iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65466

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

Advancement and Innovation in Blockchain and Cryptography: A Comparative Analysis of Traditional Systems and Emerging Solutions

Supriya B K[1], Shubha B K[2], Prajwal M N[3], Vikas C M[4], B J Jaydeva[5], Ravi J Gowda[6], Sushmitha K P[7], Anup Ravi Ghulanoor[8]

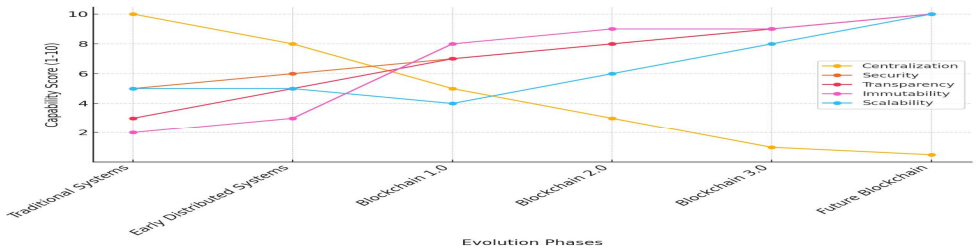
[1]*Department of Information Science Engineering, PES College of Engineering, Mandya, Karnataka, India*
[2]*Department of Computer Science Engineering, SDM Institute of Technology Ujiri, Karnataka, India*
[3]*Department of AIML, PES College of Engineering, Mandya, Karnataka, India*
[4]*Research Lead, Zakthi Innovation Lab, Davanagere*
[5]*Department of Electrical and Electronics Engineering, PES College of Engineering, Mandya, Karnataka, India*
[6]*Department of Computer Science Engineering, PES College of Engineering, Mandya, Karnataka, India*
[7]*Department of Electronics and Communication Engineering, PES College of Engineering, Mandya, Karnataka, India*
[8]*Department of Electronics and Communication Engineering, PDA College of Engineering, Kalburgi, Karnataka, India*

Abstract: ***The rise of blockchain technology and cryptography has transformed industries by enhancing security, transparency, and trust. This paper provides a comparative analysis of traditional systems and emerging solutions, focusing on the advances in blockchain and cryptography. Key innovations, challenges, and future trends are discussed. The review leverages research from multiple sources, offering a broad perspective on these fields.This paper explores the rapid advancements in blockchain technology and cryptography, comparing traditional systems with cutting-edge solutions. It highlights the evolution of consensus mechanisms, encryption methods, and their impact on scalability, security, and efficiency. By analyzing key innovations such as zero-knowledge proofs and homomorphic encryption, the study offers insights into overcoming existing limitations like high energy consumption and interoperability issues. The paper provides a comparative analysis of emerging solutions against conventional approaches, showcasing their potential to revolutionize industries. Finally, it outlines the challenges that must be addressed for mainstream adoption.***

Keywords: Blockchain, Cryptography, Decentralization, Security, Transparency, Traditional Systems, Emerging Solutions.

I. INTRODUCTION

Blockchain and cryptography have transformed data protection and transaction verification in a variety of industries. Cryptography has traditionally been used for secure communication, and blockchain provides decentralized ledger systems. Recent developments show promising solutions for enhancing system robustness, privacy, and efficiency [1][2]. Blockchain and cryptography have revolutionized the way we secure, share, and verify data across decentralized networks, offering unprecedented transparency and trust. As traditional systems struggle with inefficiencies, security vulnerabilities, and centralized control, blockchain presents an innovative alternative through distributed consensus and encryption. This comparative analysis delves into the advancements in blockchain technologies and cryptographic algorithms, highlighting their potential to reshape industries while addressing inherent limitations. By exploring emerging solutions, the study evaluates how these technologies outperform conventional methods in security, scalability, and privacy. Together, blockchain and cryptography pave the way for a future of secure, decentralized digital ecosystems.



Graph 1: Evolution of Blockchain from Traditional Systems

Table 1: Comparative Overview of Cryptographic Techniques Used in Traditional vs. Emerging Systems

Feature	Traditional Systems	Emerging Systems
Algorithms	RSA	Post-Quantum Cryptography
	AES (Advanced Encryption Standard)	- Lattice-based cryptography
	ECC (Elliptic Curve Cryptography)	- Hash-based signatures
	- SHA-256 (Secure Hash Algorithm)	- Multivariate polynomial cryptography
		- Supersingular isogeny-based encryption
Key Exchange	Diffie-Hellman (DH)	- Quantum Key Distribution (QKD)
	- RSA-based key exchange	- Lattice-based key exchange
Signature Schemes	RSA-based digital signatures	- Post-quantum digital signatures
	- DSA (Digital Signature Algorithm)	Zero-knowledge proofs (ZKP)
	- ECDSA (Elliptic Curve Digital Signature)	BLISS (Lattice-based signatures)
Security Foundation	Computational hardness of factoring integers	- Quantum-resistant mathematical problems
	- Discrete logarithms	- Assumptions about quantum-safe constructions
Vulnerability to Quantum Computing	Vulnerable (RSA, ECC, DH)	Designed to resist quantum attacks
Applications	- Internet communications, banking, etc.	- Blockchain, IoT, quantum networks
Performance	Well-optimized for current hardware	- Often slower but more secure for future needs
Future-proofing	Not quantum-safe	- Built for resistance to quantum computing

II. TRADITIONAL CRYPTOGRAPHIC SYSTEMS

Traditional cryptography, including symmetric and asymmetric algorithms, has been the cornerstone of secure communications for decades. However, with the advent of quantum computing, these systems are vulnerable to being compromised[3][4].

Traditional cryptographic systems, such as AES and RSA, have long provided secure communications and data security. However, they confront obstacles like as key management, vulnerability to attacks, and scalability concerns. The rise of quantum computing poses additional risks, prompting a need for innovative solutions. As a result, the cryptographic landscape is evolving, with emerging technologies like blockchain and post-quantum cryptographic algorithms offering new approaches to secure data transactions in an increasingly complex digital environment.

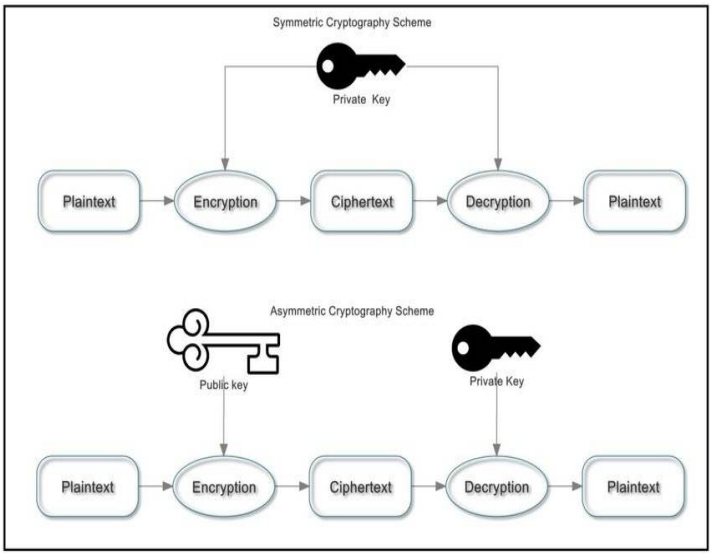


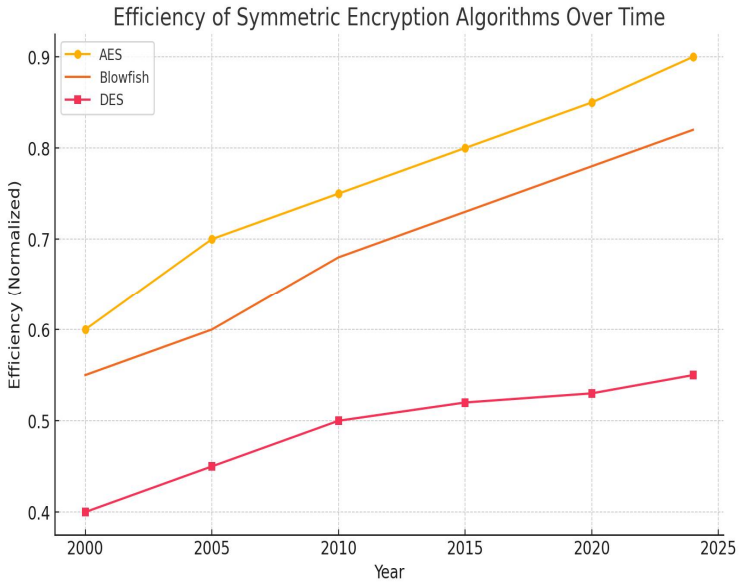
Table 2: Cryptographic Techniques and Their Key Properties (e.g., AES, RSA, ECC) [5]

Cryptographic Technique	type	Key Length	Security Level	Use Cases	Performance
AES(Advanced Encryption Standard)	Symmetric Key	128,192,256 bits	High	Data encryption files,databases, VPNs	Fast(hardware optimized)
RSA(Rivest Shamir Adleman)	Asymmetric Key	Typically 2048 bits or more	High	Security data transmission, digital signature	Slower compare to symmetric algorithms
ECC(Elliptic Curve Cryptography)	Asymmetric Key	256 bits(equivalent to 3072-bit RSA)	Very High	Security communications ,IoT devices	Faster and less resource-intensive than RSA
SHA-256 (Secure Hash Algorithm 256-bit)	Hash Function	N/A	High	Data integrity verification, digital signatures	Fast,but slower than SHA-1
Blowfish	Symmetric Key	32 to 448 bits	Moderate	File encryption, securing network communications	Fast(especially for small data)

Twofish	Symmetric Key	128,192,256 bits	High	Encryption of data at rest,secure applications	Fast and versatile
Triple DES	Symmetric Key	112 0r 168 bits	Moderate	Legacy systems, financial transactions	Slower than AES

A. Symmetric Encryption

Symmetric encryption utilizes the same key for both encryption and decryption. Although efficient, the challenge lies in secure key management[6].



Graph 2: Efficiency of Symmetric Encryption over Time

B. Asymmetric Encryption

Asymmetric encryption relies on public and private keys, providing better security for communications but at a computational cost[7][8].

1) Enhanced Security Through Public-Key Infrastructure: Asymmetric encryption utilizes a pair of keys—public and private—enabling secure data transmission without the need for prior key exchange. This advancement provides a robust foundation for secure communications in blockchain systems, where maintaining confidentiality and integrity is paramount[7].

2) Facilitation of Digital Signatures: The asymmetric encryption model supports digital signatures, which authenticate the origin and integrity of a message. This feature is essential in blockchain technology, ensuring that transactions are verifiable and non-repudiable, thus enhancing trust among participants in decentralized networks[8].

3) Scalability and Flexibility: Asymmetric encryption offers scalable solutions that can adapt to the evolving demands of blockchain applications. This flexibility allows for improved integration with various emerging technologies, facilitating innovative approaches to secure data sharing and identity management across diverse platforms[7][8].

III. BLOCKCHAIN TECHNOLOGY

Blockchain has emerged as a transformative technology due to its decentralized nature and secure verification mechanisms[9]. The blockchain ledger enables secure and transparent transactions without the need for a central authority. This section explores blockchain architecture and consensus algorithms.

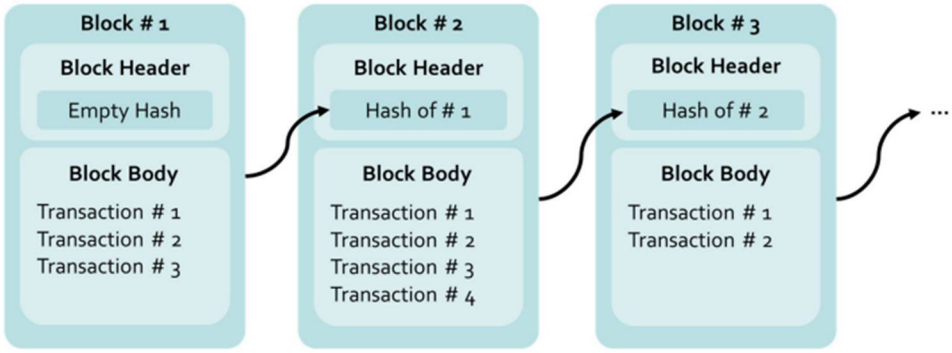


Diagram 2: Typical Blockchain Architecture

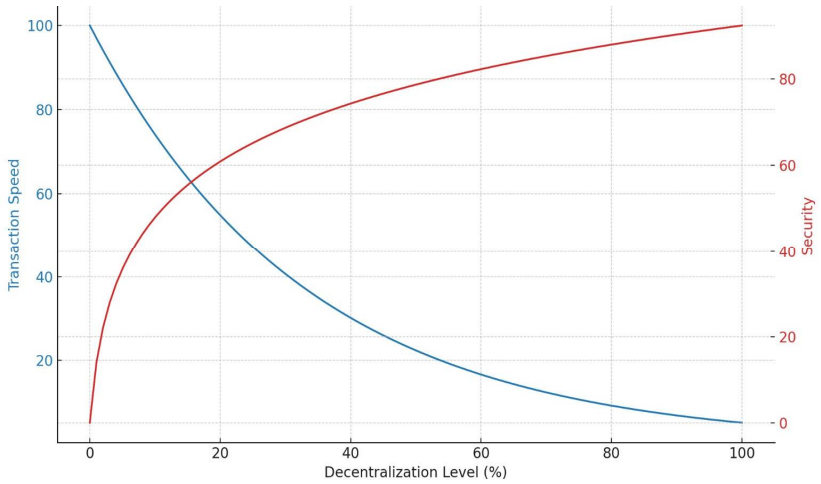
Table 3: Blockchain Consensus Algorithms and Their Features (PoW, PoS, DPoS) [11]

Consensus Algorithm	Key Features	Energy Efficiency	Scalability	Security	Examples of Use
Proof of Work (PoW)	Requires miners to solve complex cryptographic puzzles; high computational effort	Very Low	Limited	High due to decentralization and mining competition	Bitcoin, Litecoin
Proof of Stake (PoS)	Validators are chosen based on the number of tokens they hold; less energy usage	High	Moderate	Secure but depends on token distribution	Ethereum 2.0, Cardano
Delegated PoS (DPoS)	Users vote for a small number of delegates to validate transactions	High	High	Moderate, as the number of validators is smaller	EOS, Tron
Hybrid (PoW & PoS)	Combines PoW for block creation and PoS for transaction validation	Moderate	High	Combines strengths of PoW and PoS	Decred, Hcash
Practical Byzantine Fault	Consensus is achieved	Very High	High	High, especially in	Hyperledger Fabric,

Tolerance (PBFT)	through a voting system among known validators			private/permissioned networks	Tendermint

A. Decentralization and Trust

One of the key advantages of blockchain is the decentralized architecture that eliminates the need for a trusted third party[11][12]. However, this also introduces challenges in terms of scalability and energy consumption[13][14].



Graph 3: Impact of Decentralization on Transaction Speed and Securit.

B. Consensus Algorithms

Proof of Work (PoW) and Proof of Stake (PoS) have different benefits and drawbacks, with newer consensus mechanisms aiming to improve efficiency[15].

Proof of Stake (PoS) is a consensus mechanism that enhances scalability and energy efficiency in blockchain networks by allowing validators to create new blocks and confirm transactions based on the number of coins they hold and are willing to "stake" as collateral, thereby reducing the computational burden compared to traditional Proof of Work (PoW) systems[15].

Table 4: PoW vs. PoS Comparative Analysis[16][17]

Criteria	Proof of Work(PoW)	Proof of Stake (PoS)
Energy Use	High due to mining	Low,no mining needed
Security	Based on computational power	Based on staked assets
Speed	Slower,energy-intensive	Faster,efficient validation
Scalability	Limited	More scalable
Environmental Impact	Significant	Minimal
51% Attack	Vulnerable if 51% mining power is controlled	Vulnerable if 51% of stake is controlled

IV. INTEGRATION OF CRYPTOGRAPHY IN BLOCKCHAIN

Blockchain technology leverages cryptographic techniques to ensure security and privacy. This section highlights the synergy between blockchain and cryptographic protocols such as hashing and digital signatures[18].

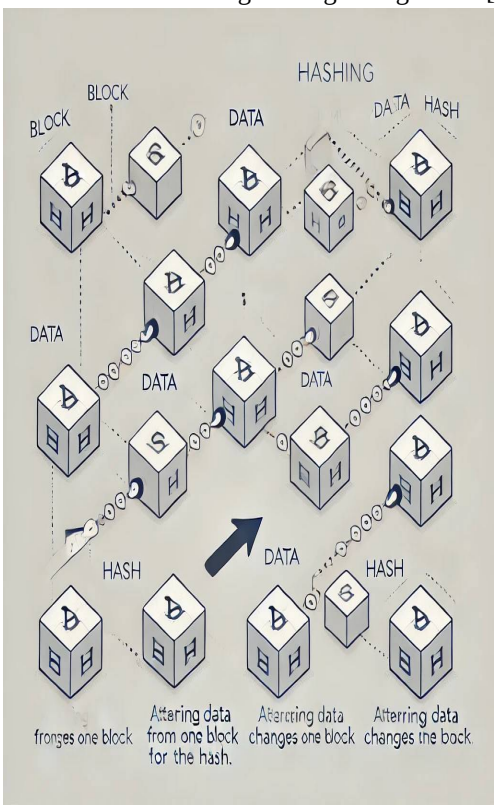


Diagram 3: Role of Hashing in Blockchain Verification

Table 5: Cryptographic Techniques Used in Blockchain Networks (SHA-256, ECDSA)

Cryptographic Technique	Description	Usage in Blockchain	Advantages	Disadvantages
SHA-256	A cryptographic hash function that generates a fixed 256-bit hash from any input data.	Used for creating block hashes and ensuring data integrity in transactions.	- High collision resistance - Fast computation	-Vulnerable to quantum attacks (theoretical)
ECDSA (Elliptic Curve Digital Signature Algorithm)	A public key cryptography method that uses elliptic curves to create digital signatures.	Provides authentication and integrity for transactions by verifying signatures.	- Shorter keys for equivalent security - Efficient for resource-constrained environments	- More complex than traditional signatures (like RSA)

V. EMERGING SOLUTIONS AND INNOVATIONS

Recent advancements in cryptography and blockchain have led to novel solutions, including quantum-resistant cryptography and Layer 2 scaling solutions for blockchain[19][20].

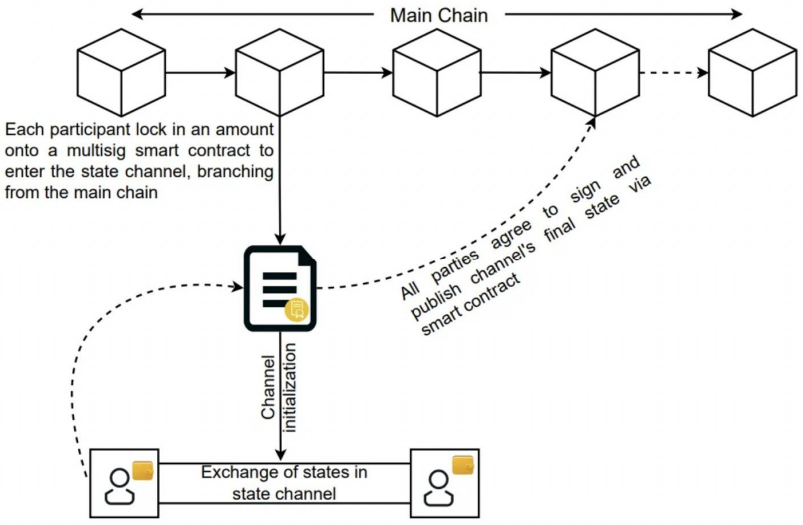
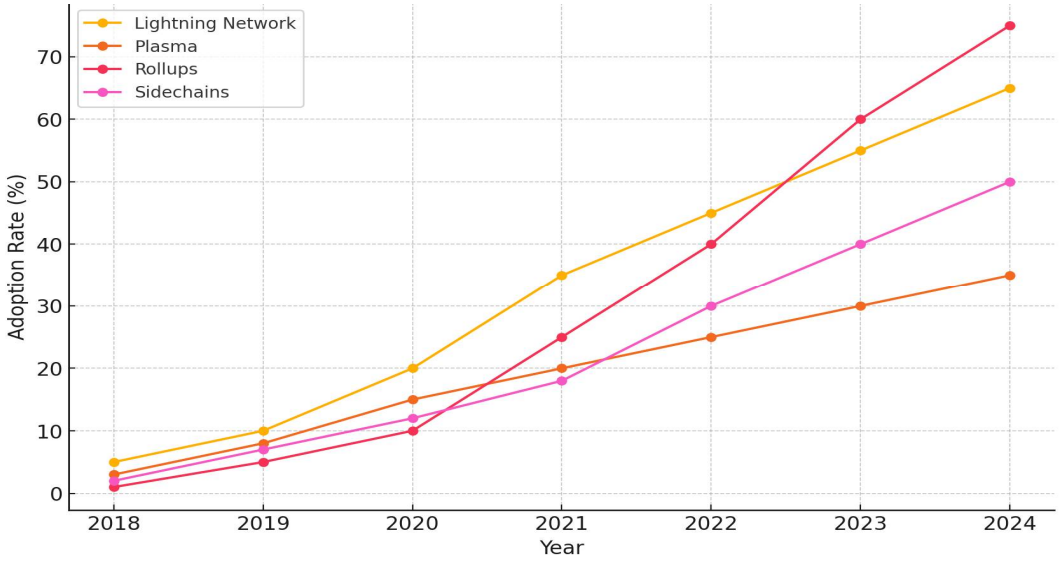


Diagram 4: Layer 2 Solutions in Blockchain (e.g., Lightning Network, Plasma)



Graph 4: Adoption Rate of Emerging Blockchain Solutions

A. Post-Quantum Cryptography

As quantum computing threatens traditional encryption, post-quantum cryptographic algorithms are under development to resist quantum attacks[21][22].

Table 6: Comparison of Traditional Cryptography and Quantum-Resistant Algorithms

Feature	Traditional Cryptography	Quantum-Resistant Algorithms
Security Basis	Relies on the hardness of mathematical problems (e.g., RSA,	Designed to resist attacks from quantum computers (e.g., Lattice-

	ECC, AES)	based, Hash-based)
Vulnerability	Vulnerable to Shor's and Grover's quantum algorithms, which can break RSA & ECC	Resistant to known quantum algorithms, offering higher security in a post-quantum era
Key Size	Shorter keys, e.g., RSA (2048-4096 bits), ECC (256-512 bits)	Requires significantly larger key sizes for equivalent security levels
Performance	Well-optimized and faster for current systems	Relatively slower due to complex mathematical structures, but optimizations are ongoing
Current Usage	Widely used in web security, financial transactions, and data encryption	Not yet widely adopted but gaining interest for future-proofing cryptographic systems
Longevity	May become obsolete with advancements in quantum computing	Expected to remain secure even in the presence of powerful quantum computers

B. Interoperability and Cross-Chain Communication

Emerging solutions also focus on improving interoperability between different blockchain networks[23][24].

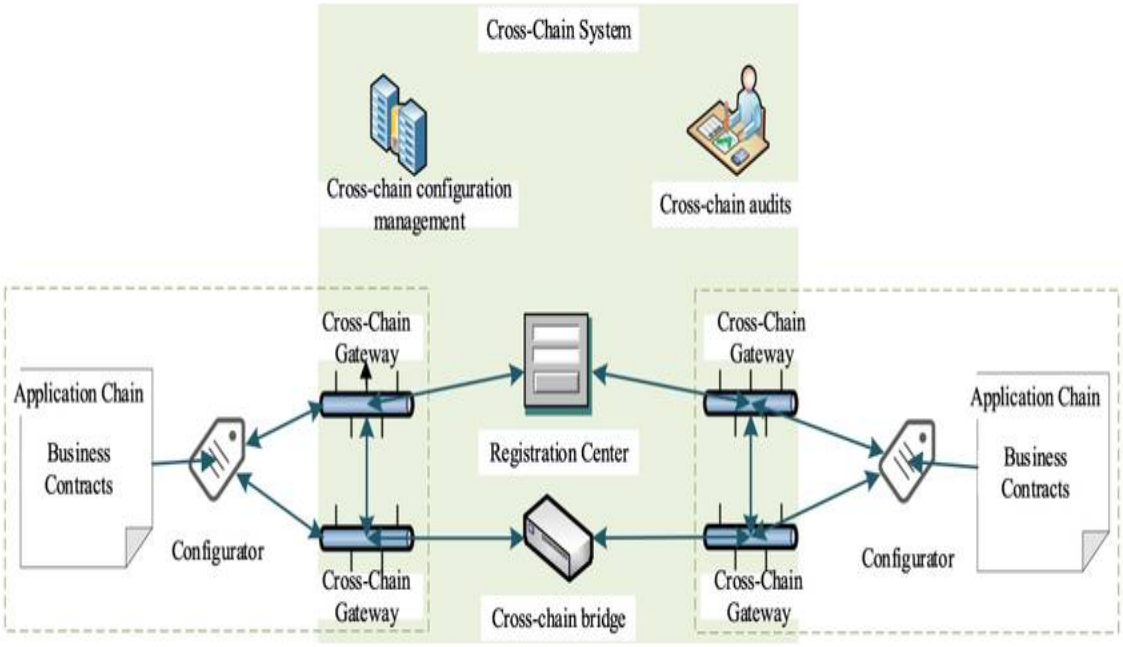


Figure 5: Cross-Chain Communication Framework

VI. APPLICATIONS IN VARIOUS SECTORS

Blockchain and cryptography have broad applications across finance, healthcare, supply chain, and government sectors. This section presents a comparative analysis of how traditional cryptographic systems and emerging blockchain-based solutions address these sectors' security and privacy challenges[25].

Table 7: Use Cases of Blockchain in Various Industries[26][27]

Industry	Use Case	Description
Healthcare	Patient Data Management	Ensures secure, immutable storage and sharing of patient records[26]
Supply Chain	Product Tracking and Traceability	Enables real-time product tracking, reducing fraud and ensuring authenticity[27].
Finance	Smart Contracts for Transactions	Automates contract execution and reduces the need for intermediaries[26].
Energy	Decentralized Energy Trading	Facilitates peer-to-peer energy trading without relying on traditional utilities[27].
Government	Voting Systems	Provides transparent, tamper-proof digital voting solutions for elections[26].

VII. CHALLENGES AND LIMITATIONS

While blockchain and cryptography offer significant potential, they face scalability, energy consumption, and privacy challenges[28][29]. This section discusses these limitations and potential solutions.

Challenges and Limitations in Blockchain and Cryptography:

1) Scalability Concerns: The inability to scale networks to handle an increasing volume of users and transactions without sacrificing speed is one of the main issues with blockchain. Because of their high computational and resource needs, traditional consensus techniques such as, Proof of Work (PoW) and Proof of Stake (PoS) might impede scalability [28][29].

2) Energy Consumption: Many consensus algorithms, especially PoW, demand significant energy resources, leading to unsustainable power consumption and environmental concerns, which remain a major limitation in decentralized systems[28]

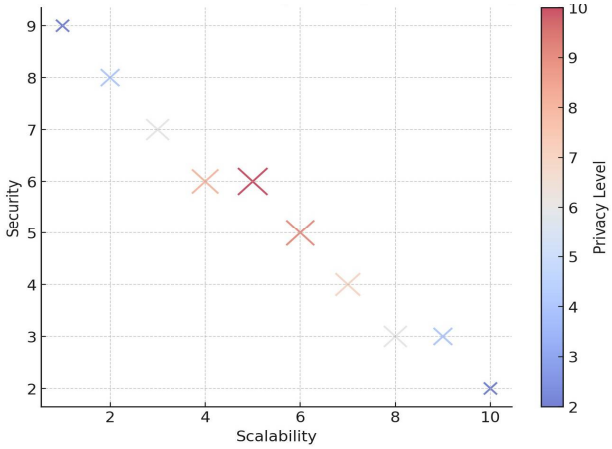
3) Security Vulnerabilities: While blockchain and cryptography offer robust security mechanisms, vulnerabilities still exist in the form of attacks such as 51% attacks, double-spending, and front-running. Advanced cryptographic protocols need further development to mitigate these risks[29].

4) Transaction Latency: Blockchain systems often suffer from delays in transaction validation due to the time taken to achieve consensus, leading to a bottleneck in high-frequency transaction environments like financial markets[28].

5) Interoperability Issues: Widespread adoption is hampered by the incompatibility of various blockchain platforms with conventional systems. It's still difficult to bridge the gap between emerging decentralized technology and well-established centralized solutions [29].

6) Complexity in Cryptographic Algorithms: Although integrating sophisticated cryptographic techniques, such homomorphic encryption or zero-knowledge proofs, improves security and privacy, it also adds complexity and computational overhead, which degrades usability and efficiency [28].

7) Regulatory and Legal Constraints: Blockchain and cryptography have advanced, but regulatory issues and legal ambiguities prevent widespread implementation, particularly when it comes to data privacy, user identification, and jurisdictional law compliance [29].



Graph 6: Trade-offs Between Security, Privacy, and Scalability in Emerging Solutions[30][31]

VIII. FUTURE TRENDS

The incorporation of artificial intelligence, the Internet of Things (IoT), and the ongoing investigation of quantum-resistant encryption are examples of future developments in blockchain and cryptography [32][33].

1) Decentralized Finance (DeFi) Growth: It is anticipated that decentralized banking platforms will continue to grow in popularity since they allow users to do business directly, bypassing middlemen, hence expanding financial inclusion and lowering transaction costs [32].

2) Integration of Blockchain with IoT: Blockchain and Internet of Things (IoT) technologies will work together to increase security and transparency in IoT devices, enabling safe data exchange and better smart contract administration [33].

3) Enhanced Privacy Solutions: Improvements in cryptographic methods like homomorphic encryption and zero-knowledge proofs will give consumers more security and privacy while engaging on blockchain platforms as worries about data privacy increase [38].

4) Tokenization of Assets: The tokenization of real-world assets, including real estate and art, is anticipated to streamline ownership transfer and create new investment opportunities, driving further adoption of blockchain technology[39].

5) Interoperability Between Blockchains: In order to facilitate smooth transactions and data exchange across several platforms, future advancements are probably going to concentrate on improving interoperability between distinct blockchain networks [40].

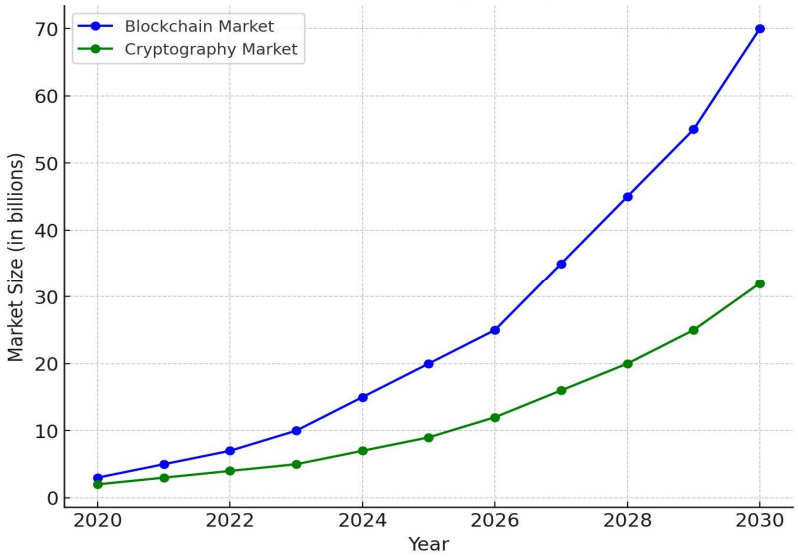
6) Regulatory Frameworks and Standards: We can anticipate the development of thorough regulatory frameworks and industry standards as blockchain use rises, which will offer direction and assistance to companies and developers in making efficient use of blockchain solutions[32].

7) Sustainable Blockchain Solutions: There is a growing emphasis on developing eco-friendly blockchain technologies that minimize energy consumption, leveraging proof-of-stake and other sustainable consensus mechanisms to address environmental concerns[33].

8) Artificial Intelligence (AI) Integration: Blockchain and AI integration may boost data analytics capabilities, streamline decision-making procedures, and produce automated insights in a number of industries, including healthcare, supply chain, and finance [38].

9) Advanced Consensus Mechanisms: Innovations in consensus algorithms will likely lead to more efficient and secure blockchain networks, addressing scalability issues and enhancing transaction speeds[39].

10) Education and Awareness Initiatives: As blockchain technology evolves, educational programs and awareness initiatives will play a crucial role in demystifying the technology for businesses and consumers, promoting wider adoption and understanding of its benefits[40].



Graph 7: Predicted Growth in Blockchain and Cryptography Markets

IX. CONCLUSION

In conclusion, the advancements and innovations in blockchain and cryptography represent a transformative shift in how traditional systems operate, providing enhanced security, transparency, and efficiency. As demonstrated through various studies, including explorations of decentralized identity systems, interoperability challenges, and the integration of privacy-enhancing technologies, the emerging solutions are poised to redefine industries ranging from finance to supply chain management. The comparative analysis of these technologies reveals a significant potential for growth and adoption, driven by the increasing need for secure and efficient data handling in our digital landscape. Furthermore, the ongoing development of quantum-resistant algorithms and sustainable practices underscores the commitment to ensuring long-term viability and ethical standards within the blockchain ecosystem. Ultimately, as these technologies evolve, they promise not only to address current challenges but also to create new opportunities for innovation, collaboration, and economic growth, paving the way for a more secure and interconnected future.

REFERENCES

[1] Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. In Computer Communications (Vol. 169, pp. 179–201). Elsevier B.V. https://doi.org/10.1016/j.comcom.2020.12.028

[2] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A comprehensive review. IEEE Access, 8, 79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579

[3] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. In IEEE Access (Vol. 9, pp. 61048–61073). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3072849

[4] Yadav, A. K. (2021). Significance of Elliptic Curve Cryptography in Blockchain IoT with Comparative Analysis of RSA Algorithm. Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021, 256–262. https://doi.org/10.1109/ICCCIS51004.2021.9397166

[5] Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. International Journal of Information Management, 54. https://doi.org/10.1016/j.ijinfomgt.2020.102120

[6] Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. In Journal of King Saud University - Computer and Information Sciences (Vol. 34, Issue 9, pp. 6719–6742). King Saud bin Abdulaziz University. https://doi.org/10.1016/j.jksuci.2022.03.007

[7] Zhu, P., Hu, J., Li, X., & Zhu, Q. (2023). Using Blockchain Technology to Enhance the Traceability of Original Achievements. IEEE Transactions on Engineering Management, 70(5), 1693–1707. https://doi.org/10.1109/TEM.2021.3066090

[8] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. In IEEE Access (Vol. 7, pp. 117134–117151). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2936094

[9] Proceedings of the 4th International Conference on loT in Social, Mobile, Analytics and Cloud (ISMAC 2020) : 7-9 October 2020. (2020). [IEEE].

[10] Jain, S., Ahuja, N. J., Srikanth, P., Bhadane, K. V., Nagaiah, B., Kumar, A., & Konstantinou, C. (2021). Blockchain and Autonomous Vehicles: Recent Advances and Future Directions. IEEE Access, 9, 130264–130328. https://doi.org/10.1109/ACCESS.2021.3113649

[11] Yadav, A. K., Singh, K., Amin, A. H., Almutairi, L., Alsenani, T. R., & Ahmadian, A. (2023). A comparative study on consensus mechanism with security threats and future scopes: Blockchain. Computer Communications, 201, 102–115. https://doi.org/10.1016/j.comcom.2023.01.018

[12] Zincir-Heywood, Nur. (2020). 16th International Conference on Network and Service Management ; 2nd International Workshop on Analytics for Service and Application Management (AnServApp 2020) ; 1st International Workshop on the Future Evolution of Internet Protocols (IPFuture 2020) : November 2-6, 2020, Virtual Conference. International Federation for Information Processing.

[13] Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., Maddikunta, P. K. R., Fang, F., & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. In Future Generation Computer Systems (Vol. 131, pp. 209–226). Elsevier B.V. https://doi.org/10.1016/j.future.2022.01.017

[14] Sarwar, M. I., Maghrabi, L. A., Khan, I., Naith, Q. H., & Nisar, K. (2023). Blockchain: A Crypto-Intensive Technology - A Comprehensive Review. IEEE Access, 11, 141926–141955. https://doi.org/10.1109/ACCESS.2023.3342079

[15] Proceedings of 2018 4th International Conference on Green Technology and Sustainable Development (GTSD) : November 23rd-24th, 2018, Ho Chi Minh City University of Technology and Education, Vietnam. (2018). IEEE.

[16] Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P. K., & Hong, W. C. (2020). Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. IEEE Access, 8, 474–448. https://doi.org/10.1109/ACCESS.2019.2961372

[17] Thiraviya Suyambu, G., Anand, M., & Janakirani, M. (2020). Blockchain - A most disruptive technology on the spotlight of world engineering education paradigm. Procedia Computer Science, 172, 152–158. https://doi.org/10.1016/j.procs.2020.05.023

[18] Lin, W., Huang, X., Fang, H., Wang, V., Hua, Y., Wang, J., Yin, H., Yi, D., & Yau, L. (2020). Blockchain Technology in Current Agricultural Systems: From Techniques to Applications. IEEE Access, 8, 143920–143937. https://doi.org/10.1109/ACCESS.2020.3014522

[19] Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. In IEEE Access (Vol. 7, pp. 164908–164940). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2950872

[20] Wang, Z., Li, M., Lu, J., & Cheng, X. (2022). Business Innovation based on artificial intelligence and Blockchain technology. Information Processing and Management, 59(1). https://doi.org/10.1016/j.ipm.2021.102759

[21] Majeed, U., Khan, L. U., Yaqoob, I., Kazmi, S. M. A., Salah, K., & Hong, C. S. (2021). Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. In Journal of Network and Computer Applications (Vol. 181). Academic Press. https://doi.org/10.1016/j.jnca.2021.103007

[22] Rajagopal, B. R., Anjanadevi, B., Tahreem, M., Kumar, S., Debnath, M., & Tongkachok, K. (2022). Comparative Analysis of Blockchain Technology and Artificial Intelligence and its impact on Open Issues of Automation in Workplace. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022, 288–292. https://doi.org/10.1109/ICACITE53722.2022.9823792

[23] Ressi, D., Romanello, R., Piazza, C., & Rossi, S. (2024). AI-enhanced blockchain technology: A review of advancements and opportunities. In Journal of Network and Computer Applications (Vol. 225). Academic Press. https://doi.org/10.1016/j.jnca.2024.103858

[24] Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. IEEE Access, 7, 17578–17598. https://doi.org/10.1109/ACCESS.2019.2895302

[25] Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M. Y. M., Koh, L. H., & Yang, L. (2021). Blockchain for Future Smart Grid: A Comprehensive Survey. In IEEE Internet of Things Journal (Vol. 8, Issue 1, pp. 18–43). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/JIOT.2020.2993601

[26] Panwar, A., & Bhatnagar, V. (n.d.). DISTRIBUTED LEDGER TECHNOLOGY (DLT): THE BEGINNING OF A TECHNOLOGICAL REVOLUTION FOR BLOCKCHAIN.

[27] Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Generation Computer Systems, 100, 325–343. https://doi.org/10.1016/j.future.2019.05.023

[28] Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Faizan, M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. IEEE Access, 8, 157959–157973. https://doi.org/10.1109/ACCESS.2020.3019829

[29] Kaur, M., & Gupta, S. (2021). Blockchain Consensus Protocols: State-of-the-art and Future Directions. Proceedings of International Conference on Technological Advancements and Innovations, ICTAI 2021, 446–453. https://doi.org/10.1109/ICTAI53825.2021.9673260

[30] Wustmans, M., Haubold, T., & Bruens, B. (2022). Bridging Trends and Patents: Combining Different Data Sources for the Evaluation of Innovation Fields in Blockchain Technology. IEEE Transactions on Engineering Management, 69(3), 825–837. https://doi.org/10.1109/TEM.2020.3043478

[31] Kassen, M. (2022). Blockchain and e-government innovation: Automation of public information processes. Information Systems, 103. https://doi.org/10.1016/j.is.2021.101862

[32] Moniruzzaman, M., Khezr, S., Yassine, A., & Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. In Computers and Electrical Engineering (Vol. 83). Elsevier Ltd. https://doi.org/10.1016/j.compeleceng.2020.106585

[33] Wang, Q., Su, M., & Li, R. (2020). Is China the world's blockchain leader? Evidence, evolution and outlook of China's blockchain research. In Journal of Cleaner Production (Vol. 264). Elsevier Ltd. https://doi.org/10.1016/j.jclepro.2020.121742

[34] Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. In Journal of King Saud University - Computer and Information Sciences (Vol. 34, Issue 9, pp. 6793–6807). King Saud bin Abdulaziz University. https://doi.org/10.1016/j.jksuci.2021.08.005

[35] Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change, 158. https://doi.org/10.1016/j.techfore.2020.120166

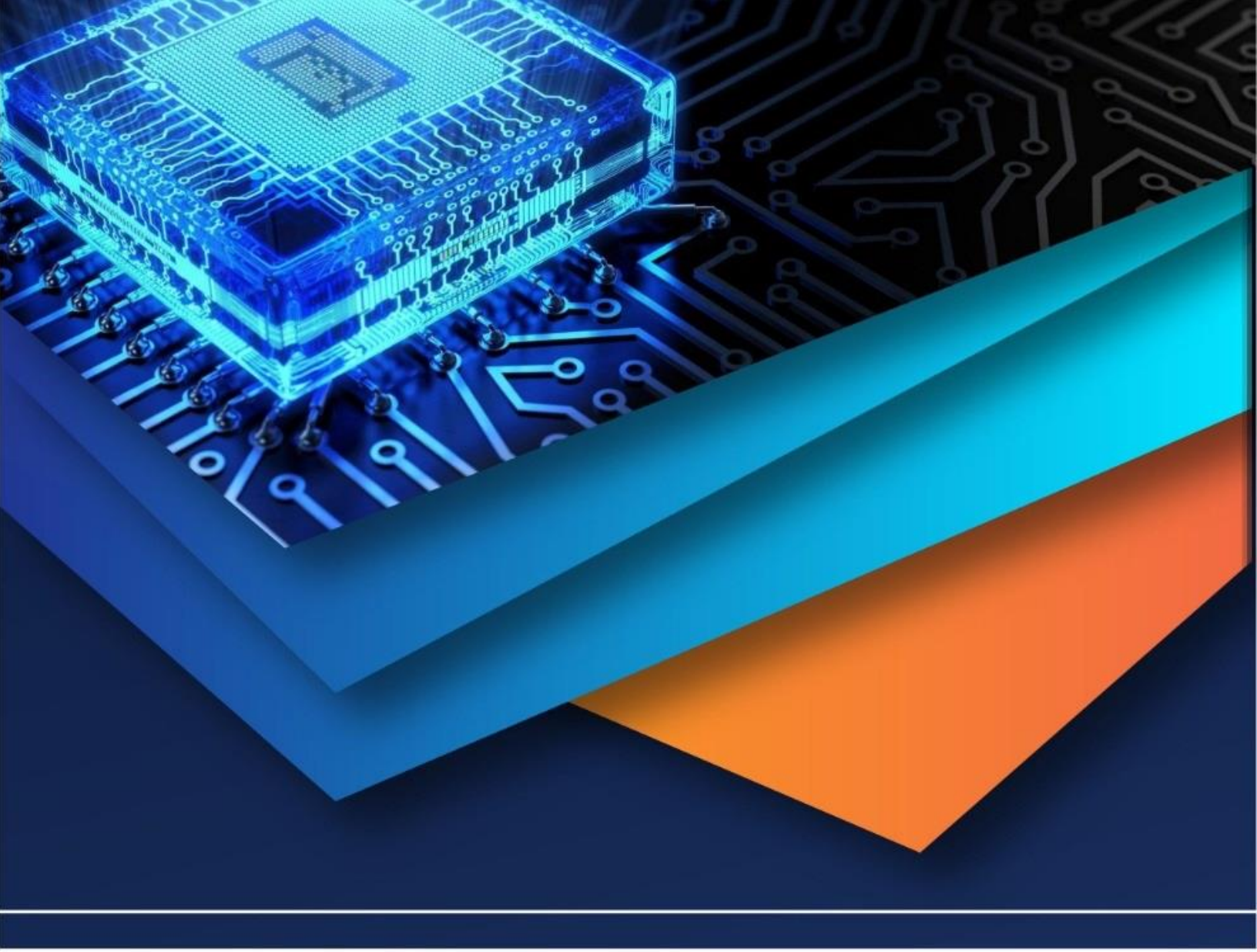
[36] Hu, J., Zhu, P., Qi, Y., Zhu, Q., & Li, X. (2022). A patent registration and trading system based on blockchain. Expert Systems with Applications, 201. https://doi.org/10.1016/j.eswa.2022.117094

[37] Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in the blockchain system. In Journal of Network and Computer Applications (Vol. 126, pp. 45–58). Academic Press. https://doi.org/10.1016/j.jnca.2018.10.020

[38] Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., & Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. Sustainable Cities and Society, 61. https://doi.org/10.1016/j.scs.2020.102360

[39] Klarin, A. (2020). The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions. In Research in International Business and Finance (Vol. 51). Elsevier Ltd. https://doi.org/10.1016/j.ribaf.2019.101067

[40] Allen, D. W. E., Berg, C., Markey-Towler, B., Novak, M., & Potts, J. (2020). Blockchain and the evolution of institutional technologies: Implications for innovation policy. Research Policy, 49(1). https://doi.org/10.1016/j.respol.2019.103865
[41] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. In BenchCouncil Transactions on Benchmarks, Standards and Evaluations (Vol. 2, Issue 3). Elsevier B.V. https://doi.org/10.1016/j.tbench.2022.100073
[42] Kalal, P., K, A. M., Dharawadmath, S. I., & M, V. C. (2023). Modern Smart Street Light Monitoring Systems. 11. www.ijraset.com
[43] Kumar M, P. B., Aatifulla Baig, M. M., Dharawadmath, S. I., & M, V. C. (2023). Review on Current Applications and Future Directions in Carbon Nanotubes for Cancer Therapy using AI. 11. www.ijraset.com
[44] C M, V. (2024). Friction Stir Welding Benefits Technique over Other Welding Techniques of Dissimilar Metals. International Journal for Research in Applied Science and Engineering Technology, 12(6), 796–813. https://doi.org/10.22214/ijraset.2024.63184



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY