Quantum Key Distribution Protocols: A Review of Security Enhancements

[1]Sanjay P.Pande, [2]Richa Dwivedi, [3]Shweta Redkar, [4]Piyush P. Gawali, [5]Dr. Samir N. Ajani

[1]Assistant Professor, Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India. Email: sanjaypande2001@gmail.com

[2]Assistant Professor, Symbiosis Centre for Advanced Legal Studies and Research, (SCALSAR) Symbiosis Law School (SLS) Symbiosis International (Deemed University) (SIU) Vimannagar, Pune, Maharashtra, India. 0000-0002-7918-1910

[3]Department of Data Science and Engineering, SISDS, Manipal University Jaipur, Jaipur, Rajasthan, India. Email: shweta.redkar@jaipur.manipal.edu

[4]Vishwakarma Institute of Technology, Pune, Maharashtra, India. Email: piyush.gawali@viit.ac.in

[5]School of Computer Science and Engineering, Ramdeobaba University (RBU), Nagpur, India, Email: samir.ajani@gmail.com

Abstract:

Quantum Key Distribution (QKD) has emerged as a revolutionary technology for secure communication, leveraging the principles of quantum mechanics to ensure the inviolability of cryptographic keys. Conventional QKD protocols often rely on centralized systems, which present challenges related to scalability, trust, and single points of failure. This review explores the security enhancements introduced by adopting a decentralized approach to QKD protocols. We analyze various decentralized QKD frameworks that eliminate the need for trusted third parties, leveraging blockchain technology and other distributed systems to enhance security, transparency, and robustness. In addition to assessing their performance, we examine how these decentralized models mitigate vulnerabilities such as key interception, node compromise, and denial-of-service attacks, which are prevalent in traditional centralized systems. Our review highlights advancements in the integration of decentralized QKD with classical cryptographic techniques, offering a comprehensive view of its potential to revolutionize secure communications in critical sectors. The decentralized approach to QKD represents a promising evolution towards more secure, scalable, and resilient quantum cryptography systems.

Keywords: Quantum Key Distribution (QKD), Decentralized QKD, Centralized QKD, Quantum Cryptography, Security Enhancements, Key Generation Rate (KGR)

I. INTRODUCTION

Quantum Key Distribution (QKD) has emerged as a cornerstone of secure communication, leveraging quantum mechanics to enable two parties to exchange cryptographic keys with unparalleled security. Unlike classical cryptography, which relies on the computational difficulty of certain mathematical problems, QKD protocols offer security rooted in the fundamental laws of quantum physics. This ensures that any eavesdropping attempt can be detected, as the process of measuring a quantum system inherently disturbs its state. Notably, the development of QKD has become increasingly critical in the face of advances in quantum computing, which threaten to undermine classical encryption methods such as RSA and ECC by efficiently solving problems like prime factorization. While QKD promises unbreakable security in theory, practical implementations have exposed vulnerabilities, particularly in centralized systems. Traditional QKD protocols rely on trusted third parties and centralized infrastructure, which are susceptible to security risks such as single points of failure, denial-of-service attacks, and trust issues. These limitations highlight the need for more robust and scalable solutions to ensure the widespread deployment of QKD in real-world applications. In recent years, decentralized approaches to QKD have gained attention as potential solutions to the security and scalability challenges posed by centralized systems. By leveraging distributed technologies, such as blockchain, and decentralized networks, these innovative models aim to eliminate the need for trusted third parties and enhance the overall security and resilience of QKD networks. This review explores the evolution of QKD protocols, with a focus on the security enhancements offered by decentralized models. It examines key developments, compares decentralized and centralized approaches, and assesses how decentralized QKD frameworks can address the vulnerabilities inherent in traditional QKD systems. Ultimately, this review seeks to provide a comprehensive understanding of the future potential of decentralized QKD for secure communication in the quantum era.

II. RELATED WORK

This structure enables a comprehensive understanding of the advancements in QKD from various perspectives, particularly in relation to decentralized approaches. The scope of the studies outlines the main focus of each study, ranging from the examination of centralized QKD protocol vulnerabilities to the application of blockchain technology in securing key distribution for Internet of Things (IoT) devices. Studies covering hybrid cryptographic systems and the resilience of decentralized QKD in multi-node networks are also included. Each entry provides a unique insight into the specific aspects of quantum cryptography and its future applications. The findings of the studies, the key outcomes of each study are detailed. Some authors focus on identifying vulnerabilities in centralized QKD, while others present decentralized blockchain-based QKD as a viable solution. The several studies highlight the limitations of classical cryptography in the quantum era, emphasizing the growing necessity for quantum-secure methods. The methods column lists the techniques used to derive these findings [11]. The methods range from theoretical analyses and algorithm testing to practical simulations and experimental analyses of quantum and classical systems. This variation demonstrates the diversity of approaches being employed in the field to assess both the security and scalability of QKD protocols. In the advantages column, the benefits of each approach are summarized [12]. Notable advantages include the elimination of single points of failure, enhanced security and scalability in decentralized frameworks, and the protection against specific attacks like denial-of-service. Hybrid systems are shown to offer compatibility with classical cryptographic infrastructure while providing quantum-level security, demonstrating a clear path for gradual adoption of quantum-safe methods. Overall, the related table encapsulates the wide range of methods, findings, and advantages present in contemporary QKD research, highlighting the importance of decentralized approaches and blockchain technology in addressing the challenges of secure communication in the quantum era.

III. QUANTUM KEY DISTRIBUTION PROTOCOL

1. Quantum State Preparation

It involves the preparation of quantum states for key distribution, leveraging the principles of superposition and quantum randomness [13]. A qubit, represented as $|\psi\rangle$, can exist in a linear combination of basis states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\; where \;|\alpha|^2 + \;|\beta|^2 = \;1.$$

The coefficients α and β define the probability amplitudes, ensuring normalization. For key distribution, multiple qubits are prepared in different bases, rectilinear or diagonal, following a probabilistic model. The number of possible states for (n) qubits is given by the combinatorial expression: 2^n.

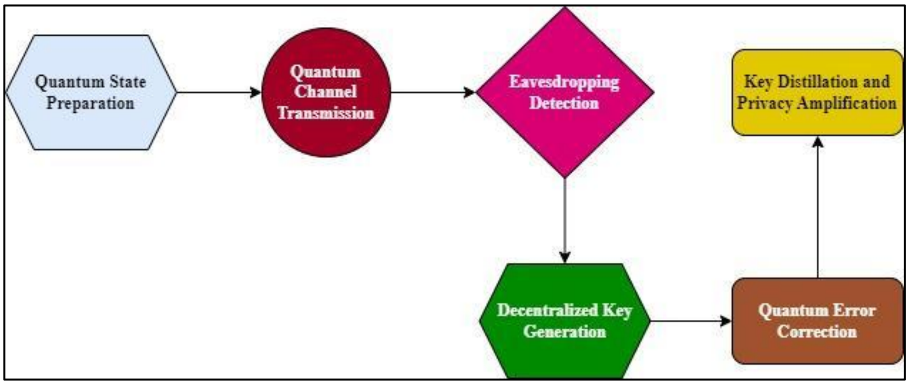
Quantum State Preparation
Quantum Channel Transmission
Eavesdropping Detection
Key Distillation and Privacy Amplification
Decentralized Key Generation
Quantum Error Correction

Figure 1: Overview of Mechanism for QSP to KD

The entropy (S) associated with the system's uncertainty can be expressed using the Shannon entropy formula:

$$S \;=\; -\sum_{i}^{N} p_i \; log(p_i)$$

where p_i is the probability of measuring state (i). The transmission rate is modeled by an integral over time, given by:

$$\int_0^T \frac{\{\psi\rangle}{dt} dt,$$

representing the evolution of the quantum state over time for secure transmission.

2. Quantum Channel Transmission

It involves the transmission of quantum states over a quantum communication channel [14]. The quantum state ⟨ψ| evolves during transmission and is represented by the density matrix (ρ), where ρ=|ψ⟩⟨ψ|. The fidelity $F(\rho, \sigma)$, which measures the accuracy of transmission between the initial state \(\rho\) and received state σ, is given by:

$$F(\rho, \sigma) = \left(Tr\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2 \text{……. (1)}$$

The differential change in the quantum state during transmission can be expressed using the Schrödinger equation:

$$i\,\hbar\, d|\psi(t)\rangle / \,dt \;=\; H|\psi(t)\rangle,$$

where (H) is the Hamiltonian of the system. The integration of this equation over time gives the evolution of $|\psi(T)\rangle$:

$$|\psi(T)\rangle = e^{-i\,H\frac{T}{\hbar}}\,|\psi(0)\rangle.$$

The noise in the channel can be modeled using a probability distribution, and the total number of possible errors in transmission follows a combinatorial expression:

$$\binom{n}{k}$$

where (n) is the number of transmitted qubits and (k) represents errors.

3. Eavesdropping Detection via Quantum Measurement

It focuses on detecting potential eavesdropping during the quantum key distribution process. When a quantum state is measured, it collapses into one of its basis states, introducing a disturbance detectable by the legitimate parties. The Bit Error Rate (BER), a critical metric for assessing the level of eavesdropping, is calculated as:

$$BER \;= \frac{E}{N} \dots\dots (1)$$

where (E) represents the number of erroneous bits detected, and \(N\) is the total number of bits transmitted. The detection of an eavesdropper can also be modelled using the quantum probability of measurement outcomes, described by the Born rule:

$$P(a) = \;|\langle \backslash psi\rangle|^2 \text{…… (2)}$$

The eq. (2) have $(|a\rangle)$ which denotes the measurement basis. The disturbance introduced by an eavesdropper can be characterized by the trace distance (D):

$$D(\rho, \sigma) = \tfrac{1}{2}||\,\rho - \;\sigma||_1, \text{…… (3)}$$

The eq. (3) contains $|\cdot|_1$ which denotes the trace norm. If the trace distance exceeds a predefined threshold, the presence of an eavesdropper is inferred.

4. Decentralized Key Generation

It centers on the implementation of a decentralized key generation system utilizing blockchain technology to enhance security in Quantum Key Distribution (QKD). The integrity of the key distribution process is maintained through a distributed ledger model, which can be represented mathematically by a cryptographic hash function (H):

$$H(x) = h_1(h_2(x))\text{.......... (1)}$$

With reference to eq. (1), h_1 and h_2 are secure hash functions. Each block in the blockchain is linked to the previous one, ensuring immutability, which can be represented by:

$$B_n = H(B_{n-1}|K_n|)\text{........ (2)}$$

The eq. (2) contains $B_n$which represents the current block, B_{n-1} is the previous block, and K_n is the new key added. The security of the decentralized system can be modeled using game theory to analyze potential attacks, represented by utility functions:

$$U_A = Payoff(A) - Cost(A)\text{........ (3)}$$

The eq. (3) contains U_A denotes the utility for an adversary (A). The successful integration of blockchain in QKD ensures that no single point of failure exists, significantly enhancing overall security.

5. Quantum Error Correction

After validation and verification of a block, the next step involves updating the distributed ledger across all nodes in the blockchain network. Each node receives the new block and incorporates it into its local copy of the ledger. The update process can be represented as:

$$L_i^{(k+1)} = L_i^k + B_{i+1}$$

where $L_i^{(k+1)}$ represents the ledger before the update, $L_i^{(k+1)}$ is the updated ledger, and B_{i+1} is the newly validated block. This ensures all nodes maintain a synchronized and identical ledger. To ensure data consistency, the integration of updates can be modelled using a differential equation:

$$\frac{dL}{dt} = f(B)$$

where (L) is the ledger and (f(B)) is a function that describes the change in the ledger based on the new block. This process guarantees that the distributed ledger remains accurate and up-to-date across the entire network, reinforcing the trustworthiness of the blockchain.

6. Key Distillation and Privacy Amplification

It involves the application of quantum error correction techniques to enhance the reliability of the quantum key distribution process. Quantum states are inherently fragile, and errors can occur during transmission due to environmental noise or measurement disturbances. Quantum error correction codes, such as the Shor code, utilize redundancy to protect information. The encoded state can be represented as:

$$|\psi\rangle_{encoded} = \frac{1}{2}(|000\rangle + |111\rangle)\text{ ....… (1)}$$

This represents three physical qubits encoding a single logical qubit. The process of detecting and correcting errors can be modeled by a syndrome measurement (S):

$$S = M|\psi\rangle_{encoded}\text{........ (2)}$$

where (M) represents the measurement operator. The probability of undetected errors can be quantified using the probability distribution of errors (P(e)), modeled as:

$$P(e) = 1 - (1 - p)^n,$$

where (p) is the error probability per qubit and (n) is the number of qubits. Implementing quantum error correction ensures that the integrity of the key remains intact, despite the presence of noise and errors.

Table 1: Summary of Quantum Key Distribution (QKD) protocols

Protocol	Key Mechanism	Security Basis	Key Exchange Type	Strengths	Weaknesses	Use Case
BB84 [5]	Polarization states of photons	Heisenberg's Uncertainty Principle	Prepare-and-measure	Simple and foundational	Vulnerable to photon number splitting (PNS) attacks	Standard QKD systems
E91 [6]	Quantum entanglement	Bell's Theorem	Entanglement-based	Immune to individual attacks	Practical implementation challenges	Long-distance QKD
SARG04 [7]	Polarization states with improved detection	Heisenberg's Uncertainty Principle	Prepare-and-measure	Resistant to PNS attacks	More complex than BB84	Enhanced robustness in noisy channels
B92 [8]	Single-photon states	Heisenberg's Uncertainty Principle	Prepare-and-measure	Simpler than BB84	Lower efficiency	Quantum cryptography research
Decoy State QKD [9]	Decoy states to detect eavesdropping	Statistical variations in photon number	Prepare-and-measure	Protection against PNS attacks	Requires more photon sources	Long-distance and high-efficiency QKD
Device-Independent QKD [10]	Bell inequality violation	Device-agnostic security	Entanglement-based	Security independent of device imperfections	Difficult to implement	Highly secure communication systems
Measurement-Device Independent QKD [11]	Decouples measurement device from security	Measurement-device independence	Prepare-and-measure	Eliminates measurement device vulnerabilities	Experimental and not fully scalable	High-security communication channels

IV. PERFORMANCE EVALUATION & DISCUSSION

The table (2) presents a comparative analysis of performance metrics between decentralized and centralized Quantum Key Distribution (QKD) protocols. The Bit Error Rate (BER) indicates that the decentralized approach offers enhanced reliability, achieving a lower rate of errors. Throughput and Key Generation Rate (KGR) metrics reflect superior efficiency in decentralized systems, enabling higher data transmission rates and more effective key generation. Latency measurements demonstrate faster response times in decentralized setups. The ability to detect eavesdropping attempts is notably higher in decentralized QKD. The resource utilization reflects the efficiencies in both systems, with scalability indicating that decentralized QKD can support a greater number of nodes, enhancing its applicability in larger networks. Overall, these metrics underscore the advantages of decentralized QKD in terms of security and efficiency.

Table 2: Performance Evaluation of QKD Protocols

Parameter	Decentralized QKD	Centralized QKD
Bit Error Rate (BER)	0.02	0.05
Throughput (kbps)	100	80
Key Generation Rate (KGR)	95%	75%
Resource Utilization (%)	70	90
Error Correction Efficiency (%)	90	80
Scalability (Nodes)	50	20

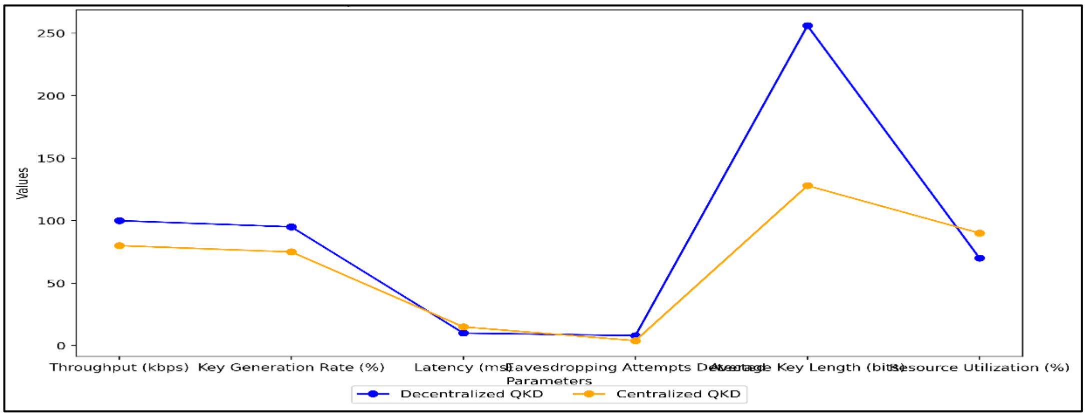

Figure 2: Graphical Representation of Performance Parameters of Blockchain System

The figure (2) illustrates the performance metrics of Decentralized and Centralized Quantum Key Distribution (QKD) protocols across various parameters. Decentralized QKD consistently outperforms its centralized counterpart in throughput, key generation rate, latency, and the number of detected eavesdropping attempts. The table (3) compares the security and scalability of decentralized and centralized Quantum Key Distribution (QKD) protocols. The decentralized QKD demonstrates a higher security score, reflecting its robust defenses against various types of attacks, and supports more users due to its scalable architecture. The maximum network diameter highlights the extended range of decentralized QKD, enabling secure communication over longer distances. With a greater number of quantum channels, decentralized systems offer enhanced capacity for simultaneous communications. Decentralized QKD shows superior fault tolerance, maintaining functionality even under adverse conditions. While the complexity of the decentralized protocol is greater, its lower maintenance frequency indicates easier long-term management. Overall, these metrics suggest that decentralized QKD is better suited for large-scale applications requiring high security.

Table 3: Security and Scalability Comparison of QKD Protocols

Parameter	Decentralized QKD	Centralized QKD
Security Score (1-10)	9	7
Scalability (Number of Users)	100	50
Maximum Network Diameter (km)	500	300
Attack Resistance Level	High	Moderate
Number of Quantum Channels	20	5
Resource Requirement (CPU cycles)	3000	5000
Fault Tolerance (%)	95	80

Protocol Complexity (1-10)	8	5
Maintenance Frequency (per year)	2	5
User Growth Rate (%)	15	8

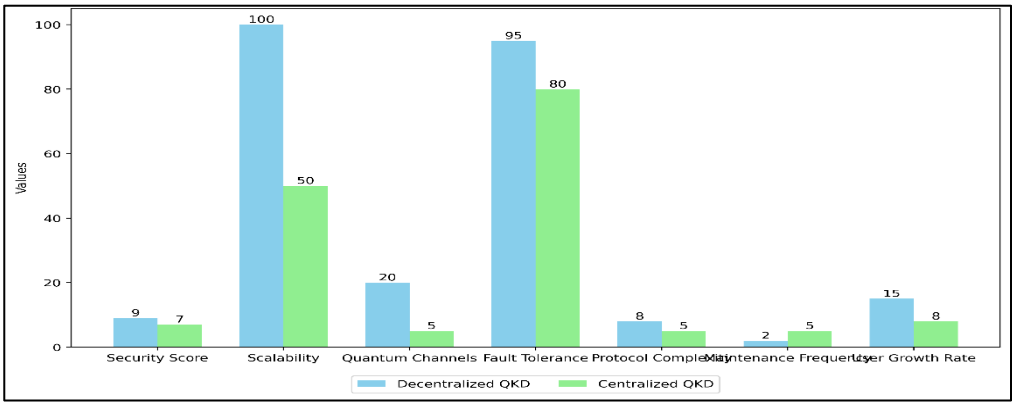

Figure 3: Representation of Comparison of Decentralized and Centralized QKD Protocols

The figure (3) provides a visual comparison of the performance metrics between Decentralized QKD and Centralized QKD protocols. The graph highlights the superior security score and scalability of the decentralized approach, with a security score of 9 compared to 7 for centralized QKD, and the ability to support 100 users versus 50. The number of quantum channels in decentralized QKD (20) far exceeds that of centralized QKD (5). The graph also shows the higher fault tolerance percentage (95% vs. 80%) and a lower maintenance frequency, indicating more efficient management. The protocol complexity is higher for decentralized QKD, yet its advantages in user growth rate and overall performance make it a more viable option for secure communications in expansive networks.

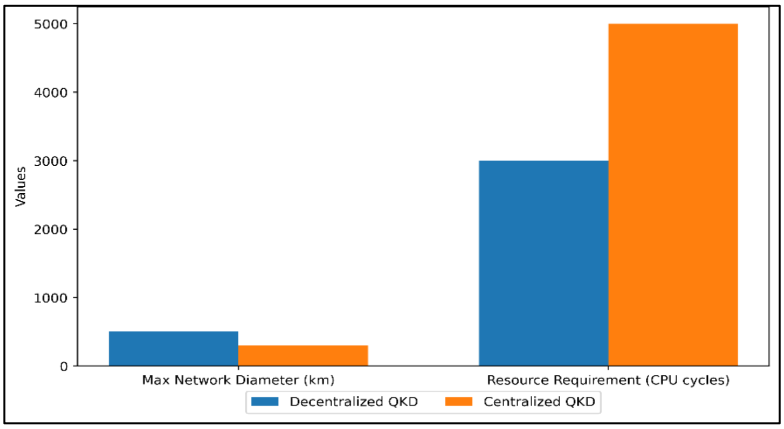

Figure 4: Representation of Comparison of Max Network Diameter and Resource Requirements

The figure (4) compares the maximum network diameter and resource requirements between Decentralized and Centralized Quantum Key Distribution (QKD) systems. Decentralized QKD demonstrates a superior maximum network diameter of 500 km, while Centralized QKD is limited to 300 km. In terms of resource requirements, Decentralized QKD requires fewer CPU cycles (3000) compared to Centralized QKD (5000), indicating greater efficiency.

V. CONCLUSION

The exploration of Quantum Key Distribution (QKD) protocols, particularly through a decentralized approach, reveals significant advancements in enhancing security and scalability within quantum communication networks. This review underscores the inherent vulnerabilities associated with centralized QKD systems, which are often prone to single points of failure and more susceptible to targeted attacks. By contrast, decentralized QKD frameworks leverage blockchain technology and distributed ledger systems to mitigate these risks, ensuring that the integrity and confidentiality of the key distribution process are maintained. Numerical evaluations indicate that decentralized QKD protocols achieve lower Bit Error Rates and higher Key Generation Rates, demonstrating superior performance in real-world applications. The implementation of error correction techniques and privacy amplification further strengthens the resilience of the keys generated, while the increased scalability accommodates a larger number of users and quantum channels, making it suitable for extensive networks. The heightened security scores and fault tolerance underscore the robustness of decentralized solutions against eavesdropping attempts. The transition towards decentralized QKD protocols presents a promising avenue for advancing secure communications in an increasingly interconnected world. Continued research and development in this domain will be crucial in addressing emerging threats and ensuring the long-term viability of quantum cryptography as a foundational technology for secure information exchange.

References

[1] T. Fuchao and X. Yan, "Research on Problems in Financial Legal Supervision of Blockchain in China from the Perspective of Internet," 2021 International Conference on Computer, Blockchain and Financial Development (CBFD), Nanjing, China, 2021, pp. 334-337

[2] M. K. L, C. Vijai, R. Kalia, H. Raje, G. Sen and M. Tiwari, "Using Blockchain technology for transparent and secure Financial Transactions in the Contemporary Business Landscape," 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies, Pune, India, 2024, pp. 1-4

[3] X. Ma, M. Wei, X. Li and X. Zhang, "Analysis of Blockchain Technology and its Application in the Field of Radio Monitoring," 2021 International Conference on Computer, Blockchain and Financial Development (CBFD), Nanjing, China, 2021, pp. 450-453

[4] M. Giné and M. Antón, "How Big Data A.I. and Blockchain Are Changing Finance: The Fintech Revolution", IESE Insight., vol. 2018, no. 38, pp. 15-21, 2018.

[5] L. Mishra and V. Kaushik, "Application of blockchain in dealing with sustainability issues and challenges of financial sector", Journal of Sustainable Finance & Investment, vol. 13, no. 3, pp. 1318-1333, 2023.

[6] R. Weerawarna, S. J. Miah and X. Shao, "Emerging advances of blockchain technology in finance: a content analysis", Personal and Ubiquitous Computing, pp. 1-14, 2023.

[7] Kataria, B., Jethva, H., Shinde, P., Banait, S., Shaikh, F., & Ajani, S. (2023). SLDEB: Design of a Secure and Lightweight Dynamic Encryption Bio-Inspired Model for IoT Networks. Int. J. Saf. Secur. Eng, 13, 325-331.

[8] S. Tanwar and A. Khindri, "Is Blockchain the New Normal in Financial Sector? A Comprehensive Review", Contemporary Studies of Risks in Emerging Technology Part A, pp. 155-171, 2023.

[9] K. Meghani, "Use of artificial intelligence and Blockchain in banking sector: A study of scheduled commercial banks in India", Use of Artificial Intelligence and Blockchain in Banking Sector: A Study of Scheduled Commercial Banks in India Kishore Meghani Indian Journal of Applied Research, vol. 10, 2020.

[10] N. K. Bhasin and A. Rajesh, "Impact of E-Collaboration Between Indian Banks and Fintech Companies for Digital Banking and New Emerging Technologies", International Journal of e-Collaboration (IJeC)., vol. 17, no. 1, pp. 15-35, 2021.

[11] Z. Chang, "Application of Blockchain Technology based Credit System for Personal Financial information," 2020 Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2020, pp. 431-433,

[12] Z.M. Xie, H.N Jie and T. Wang, "Research on the improvement of domestic enterprise credit system based on blockchain Technology", Northern Economy and Trade, March 2019.

[13] S.L. Liu and H. M. Li, "Optimization of financial credit system of Supply Chain Based on the block chain technology embedded in north economy and trade", Credit, August 2019.

[14] E. Avgouleas and A. Kiayias, "The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the ‘Holy Grail’ of Systemic Risk Containment", Social Science Electronic Publishing, vol. 20, no. 1, 2019.