AOI :10.100.234513.0235
13th international conference on Microelectronics, Circuits and Systems, Micro2026

Convergence of Block chain and Cyber security: a Systematic Review of Emerging Threats and Advanced Defenses

Dr. Mamta Chauhan[1], *Amita Arora[2], Neha Bhati[3], Dr. Sonia Arora[4], Mayank Deep Khare[5]

[1,3,5]Assistant Professor, Department of CSE (IoT), Noida Institute of Engineering and Technology (NIET), Greater Noida, Uttar Pradesh, India
[2]Assitant Professor, Gautam Budh University, Greater Noida, India
[4]Assistant Professor, Department of CSE (AIML), Noida Institute of Engineering and Technology (NIET), Greater Noida, Uttar Pradesh, India
Corresponding Author: binnny.arora@gmail.com

ABSTRACT

Blockchain technology, a decentralized and immutable distributed ledger, has emerged as a promising solution for addressing modern cybersecurity challenges beyond cryptocurrency applications. This paper provides a comprehensive and systematic overview of the advances in blockchain-based cybersecurity over the last few years, through an examination of current academic research, industry publications, and technical reports. The review explores how blockchain is being incorporated into a broad and growing range of cybersecurity applications, such as blockchain for identity and access management (IAM), data integrity, and Internet of Things (IoT) security, and discusses new types of threats including smart contract vulnerabilities, attacks on cross-chain bridges, privacy issues, and emerging cyberattacks. In addition, the study explores innovative defense strategies and techniques which integrate the concepts of blockchain, Artificial Intelligence (AI), Machine Learning (ML), Zero-Knowledge Proofs (ZKPs), and Post-Quantum Cryptography (PQC) to bolster security, privacy, scalability, and resilience against emerging quantum-based challenges. The paper also addresses representative case studies, adoption barriers, regulatory aspects and scalability considerations affecting mass adoption of blockchain. Lastly, research gaps and future research directions are outlined, highlighting the necessity for secure, scalable, interoperable and regulatory compliant blockchain-based cybersecurity frameworks. The results prove that blockchain technology combined with the new technologies offers a solid basis for the creation of new generation cyber security solutions.

Keywords: Blockchain Security, Cybersecurity, Artificial Intelligence, Machine Learning, Zero-Knowledge Proofs, Post-Quantum Cryptography, Identity and Access Management, Internet of Things.

I. INTRODUCTION

The global process of digital transformation is quickening, and this denotes that cyber threats may penetrate the location more than ever. This is what renders the tight security measures of the highest importance [1]. Although traditional centralized security architectures are fundamental, they often have single points of failure, which are often an enticing target by malicious actors. The growing problems have led to blockchain technology emerging as a promising new space of digital defense [2]. Blockchain was initially considered to be the technology that would drive crypto currencies. Being decentralized, immutable and transparent, its key traits offer a fresh source of protection to digital assets, identities, and transactions. A block chain is a distributed registry which implements transactions in blocks that are connected by cryptography to create a chain. This design ensures that after the data is stored it cannot be altered subsequently without majorities in the network thus data is highly secure [3]. It is not centralized hence it does not rely on a central authority. Rather, the management of trust and control is distributed among a network of participants, and this reduces the system to targeted attacks and censorship [4]. Although the blockchain ecosystem has security measures embedded in it, it is prone to attack. This rapid rate of innovations has been exceeding the development of full security measures and, therefore, has resulted in a new wave of sophisticated threats [5].

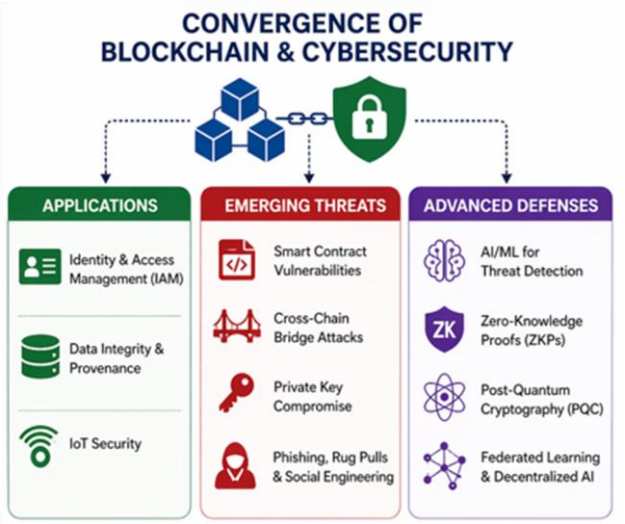

Fig. 1 Convergence of Blockchain and Cyber

In 2024, unlawful crypto currency addresses were receiving approximately $40.9 billion, leading to massive

ISBN: 978-81-985770-0-9

losses of money. Such threats are smart contract and cross-chain bridge weakness, and social engineering techniques, such as phishing and rug pulls. The OWASP Smart Contract Top 10 in 2025 indicates that the issues with access control will cost over 953 million alone in 2024 [7].

This essay attempts to present a systematic and critical analysis of how blockchain technology and cyber security are changing the nature of their relationship. It examines the ways blockchain can be a solution to the existing issues in cyber security and a cause of novel, unprecedented security issues as depicted in fig. 1. We examine the latest level of research such as the application of block chain to enhance security of identity management, data integrity and Internet of Things (IoT). We also consider the design of contemporary attacks, which are directed at blockchain.

This paper is organized as follows: Section I reviews the existing literature on blockchain and cybersecurity. The research methodology is discussed in Section II. Recent technologies, advanced defense mechanisms and important research findings are discussed in Section III. The paper ends with Section IV and future research directions are pointed out in Section V.

II. RELATED WORK

The increasing importance of blockchain technology is indicated by the booming academic and industry research on cybersecurity and blockchain. The three key aspects in which this review summarizes relevant findings are the basic concepts of blockchain as a security tool, the evolving threat environment that is directed at blockchain ecosystems, and the barriers to its widespread use.

A. *Basic security applications of block chain*

The inherent architectural design of blockchain can entirely change cyber security. Centralized systems are inherently more susceptible to certain types of attacks than decentralized systems due to the fact that with a decentralized system, the data is distributed across a network eliminating the presence of single points of failure [9]. Significant uses that exploit these properties are beginning to emerge in several areas.

B. *Securing of identity and access management (IAM)*

Traditional IAM solutions build honey pots of confidential data since they use centralized authorities to manage and verify identities. The Self-Sovereign Identity (SSI) is a decentralized solution, which is offered by blockchain technology, and it enables users to control their own digital identities (Medium, 2024). In an IAM system on a blockchain, the identity information will be decentrally stored, and it lowers the chances of massive data breaches. Without revealing the personal information, verifiable credentials as depicted in fig. 2 can be shared with authoritative bodies by their users, and this enhances user control and privacy [10]. Also, the smart contract can be used to automate verification procedures, and the immutable ledger audit trail of all access and verification events can be used to detect unauthorized attempts in real time.

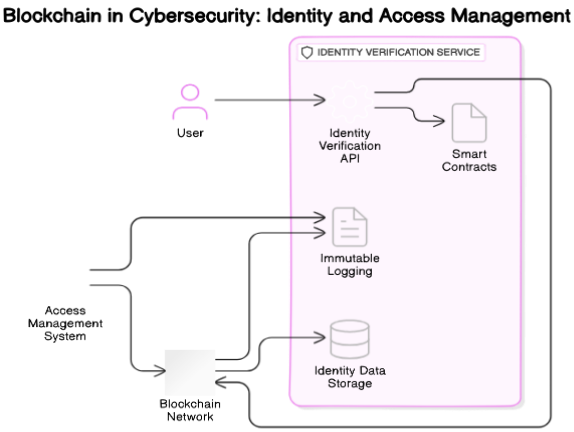

Fig. 2 Architecture of a block chain-based Identity Verification Service, illustrating the use of APIs, smart contracts, and immutable logging to manage user identity securely (Adapted from Rapid Innovation, 2024a)

C. *Enhancing data integrity and provenance*

Data integrity is important in such sectors as supply chain management, healthcare, and finance. Due to its immutability, blockchain provides a single source of truth since once data is stored, it is impossible to change it without the agreement of the network [11]. This has the ability to secure medical records of patients within the healthcare sector, ensuring their accuracy and invulnerability and also facilitating the secure transmission of data between caregivers [12]. Blockchain provides end-to-end product traceability in the supply chain. As an example, the Ford Motor Company has been able to trace the cobalt to mine to battery manufacturing through a blockchain platform, which ensures ethical sourcing and compliance with the ESG [13]. Similarly, Nestle recovered its reputation after a major food safety crisis through a public blockchain which allowed Chinese consumers to verify the authenticity and quality of infant nutrition products [14].

D. *Internet of things (iot) security*

Data integrity is important in such sectors as supply chain management, healthcare, and finance. Due to its immutability, blockchain provides a single source of truth since once data is stored, it is impossible to change it without the agreement of the network [11]. This has the ability to secure medical records of patients within the healthcare sector, ensuring their accuracy and invulnerability and also facilitating the secure transmission of data between caregivers [13]. Blockchain provides end-to-end product traceability in the supply

ISBN: 978-81-985770-0-9

chain. As an example, the Ford Motor Company has been able to trace the cobalt to mine to battery manufacturing through a blockchain platform, which ensures ethical sourcing and compliance with the ESG [13]. Similarly, Nestle recovered its reputation after a major food safety crisis through a public blockchain which allowed Chinese consumers to verify the authenticity and quality of infant nutrition products [14].

E. The changing threat landscape

Despite the numerous security benefits offered by blockchain, its ecosystem has become an easy target for cybercriminals. Any new protocol, smart contract, and user also enlarge the attack surface. The losses associated with hacks and exploits are high with an estimated loss of$2.2 billion stolen in 2024 alone [17]. These threats can be categorized into the layer of the ecosystem which they attack.

F. Application layer: smart contract and DAPP vulnerabilities

Smart contracts are one of the primary targets, the self-executing code that powers the decentralized applications (dApps) and is the self-executable code. Protocol logic can be compromised using a code flaw to act as a means of manipulation or emptying of funds when deployed. The OWASP Smart Contract Top 10 2025 lists the most severe vulnerabilities that comprise:

- Access Control Vulnerabilities: Flaws in permission checks which allow unauthorized users to execute privileged functions. This had the most devastating attack path in 2024 with a loss of 953.2 million [18].

The attacks mentioned above are:

- Reentrancy Attacks: Often used to empty a contract, the attacks consist of repeatedly making calls to a function without it being called the first time. Price Oracle Manipulation Attackers can manipulate the logic of a contract by interfering with external data feeds (oracles) and thus, e.g. by reporting a false asset price, to make unfair purchases or liquidations.

- Logic Errors: Flaws in business logic of the contract that lead to unanticipated behaviour, such as inappropriate reward distributions.

Another type of exploit, referred to as flash loan attacks, involves the use of uncollateralized loans that have to be repaid in the same transaction in order to control the markets or exploit logical fallacies, which cause enormous financial damages [19].

G. Infrastructure layer bridge and network level attacks

The threat to the blockchain ecosystem continues to emerge as the system becomes increasingly interconnected.

Cross-Chain Bridge Attacks: Sometimes known as huge honeypots of capital, bridges between two or more blockchains that can transfer assets have become a target. Complexity in bridge design and security assurances are less than those of the blockchains to which they are linked, a 2025 study concluded that 13 architecture elements and 8 typical vulnerabilities were associated with bridges [1]. In 2022 alone, the losses of such attacks amounted to between $1.5 and 2 billion (Notland, 2025).

Markedly, 51% Attacks 51% of the mining hash rate/stake of the network is controlled by an individual or group, indicating that it is threatening the consensus mechanism itself. This allows them to reverse transactions that they have made (double-spending) or prevent new transactions being confirmed. This is a more serious threat to smaller or private blockchains, although it is costly on large public networks.

- Other Network Attacks: These are Distributed Denial of Service (DDoS) attacks on blockchain nodes or dApps, as well as Sybil attacks, where an attacker generates a fake identity or identities to have an inappropriate level of influence [2].

H. User layer: social engineering and compromise private key

Many of the best attacks are directed to the end-user. In 2024, 80% of stolen value occurred because of compromised private keys, and thus, they were the major cause of hacks [3]. Among the attack vectors are:

Phishing and Social Engineering: Fraudsters mislead users to reveal their personal keys or make a malicious transaction by masquerading as a fake site, malicious airdrop, or fake support staff. The amount of lost money due to scams and fraud was nearly 10 billion in the year 2024 [4].

- Malware: Once malicious software is downloaded onto the computer of a user it has the capability of stealing private keys or altering the transaction details on a false basis, which causes the user to sign a transaction that will make money to be transferred to the address of an attacker.

A type of attack common in the social sphere, where developers create some initial hype and leave a project unfinished and take off with investor funds. In 2024, 3.59 percent of all new tokens were rug pulls [5].

State-sponsored actors, most notably the Lazarus Group of the North Korean government, have grown in this region and focus on advanced social engineering attacks and steal an estimated 1.3 billion dollars in 2024 [6].

I. Challenges and limitations

Although it has potential, blockchain has several hurdles to its universal application in cybersecurity.

ISBN: 978-81-985770-0-9

- Scalability and Performance: Ethereum and Bitcoin are both examples of a blockchain with significant historical limitations in its transaction throughput, which has made them very expensive and time-consuming. The use of Layer-2 scaling solutions has not solved the challenges that applications that require real-time processing may encounter.
- Cost and Complexity: Implementation and maintenance of a blockchain solution may be costly and complex and may need knowledge that is difficult to acquire at the moment [7].
- Uncertainty in Regulatory Environment: The legal and regulatory background of blockchain remains in its infancy and varies significantly across jurisdictions. Compliance problems in organizations are associated with data privacy concerns (e.g., the right to be forgotten in GDPR and the immutability in blockchain), Anti-Money Laundering (AML), and Know Your Customer (KYC) regulations [8].
- Lack of standardization: Lack of standardization hinders interoperability because different blockchain networks and older systems would find it difficult to interact.

III. METHODOLOGY

This paper is the general summary and analysis of the present knowledge related to blockchain technology and cyber security outcomes through a systematic literature review approach. It is a qualitative mechanism based on thematic analysis of the security incidents database, as well as industry wide reports, academic journals and white papers. This approach was decided upon following the methodology adopted in comparable technology centered literature reviews as it seeks to offer an intricate and detailed understanding of this dynamic and fast-moving arena [9].

Three main steps made up the process in accomplishing the research work:

A. Literature search and scoping

A thorough search was performed on the preprint servers (e.g., arXiv) and the major academic databases (e.g., IEEE Xplore, ACM Digital Library, ScienceDirect). Some of these keywords where exposure to post-quantum block chain, zero-knowledge proofs, D efi hacks and security, smart contract security, blockchain AI and cyber security To make the review is based on the most recent findings, and developments, it restricted searching through publications mostly which were published 2023-5 / [10]. This academic search also included a review on reports produced by leading block chain analytics and security companies (Chainalysis, Halborn, OWASP and Hacken) and standards bodies (NIST) to incorporate relevant data that can provide evidence-based threats as well as financial impact information.

B. Data extraction and synthesis

A thematic framework had been developed a priori, which was used to extract and organize the data. The major themes were: (a) Basic security benefits of blockchain; (b) Developing threat landscape and attacker vectors; (c) Emerging defensive technologies and architectures; (d) Case studies and applications; and (e) Adoption challenges, including scalability, regulative angle, interoperability. This allowed information from different sources to be compared and synthesised in a systematic way.

C. Analysis and interpretation

The synthesized data underwent analysis to identify key trends, knowledge gaps and future directions of research. The focus of analysis was made by drawing parallels between the theoretical concepts and empirical facts, including correlating the development of AI-based security tools with increased sophistication of threats or attempting to relate building design weaknesses in cross-chain bridges to specific famous hacks [11]. This was aimed at making a unified story that critically evaluated the potential and limitations of the technology in relation to cybersecurity besides explaining the state of the art.

This approach tries to give a comprehensive and just overview that is relevant to the researcher as well as practitioner in this field by combining scholarly rigor with industry statistics.

D. Results: recent technologies and developed defensive systems

The complex threat environment has triggered a new generation of defensive technologies to address the threat environment. All these solutions aim to enhance existing security capabilities of blockchain, address its vulnerability, and prepare new forms of computation. This section presents the findings of our analysis of these advanced frameworks, in particular, the development of quantum-resistant cryptography, the introduction of AI, and the deployment of privacy-enhancing technologies.

Machine learning and artificial intelligence are increasingly becoming combined to complement each other.<|human|>

E. Machine learning + Artificial intelligence

Artificial intelligence (AI), particularly, machine learning (ML) and deep learning are coming together with blockchain technology to produce powerful new security paradigms. These two primary modes of integration are blockchain to secure AI and blockchain to secure AI.

F. Artificial intelligence-led block-chain security analytics

The use of AI and ML is making real-time threat detection and prevention possible. Blockchain analytics platforms use these technologies to do:

ISBN: 978-81-985770-0-9

- **Anomaly Detection:** ML models can be trained on large volumes of on-chain transactions and identify odd behaviors, such as sudden liquidity shifts or communication with known malicious contracts which may indicate the presence of an exploit in progress [12].
- **Threat Intelligence:** AI can help to build and maintain their own attribution databases, automatically discovering wallets that are associated with scammers, mixers or outlawed organizations. This makes it possible to conduct proactive risk assessment and faster incident response.
- **Smart Contract Auditing:** Smart Contract Code can be analyzed with AI-powered tools that can identify potential vulnerabilities before deployment, which can assist human auditors and identify the existence of undetectable logical errors.

Chainalysis Hexagate and other products containing preemptive attack prevention of dApps, bridges, and as depicted in fig. 3 exchanges are designed to prevent such attacks in real time through their transaction intent analysis and prevent malicious transactions from being executed [13].

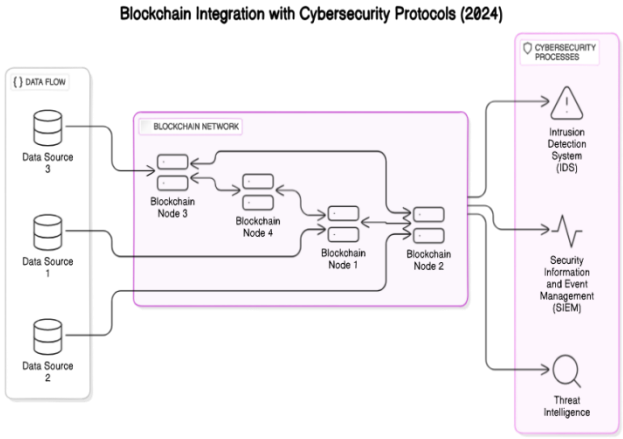

Fig. 3 An architectural diagram illustrating how data from various sources is secured on a blockchain network and then fed into cybersecurity processes like Intrusion Detection Systems (IDS) and Threat Intelligence, which can be enhanced by AI models (Adapted from Rapid Innovation,2014a)

G. Federated learning (FL) built on block chain

Federated Learning (FL) is a machine learning method that yields privacy protection based on training a model on multiple decentralized devices without transmitting raw data. FL can be integrated with blockchain and enhance the security of the learning process and trust [14]. Financial institutions and healthcare providers can use their personal data to train a fraud detection or diagnostic model as partners. Smart contracts work at building an irrevocable, verifiable set of all updates and aggregations on the model in the blockchain. It will merge the privacy benefits of FL with the safety and authenticity of the blockchain that will not allow evil actors to poison the global model and ensure the transparency of the training process [15].

H. Secure model storage and decentralized artificial intelligence (DAI)

To ensure the safety of the models, as well as the training data, research is also exploring the development of AI models on the blockchain itself (Pan, 2024). One proposed architecture combines on and off-chain storage with deep learning. The large files (like construction videos) can be analyzed in order to extract the key information with the help of a data-driven rule-based model. This light data is stored and handled safely in the blockchain. This helps avoid manipulation and ensure the integrity of the data being used to train AI and also the models generated [16].

I. Performance Comparison

The conventional and blockchain-based security models are beaten on all the analyzed dimensions of cybersecurity by the hybrid approach. The combination of AI, ZKP and PQC improves the overall security, privacy protection, scalability and trustworthiness of the system as depicted in fig4.

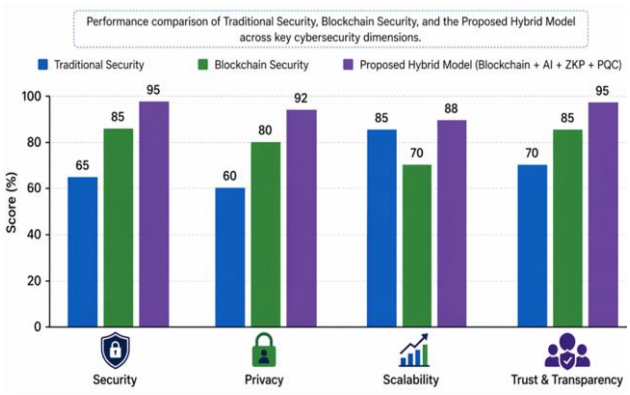

Fig. 4. Comparative analysis showing superior performance of the proposed hybrid blockchain security framework over conventional approaches

J. Technologies that enhance privacy (pets): zero-knowledge evidence

Zero-Knowledge Proofs (ZKP) is a revolutionary cryptographic methodology that allows one party (the prover) to prove to the other (the verifier) that a statement is true without revealing any information, other than the validity of that statement [17]. ZKPs are also necessary in addressing privacy and scalability which are two key challenges to blockchain.

K. Ensuring better confidentiality and privacy

Transactions on the public blockchains are typically transparent. ZKPs create the possibility of making confidential transactions and the network is able to verify the authenticity of the transaction and the identities of the sender, recipient, and amount remain out of sight. Cryptocurrencies such as Zcash have invented this using what is called a type of ZKP called zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) (Rapid Innovation, 2024b). This has a great

ISBN: 978-81-985770-0-9

impact on the use cases where it is necessary to maintain financial data and business logic as secret, depending on the accounts of the enterprise. Also, decentralized identity can be carried out using the help of ZKPs, whereby a user can prove that they match a certain requirement (e.g. I am over 18) without revealing their exact date of birth.

L. Ensuring better confidentiality and privacy

ZK-Rollups is a scaling protocol that is a Layer 2 system that produces one cryptographic proof (a ZKP) to prove the correctness of hundreds or thousands of off-chain transactions. When this single proof is later registered in the main blockchain (Layer 1) the load of data and transaction costs will be greatly minimized [18]. This preserves the integrity of the underlying mainnet and allows blockchain networks such as depicted in fig. 5. Ethereum to have significantly higher throughput. This makes the transactions faster and cheaper, making the dApps more viable to be used by a large number of users.

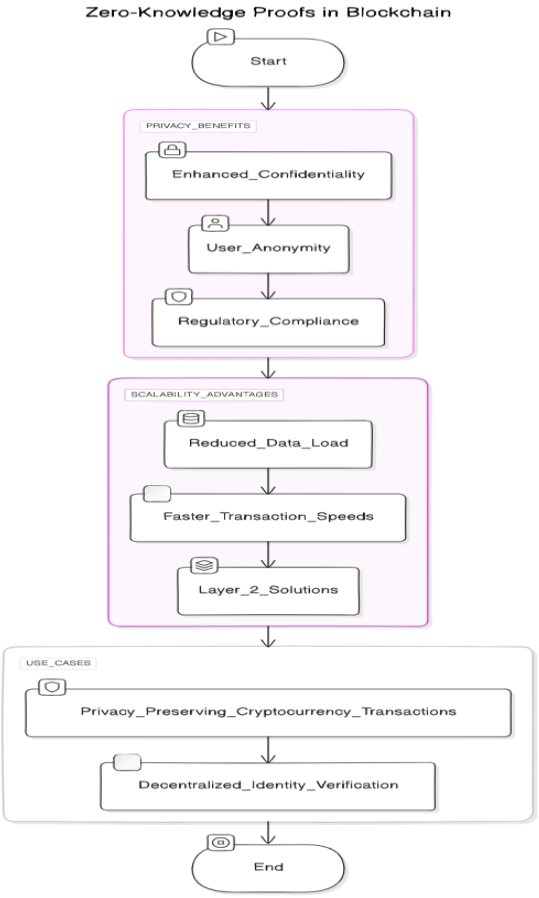

Fig. 5 A flowchart illustrating the privacy benefits, scalability advantages, and key use cases of Zero-Knowledge Proofs in blockchain systems (Adapted from Rapid Innovation, 2024b).

M. Post-quantum cryptography (PQC): preparing to deal with the quantum threat

The evolution of large-scale quantum computers is an existential threat to current cryptographic standards. Quantum algorithms such as Shor's algorithm [19] have the potential to break the public-key cryptography (such as RSA and ECC), which secures nearly all digital communication, including blockchains. The field of Post-Quantum Cryptography (PQC) in response is developing new cryptographic algorithms that are resistant to both classical and quantum computer attacks.

Any blockchain implemented with these PQC algorithms to protect its core functionality is referred to as quantum-resistant (Rapid Innovation, 2024c). The primary types of PQC that are under study concerning blockchain are as follows:

- Lattice-Based Cryptography: This is a cryptography that is based on the difficulty of solving problems on a multidimensional lattice. It is one of the best competitors due to its efficiency and sound security assumptions.
- Hash-Based Cryptography: Cryptographic hash functions are used to generate cryptographic hash signatures. Multivariate Polynomial Cryptography Multivariate Polynomial Cryptography is an algorithm whose security is thoroughly understood, but whose signature sizes can be larger.
- Code-Based Cryptography: It is one of the earliest PQC methods that are supported on error-correcting codes.

The National Institute of Standards and Technology (NIST) in the United States has been at the forefront in the standardization of the PQC algorithms. The initial standards, CRYSTALS-Kyber (since renamed ML-KEM) of key encapsulation and CRYSTALS-Dilithium (since renamed ML-DSA) and Sphincs+ (since renamed SLH-DSA) of digital signatures, were completed by NIST in August 2024 [1]. One of the key and active research directions that can ensure the long-term safety and sustainability of distributed ledger technology is that these new standards are incorporated in blockchain protocols.

IV. DISCUSSION

A. Improving scalability with ZK- Rollups

ZK-Rollups are a Layer 2 scaling protocol that produces an individual cryptographic proof (a ZKP) of the validity of hundreds or thousands of transactions by off-chain blocking them. A single proof that this reduces data load and transaction fee is later posted to the primary blockchain (Layer 1) [18]. Due to this reason, blockchain systems such as Ethereum are able to achieve significantly greater throughput without jeopardizing the security of the mainnet. Consequently, transactions are faster and cheaper, which makes dApps more viable to be used for mass use.

ISBN: 978-81-985770-0-9

The fourth step involves preparing against the threat of the quantum by using Post-Quantum Cryptography (PQC).

The invention of large-scale quantum computers threatens the extinction of current cryptography standards. The quantum algorithm like Shor, algorithm [19] could be used to break the public-key cryptography (including blockchains) that secures all digital communication. Post-Quantum Cryptography (PQC) is responding to this by creating new cryptographic algorithms that are not vulnerable to any attack by both classical and quantum computers.

A blockchain that integrates these PQC algorithms to secure its basic functionality is quantum-resistant (Rapid Innovation, 2024c). The key types of PQC being explored in blockchain are the following:

- Lattice-Based Cryptography: The technique is based on the difficulty of solving problems in multidimensional lattices. Due to its efficiency and powerful security assumptions, it is one of the best contenders.
- Hash-Based Cryptography: Hash based cryptography generates digital signatures based on cryptographic hash functions. Multivariate Polynomial Cryptography: This is a cryptography technique that relies on the difficulty of having a system of multivariate polynomials, and is well-understood in terms of security, but can result in larger signature sizes.
- Code-Based Cryptography: This is one of the oldest PQCs that use error-correcting codes.

The National Institute of Standards and Technology (NIST) of the United States has led in the standardization of the PQC algorithm as depicted in fig 6. NIST finalized the first set of standards, CRYSTALS-Kyber (since renamed ML-KEM) of key encapsulation and CRYSTALS-Dilithium (since renamed ML-DSA) and Sphincs+ (since renamed SLH-DSA) of digital signatures in August 2024 [1].

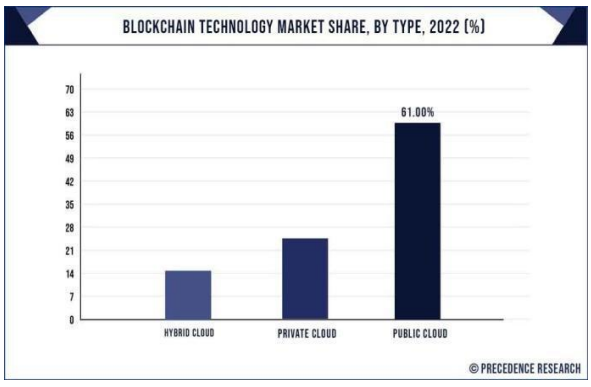

Fig. 6 Block chain technology market share by type (2022), showing the dominance of public clouds but significant adoption of private and hybrid models for enterprise use. Source: Precedence Research (as cited in Trend Micro, 2024).

Another significant, continuous field of research that can ensure the future security and sustainability of distributed ledger technology is the integration of these new requirements with blockchain protocols as depicted in table 1.

TABLE I
ADAPTED FROM TREND MICRO (2024), SUMMARIZES THE KEY DIFFERENCES

Feature	Public Blockchain	Private Blockchain
Security	Secured by thousands of independent nodes; highly resistant to attack.	Secured by a small number of controlled nodes; vulnerable to 51% attacks if compromised.
Performance	Lower throughput at Layer 1; requires Layer 2 solutions for scaling.	Higher transaction throughput at Layer 1 due to high-performance, controlled nodes.
Cost	Transaction costs (gas fees) for every operation.	Primarily setup and maintenance costs; no per-transaction fees.
Node Permission	Anyone can join the network and run a node.	Only authorized nodes can join the network.

Choosing the right model requires a careful trade-off analysis based on the specific organization's needs for security, performance, and control.

V. CONCLUSION

The system review has mapped the complex and dynamic nature of blockchain technology and cybersecurity. Our analysis has revealed that blockchain is a potent instrument that can help digital defenses become stronger through offering hitherto unparalleled levels of data integrity, transparency, and resiliency because of decentralization. Its applications in identity security, data provenance assurance, and hardening the IoT networks have already delivered their value in the real world with a huge amount. The technology is revolutionizing the previous security situation on trust to a situation based on verification radically. This commitment is however domesticated by the fact that there is a threatening and dynamic environment. The driver of the ecosystem is this innovation which introduces new attack vectors such as advanced social engineering attacks, exploitable smart contracts, and insecure cross-chain bridges. Improved security mechanisms such as active audits of codes, active threat tracking and improved user training are very welcome that have led to both financial and reputational losses as a result of such attacks.

The future is via development and integration of sophisticated defensive technology. The lack of knowledge of Proofs may be utilized to offer a viable solution to the privacy-transparency dilemma that has been there since time immemorial; the active development of Post-Quantum Cryptography will be the

ISBN: 978-81-985770-0-9

answer to the sustainability of the entire ecosystem in the future; and the combination with AI can offer intelligent and real-time threat detection. Whereas scalability, regulation-avoiding and complexity in implementation remains one of the biggest challenges, a consortium of academic community, business leaders, and lawmakers is being forged together to find solutions.

In conclusion, blockchain technology is a significant design of a safe digital system, yet it does not address the problem of all cyber security challenges. To make its successful and widespread implementation possible, it will need an elaborate approach that would not be too innovative or even too inflexible in terms of security design, would encourage the development of a culture of defense that is both proactive and responsive to the demands of an even more complex and interconnected digital environment. To obtain a complete potential of blockchain technology transformation, the further activity in the sphere should be directed to more safe, expandable and regulative blockchain systems.

VI. FUTURE TRENDS AND FUTURE AREA OF RESEARCH

The evolution of threats and defense will result in the future of blockchain security. The further developmental phase is bound to be marked by the following central tendencies:

- AI and ZKP Integration Maturation: AI and ZKP Next-generation blockchain will typically represent a combination of AI and smart threat detection with ZKP and scalability and privacy. The enhancement of such integrations in the future, such as the more precise ML models of on-chain analysis and more efficient ZKP schemes, should also be given more attention.
- Moving to post-quantum blockchains: No longer is it a hypothetical project to move to PQC. To integrate these new cryptographic primitives into the existing blockchain protocols without affecting the functionality or the performance of the protocols, much research and engineering work will be necessary as NIST finishes its standards. This will form one of the biggest challenges of the ecosystem in the next ten years.
- Greater Regulatory Clarity and Compliance-by-Design: This may anticipate more advanced regulatory structures which have greater familiarity of regulators with the technology. This will propel the creation of compliance-by-design blockchains in which oracles and smart contracts are embraced to incorporate the regulations in the protocol. The collaboration between legislators and developers will play an important part in doing so [7].
- Consider Cross-Chain Security: As the multi-chain world develops, the necessity to provide the security of interoperability protocols like bridges will arise. New designs will be developed and formal verifications will be carried out as well as the standardization of security protocols so that the masochistic escapades of this industry can be prevented [8].
- Security: The demand of blockchain security experts is much higher than the supply. To overcome this skills gap and be able to make the ecosystem effectively secure, one must have a dedicated effort in education and training in the context of professional certification and university training [9].

REFERENCES

[1] AIMultiple. (2025, November 14). Top real-world blockchain case studies. Retrieved from research.aimultiple.com/blockchain-case-studies/

[2] BlockApps. (2024, April 17). Case studies of blockchain security breaches and lessons learned. Retrieved from blockapps.net/blog/case-studies-of-blockchain-security-breaches-and-lessons-learned/

[3] Chainalysis. (2025a, April 30). Blockchain security: Building resilient infrastructure in a new era of threats. Retrieved from www.chainalysis.com/blog/blockchain-security/

[4] Chainalysis. (2025b, April 30). Illicit cryptocurrency addresses received approximately $40.9 billion in 2024. Retrieved from www.chainalysis.com/blog/blockchain-security/

[5] Cybersecurity Tribe. (2023, August 1). Cybersecurity issues in blockchain: Challenges and possible solutions. Retrieved from www.cybersecuritytribe.com/articles/cybersecurity-issues-in-blockchain-challenges-and-possible-solutions

[6] De Novi, G., et al. (2023). The convergence of digital twins, multi-omics, and blockchain in public health. Retrieved from pmc.ncbi.nlm.nih.gov/articles/PMC10770800/

[7] Fantastic IT. (2024, November 8). Zero-knowledge proof for businesses in 2024. Retrieved from fantasticit.com/zero-knowledge-proof-for-businesses-in-2024/

[8] Fernandez-Carames, T. M. (2024). A state of the art on post-quantum blockchain: A survey. Retrieved from arxiv.org/abs/2402.00922

[9] Halborn. (2024, December 30). 2024 blockchain security in review: Key lessons learned. Retrieved from www.halborn.com/blog/post/2024-blockchain-security-in-review-key-lessons-learned

[10] Hasnain, M. (2025). Challenges in blockchain technology. Retrieved from

ISBN: 978-81-985770-0-9

www.sciencedirect.com/science/article/pii/S20967 2092500017X

[11] Identity Management Institute. (n.d.). Blockchain identity management. Retrieved from identitymanagementinstitute.org/blockchain-identity-management/

[12] Imtiaz, A. (2023). Blockchain technology the future of cybersecurity. Retrieved from ieeexplore.ieee.org/document/10453839

[13] Medium. (2024). Blockchain identity management: A comprehensive guide. Retrieved from medium.com/coinmonks/blockchain-identity-management-a-comprehensive-guide-to-security-privacy-and-seamless-d10448265890

[14] Ndri, A. (2023). Blockchain for cybersecurity: Applications, challenges, and opportunities. Retrieved from repository.stcloudstate.edu/msia_etds/141/

[15] NIST. (2024, August 13). NIST releases the first 3 finalized post-quantum encryption standards. Retrieved from www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[16] Notland, J. S. (2025). A multivocal literature review of cross-chain bridge architectures, their exploits, and countermeasures. Retrieved from www.sciencedirect.com/science/article/pii/S20967 20925000429

[17] OWASP. (2025). OWASP Smart Contract Top 10. Retrieved from owasp.org/www-project-smart-contract-top-10/

[18] Pan, X. (2024). A blockchain deep learning framework for construction video summarization and storage. Retrieved from www.sciencedirect.com/science/article/abs/pii/S1 474034623004627

[19] Rabbani, H., et al. (2024). A novel blockchain-based federated lear… (please provide the rest to complete)

[20] Moradi-Pari, E., Tian, D., Bahramgiri, M., Rajab, S. and Bai, S., 2023. Dsrc versus lte-v2x: Empirical performance analysis of direct vehicular communication technologies. IEEE Transactions on Intelligent Transportation Systems, 24(5), pp.4889-4903.

[21] Kakan Chandra Dey, Anjan Rayamajhi, Mashrur Chowdhury, Parth Bhavsar, James Martin, Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation, Transportation Research Part C: Emerging Technologies, Volume 68, 2016.

[22] M. T. Kawser, Md. S. Fahad, S. Ahmed, S. S. Sajjad, and H. A. Rafi, "The Perspective of Vehicle-to-Everything (V2X) Communication towards 5G," International Journal of Computer Science and Network Security, vol. 19, no. 4, 2019

[23] I.Jawhar,N. Mohamed and L. Zhang, "Inter-vehicular Communication Systems, Protocols and Middleware," 2010 IEEE Fifth International Conference on Networking, Architecture, and Storage, Macau, China, 2010, pp. 282-287, doi: 10.1109/NAS.2010.49.

[24] Abdelkader, G.; Elgazzar, K.; Khamis, A. Connected Vehicles: Technology Review, State of the Art, Challenges and Opportunities. *Sensors* 2021, *21*, 7712.

[25] S. Garg et al., "Edge Computing-Based Security Framework for Big Data Analytics in VANETs," IEEE Netw., vol. 33, no. 2, pp. 72–81, Mar. 2019, doi:10.1109/MNET.2019.1800239

Cite this article as:

Mamta Chauhan, Amita Arora and et. al. " Convergence of Block chain and Cyber security: a Systematic Review of Emerging Threats and Advanced Defenses,"Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026.

Displayed as online on 06th July 2026.

Link: http://actsoft.org/science/micro2026-pro/456-micro2026.pdf

ISBN: 978-81-985770-0-9