryptography and hash-based signatures. Parallel to this, training programs must be developed and executed, offering tailored educational content on quantum resistance for various organizational roles. Pilot implementations should then be conducted in controlled settings to evaluate the performance and integration of these new cryptographic methods.

6. FUTURE ROADMAP AND RECOMMENDATIONS

The intersection of quantum computing and blockchain in the context of Electronic Health Record (EHR) systems is paving the way for an exciting era dubbed Healthcare 4.0-a vision of healthcare characterized by seamless integration, unparalleled security, and patient-centricity. As we stand at the cusp of this transformative phase, certain predictions, recommendations, and roadmaps can help chart the course ahead.

6.1. Emerging Healthcare 4.0 Technology

"Healthcare 4.0" refers to the transformative integration of digital technologies into healthcare systems, mirroring the principles of Industry 4.0, which emphasizes automation, interconnectivity, machine learning, and real-time data. Originating from the broader concept of the fourth industrial revolution, Healthcare 4.0 focuses on enhancing the efficiency, accuracy, and customization of healthcare services through advanced technologies such as artificial intelligence (AI), the Internet of Things (IoT), big data analytics, and blockchain. This paradigm shift aims to create a more patient-centered approach in healthcare, where systems are not only interconnected but also capable of predictive analytics, personalized treatment plans, and remote care delivery. The term serves as a critical descriptor within academic and practical discourse, highlighting the ongoing evolution and digital maturity of healthcare infrastructures to meet modern healthcare demands effectively.

The convergence of powerful quantum computational capabilities and secure, immutable blockchain systems, healthcare is poised to become highly personalized. Quantum computing will enable swift analysis of vast datasets, including genomics, allowing for treatments tailored to individual genetic makeup. Blockchain will facilitate decentralized EHRs where patients have control over their data. Patients can grant access to specific parts of their data to particular healthcare providers, ensuring confidentiality and fostering trust. Wearable devices, integrated with quantum-enhanced blockchain platforms, will allow for real-time monitoring of patients, enabling timely interventions and reducing hospital readmissions. The silos separating different medical specialties will collapse, facilitated by a unified, accessible, and secure blockchain-based EHR system. This will lead to holistic patient care, incorporating insights from various medical disciplines.

6.2. Recommendations for Implementation

Healthcare institutions should start investing in quantum-resistant cryptographic methods and infrastructure. While full-scale quantum computers capable of undermining current encryption might still be a few years away, being proactive will ensure a smoother transition when the time comes. The complexities of quantum computing and blockchain are not trivial. Training programs for healthcare professionals, IT staff, and administrative personnel can ensure that the transition to Healthcare 4.0 is smooth and that these stakeholders can harness the full potential of these technologies. Before a full-scale rollout, pilot programs should be initiated. These programs, focusing on integrating quantum and blockchain capabilities into EHR systems, can provide valuable insights into challenges, potential pitfalls, and areas of improvement. The journey to Healthcare 4.0 demands collaboration. Healthcare providers, IT companies, quantum computing startups, regulatory bodies, and patients should come together to shape the future. Collective insights will lead to a system that balances security, efficiency, and patient care. Regulatory bodies must keep pace with technological advancements. Current healthcare regulations might not fully address the nuances introduced by quantum and blockchain technologies. A proactive approach involving the revision of existing regulations and the formulation of new guidelines is crucial. The potential of quantum and blockchain in healthcare is vast, but so are the ethical implications. Decisions about data ownership, patient consent, and data sharing need to be made with utmost care, prioritizing patient rights and well-being.

CONCLUSION

The digital landscape of healthcare, particularly Electronic Health Record (EHR) systems, stands at a transformative juncture. Our exploration into the intersection of quantum computing and blockchain reveals profound insights ripe with both promise and challenge.

The evaluations presented showcased that popular blockchain platforms, like Bitcoin with its 7 transactions per second and Ethereum's 30, face tangible vulnerabilities to quantum threats, emphasizing a pressing need for quantum-resistant evolutions. While platforms like Ripple boasted high transaction speeds of 1500 per second, they also mirrored significant vulnerabilities, indicating that efficiency does not equate to security. Cardano, emerging as a blend of research-driven promise and moderate quantum vulnerability, exemplifies the evolving nature of this space. Furthermore, the energy footprints, as exemplified by Bitcoin's substantial 707 kWh per transaction, juxtaposed against Ripple's mere 0.0078 kWh, underscore the broader environmental and sustainability implications of these platforms. Our journey revealed gaps in empirical research, particularly in real-world quantum threats and the practicalities of transitioning to quantum-safe systems. The roadmap to the much-anticipated Healthcare 4.0, characterized by personalization, decentralization, and real-time monitoring, demands collaboration, foresight, and a commitment to balancing innovation with patient well-being. Personalization refers to tailoring medical treatments and health management plans refer to individual patient characteristics driven by genetic information, lifestyle data, and real-time health monitoring. Furthermore, Decentralization indicates the shift from traditional, centralized healthcare facilities to distributed care models, enabled by digital technologies that allow for effective healthcare delivery in community settings and even patient homes. Furthermore, Enhanced monitoring involves the continuous tracking of patient health metrics using sophisticated sensor technologies and wearable devices, facilitating early detection of potential health issues and enabling proactive medical interventions. As we forge ahead, it is evident that the confluence of blockchain and quantum computing will indelibly shape the future of digital healthcare, setting the stage for unparalleled advancements and novel challenges.

AUTHOR'S CONTRIBUTIONS

It is hereby acknowledged that all authors have accepted responsibility for the manuscript's content and consented to its submission. They have meticulously reviewed all results and unanimously approved the final version of the manuscript.

LIST OF ABBREVIATIONS

EHRs	=	Electronic Health Records
BioMEMS	=	Biomedical Microelectromechanical Systems
PKI	=	Public Key Infrastructure
PoW	=	Proof of Work
PoW	=	Proof-of-work
AI	=	Artificial Intelligence

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable.

HUMAN AND ANIMAL RIGHTS

Not applicable.

CONSENT FOR PUBLICATION

Not applicable.

AVAILABILITY OF DATA AND MATERIALS

The data and supportive information are available within the article.

FUNDING

None.

CONFLICT OF INTEREST

Dr. Vinayakumar Ravi is the Associate Editorial Board Member of The Open Bioinformatics Journal.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Goldstein JE, Guo X, Boland MV, Smith KE. Visual Acuity: Assessment of data quality and usability in an electronic health record system. Ophthalmol Sci 2022; 3(1): 100215. http://dx.doi.org/10.1016/j.xops.2022.100215 PMID: 36275199

[2] Heath M, Appan R, Henry R. Value alignment's role in mitigating resistance to IT use: The case of physicians'resistance to electronic health record systems. Inf Manage 2022; 59(8): 103702. http://dx.doi.org/10.1016/j.im.2022.103702

[3] Senerchia CM. Using passive extraction of real-world data from eConsent, electronic patient reported outcomes (ePRO) and electronic health record (EHR) data loaded to an electronic data capture (EDC) system for a multi-center, prospective, observational study in diabetic patients. 2022.

[4] Stolte A, Merli MG, Hurst JH, Liu Y, Wood CT, Goldstein BA. Using Electronic Health Records to understand the population of local children captured in a large health system in Durham County, NC, USA, and implications for population health research. Soc Sci Med 2022; 296(March): 114759. http://dx.doi.org/10.1016/j.socscimed.2022.114759 PMID: 35180593

[5] Trang K, Pierce L, Wick EC, Hirose K. Using electronic health record meta-data to identify variation in trainee progress note writing patterns: Opportunity to enhance systems-based care. J Surg Educ 2022; 79(6): e257-62. http://dx.doi.org/10.1016/j.jsurg.2022.08.011 PMID: 36096881

[6] Negro-Calduch E, Azzopardi-Muscat N, Krishnamurthy RS, Novillo-Ortiz D. Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews. Int J Med Inform 2021; 152: 104507. http://dx.doi.org/10.1016/j.ijmedinf.2021.104507 PMID: 34049051

[7] Valenti K, Giano Z, Rieck J. Sexual orientation and gender identity data collection in electronic health records: Application of recommendations within the university of colorado health system (Sci253). J Pain Symptom Manage 2023; 65(5): e669. http://dx.doi.org/10.1016/j.jpainsymman.2023.02.303

[8] Shuaib K, Abdella J, Sallabi F, Serhani MA. "Secure decentralized electronic health records sharing system based on blockchains," J. King Saud Univ. Comput Inf Sci 2022; 34(8): 5045-58. http://dx.doi.org/10.1016/j.jksuci.2021.05.002

[9] Walle AD, Shibebaw AA, Atinaf WT, *et al*. Informatics in Medicine Unlocked. Readiness to use electronic medical record systems and its associated factors among health care professionals in Ethiopia: A systematic review and meta-analysis. 2023; 1;36: p. : 101140.

[10] Matson RP, Niesen MJM, Levy ER, *et al*. Paediatric safety assessment of BNT162b2 vaccination in a multistate hospital-based electronic health record system in the USA: A retrospective analysis. Lancet Digit Health 2023; 5(4): e206-16. http://dx.doi.org/10.1016/S2589-7500(22)00253-9 PMID: 36963910

[11] Macabasag RLA, Mallari EU, Pascual PJC, Fernandez-Marcelo PGH. Normalisation of electronic medical records in routine healthcare work amidst ongoing digitalisation of the Philippine health system. Soc Sci Med 2022; 307(March): 115182. http://dx.doi.org/10.1016/j.socscimed.2022.115182 PMID: 35797835

[12] Caldis M, Schumacher J, Pickhardt P, Gigot M, Slattery B, Weiss J. Measuring potential modality-specific interval colorectal cancer rates utilizing an electronic health record algorithm across multiple health systems. Gastrointest Endosc 2023; 97(6): AB247. http://dx.doi.org/10.1016/j.gie.2023.04.407

[13] Caldis M, Schumacher J, Pickhardt P, Gigot M, Slattery B, Weiss J. Measuring potential modality-specific interval colorectal cancer rates utilizing an electronic health record algorithm across multiple health systems. Gastrointest Endosc 2023; 97(6): AB145-6. http://dx.doi.org/10.1016/j.gie.2023.04.248

[14] Mageras A, Wood E, Wyatt B, *et al*. Improving hepatitis B screening and linkage to care rates *via* the electronic medical record, provider engagement, and patient navigation in a large, urban health system. J Hepatol 2023; 78: S116-7. http://dx.doi.org/10.1016/S0168-8278(23)00605-0

[15] Wilson M G, Palmer E, Asselbergs F W, Harris S K. Integrated rapid-cycle comparative effectiveness trials using flexible point of care randomisation in electronic health record systems. J Biomed Inform 2023; 137: 104273.

[16] Hull LE, Vassy JL, Stone A, *et al*. Identifying end users' preferences about structuring pharmacogenetic test orders in an electronic health record system. J Mol Diagn 2020; 22(10): 1264-71. http://dx.doi.org/10.1016/j.jmoldx.2020.06.015 PMID: 32980074

[17] Luyten J, Marneffe W. Examining the acceptance of an integrated Electronic Health Records system: Insights from a repeated cross-sectional design. Int J Med Inform 2021; 150(June): 104450. http://dx.doi.org/10.1016/j.ijmedinf.2021.104450 PMID: 33848941

[18] Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. Sensors (Basel) 2023; 23(21): 8944. PMID: 37960646

[19] Goulding M, Ryan G, Frisard C, *et al*. Disparities in receipt of guideline-adherent blood pressure screening: An observational examination of electronic health record data from a massachusetts healthcare system. J Pediatr 2023; 261: 113592. http://dx.doi.org/10.1016/j.jpeds.2023.113592 PMID: 37399919

[20] Poulos J, Zhu L, Shah AD. Data gaps in electronic health record (EHR) systems: An audit of problem list completeness during the COVID-19 pandemic. Int J Med Inform 2021; 150(June): 104452. http://dx.doi.org/10.1016/j.ijmedinf.2021.104452 PMID: 33864979

[21] Nagy Z, Gunay B, Miller C, *et al*. Ten questions concerning occupant-centric control and operations.Build Environ 2023; 242: 110518. https://www.sciencedirect.com/science/article/pii/S0360132323005450

[22] Shi S, He D, Li L, Kumar N, Khan MK, Choo KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Comput Secur 2020; 97: 101966. http://dx.doi.org/10.1016/j.cose.2020.101966 PMID: 32834254

[23] Mihova P, Stankova M. Application of an electronic health record system for studying the influence of the daylight-saving time change on health needs. Procedia Comput Sci 2021; 192: 3815-21. http://dx.doi.org/10.1016/j.procs.2021.09.156

[24] Hajian A, Prybutok VR, Chang HC. An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective. Comput Human Behav 2023; 138: 107471.