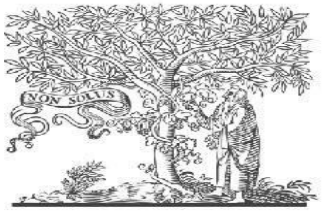
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 12th Oct 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 10

10.48047/IJIEMR/V12/ISSUE 10/09

Title **BLOCKCHAIN TECHNOLOGY A REVIEW**

Volume 12, ISSUE 10, Pages: 80-88

Paper Authors **Miss. Shreeya D. Bijwe,Mr.Shrihari V. Rathod, Miss. Shruti R. Satpute, Mr. Shubham R. Bulle, Miss. Sonal P. Lilhare**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

BLOCKCHAIN TECHNOLOGY A REVIEW

Miss. Shreeya D. Bijwe[1] Mr.Shrihari V. Rathod[2]
Miss. Shruti R. Satpute[3] Mr. Shubham R. Bulle[4]
Miss. Sonal P. Lilhare[5]
Student (UG) Department of Computer Engineering
Jagdambha College of Engg. & Tech. Yavatmal
Email : shreeyabijwe@gmail.com shreerathod8767@gmail.com
shruti.compengg@gmail.com shubhamrbulle@gmail.com
sonallilhare24@gmail.com

Abstract:

Blockchain technology has emerged as a transformative force with the potential to revolutionize various industries. This paper provides an accessible introduction to the fundamental concepts that underpin blockchain technology. We delve into the essence of distributed ledgers, consensus algorithms, and cryptographic mechanisms that collectively form the foundation of this innovative technology. Starting with an exploration of the historical context, we trace the evolution of blockchain from its inception as the underlying framework for cryptocurrencies to its broader applications across sectors. We elucidate the structure and characteristics of blockchain, emphasizing its distributed and immutable nature achieved through cryptographic hashing. A crucial aspect of blockchain is consensus mechanisms, which ensure agreement on the state of the network. We elucidate the working principles of proof-of-work (PoW) and highlight other consensus models, such as proof-of-stake (PoS) and practical Byzantine fault tolerance (PBFT), showcasing their diverse applications. Cryptography plays a pivotal role in securing transactions and data integrity within the blockchain. We demystify cryptographic functions, including hashing and digital signatures, outlining their significance in achieving a trustless environment. Furthermore, we explore the concepts of decentralization and trust, elucidating how blockchain technology minimizes the dependence on central authorities while fostering transparency and accountability. `

Keywords:

Blockchain technology ,Distributed ledger, Consensus algorithm ,Cryptography, Decentralization, Trust, Proof-of-work (PoW),Proof-of-stake (PoS),Practical Byzantine fault tolerance (PBFT),Cryptographic hashing ,Immutability, Transparency, Smart contracts, Use cases, Supply chain management ,Healthcare ,Identity verification, Scalability ,Regulatory challenges, Future directions.

Introduction:

[1]"" Aste, P. Tasca, and T. D. Matteo…. In the modern landscape of technological advancement, blockchain technology has emerged as a transformative force with the potential to reshape industries and redefine systems. Born as the underlying infrastructure for cryptocurrencies, blockchain has transcended its origin to offer a decentralized, transparent, and secure foundation for a wide range of applications. This paper serves as a comprehensive introduction to the fundamental principles that underlie blockchain technology, shedding light on distributed ledgers, consensus algorithms, and cryptographic mechanisms that collectively constitute its essence.The journey into understanding blockchain technology begins with tracing its roots. Stemming from the desire to create a digital currency that operates independently of centralized financial institutions, blockchain first came to prominence as the technology powering Bitcoin. However, its scope and potential swiftly expanded beyond the realm of cryptocurrency, sparking interest across industries eager to harness its capabilities. At its core, blockchain presents a paradigm shift in the way data is stored and verified. The concept of a distributed ledger, a decentralized and shared database maintained by a network of participants, forms the basis of this innovation.

The distributed ledger ensures that data is not only securely stored but also verified through

cryptographic methods, minimizing the risk of manipulation and fraud. Central to the viability of blockchain networks is the notion of consensus mechanisms. These mechanisms enable agreement among participants on the state of the network, effectively eliminating the need for intermediaries to validate transactions. The iconic proof-of-work (PoW) algorithm, utilized by Bitcoin, revolutionized the validation process by requiring participants to solve complex mathematical puzzles. Beyond PoW, a diverse array of consensus models, including proof-of-stake (PoS) and practical Byzantine fault tolerance (PBFT), have emerged, each tailored to specific use cases and requirements. Cryptography serves as the bedrock of blockchain security, ensuring the confidentiality, integrity, and authenticity of data. Hash functions and digital signatures play pivotal roles in creating an immutable and tamper-proof environment, further bolstering the trustworthiness of blockchain systems.

In this paper, we embark on an exploration of these fundamental concepts, delving into the intricacies of distributed ledgers, consensus algorithms, and cryptographic mechanisms that collectively give rise to blockchain technology. We traverse real-world applications across diverse sectors, from supply chain management to healthcare and identity verification, demonstrating how blockchain's potential transcends theoretical boundaries to address practical challenges. Despite its promise, blockchain technology is not without its challenges. Scalability issues, energy consumption concerns, and regulatory considerations pose intricate hurdles to be overcome. As we conclude our exploration, we reflect on the future directions of blockchain technology, including ongoing research and potential solutions aimed at addressing these challenges. By offering an accessible yet comprehensive foundation for understanding blockchain, this paper aims to serve as a resource for both newcomers and enthusiasts, illuminating the path toward a deeper appreciation of the revolutionary impact of blockchain technology.

Blockchain Fundamentals:

- **Distributed Ledger: [4]** A foundational concept of blockchain technology is the distributed ledger, a decentralized and tamper-proof database that records transactions across a network of participants. Unlike traditional centralized systems, where a single authority maintains control, a distributed ledger is collectively managed by network nodes. This ensures transparency and immutability, as transactions are recorded in a chronological order within blocks, each linked to the previous block, forming a chain.
- **Structure of Blockchain:** At the heart of blockchain is its distinctive structure of interconnected blocks. Each block contains a batch of verified transactions, along with a cryptographic hash of the preceding block. This linkage creates a continuous, unalterable chain of blocks, securing the integrity of the data within the blockchain. The cryptographic hash functions used in this process contribute to the immutability of the recorded information.
- **Immutability and Consensus:** The immutability of blockchain data is a result of cryptographic hashing and consensus mechanisms. Once a transaction is included in a block and added to the chain, altering any data within the block would require changing all subsequent blocks and obtaining the consensus of the network, making tampering practically infeasible. This process guarantees the integrity and permanence of recorded information.
- **Transparency and Trust:** Blockchain's transparency arises from its decentralized nature. All participants in the network possess a copy of the entire blockchain, enabling them to independently verify and audit transactions. This transparency reduces the need for trust in centralized entities, as each participant can verify the validity of transactions through the distributed consensus mechanism.

- **Cryptographic Hashing: [6]** Cryptography plays a crucial role in ensuring the security of blockchain data. Hash functions convert data into fixed-length strings of characters, known as hashes. These hashes are unique to the input data and irreversible, meaning that even a slight change in the input would result in a significantly different hash. This property

enhances the security of transactions and blocks, making them resistant to tampering.

- **Decentralization and Network Participation:**

Decentralization is a core principle of blockchain, eliminating single points of control and failure. Instead of relying on a central authority, blockchain networks are maintained by a distributed network of participants, each possessing a copy of the ledger. This redundancy enhances network robustness, reducing vulnerabilities. In essence, blockchain technology's fundamentals offer a novel approach to data management and transaction validation. The combination of distributed ledgers, cryptographic security, and consensus mechanisms gives rise to a secure, transparent, and tamper-resistant framework that has the potential to revolutionize various industries beyond its cryptocurrency roots.

Consensus Mechanisms:

- **Introduction to Consensus:[12]**In a decentralized network like a blockchain, where multiple participants contribute to the maintenance of the ledger, the challenge arises of reaching an agreement on the state of the ledger without a central authority. This problem, known as the Byzantine Generals' Problem, led to the development of consensus mechanisms – protocols that ensure all participants in the network agree on the validity of transactions and the order in which they are added to the blockchain.
- **Proof-of-Work (PoW):** One of the earliest and most well-known consensus mechanisms is Proof-of-Work (PoW). Introduced alongside Bitcoin, PoW requires participants, known as miners, to solve complex mathematical puzzles to validate transactions and create new blocks. The first miner to solve the puzzle broadcasts the solution to the network, which is then verified by other nodes. Once verified, the new block is added to the blockchain. PoW's security stems from the fact that solving these puzzles demands significant computational power and effort, making the creation of fraudulent blocks computationally infeasible.
- **Proof-of-Stake (PoS):** An alternative approach to achieving consensus is Proof-of-Stake (PoS). Instead of relying on computational work, PoS relies on the concept of ownership. Participants, referred to as validators, are chosen to create new blocks based on the number of cryptocurrency tokens they "stake" as collateral. This stake represents their vested interest in maintaining the network's integrity. PoS is considered more energy-efficient than PoW, as it eliminates the need for resource-intensive computations, while still ensuring security.
- **Practical Byzantine Fault Tolerance (PBFT):** Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism designed for permissioned blockchain networks, where participants are known and trusted. PBFT ensures consensus by having a leader node propose a block of transactions, and the other nodes collectively agree on its validity. Nodes then follow a multi-step process to confirm the block, ensuring a predefined threshold of nodes reach consensus before proceeding. PBFT offers fast transaction confirmation times and higher efficiency but is constrained by the assumption of a certain level of trust among network participants.
- **sHybrid Approaches and Beyond:** Blockchain's evolution has spurred the development of hybrid consensus mechanisms that combine elements of PoW, PoS, and other approaches. These mechanisms aim to leverage the strengths of different methods while mitigating their weaknesses. Additionally, new consensus models are continually being researched, exploring novel methods to achieve secure and efficient agreement in decentralized networks.
- **Choosing the Right Consensus Mechanism:** Selecting the appropriate consensus mechanism depends on the specific use case and requirements of the blockchain network. Factors such as security, scalability, energy efficiency, and network structure influence this choice. Different industries and applications may find certain consensus mechanisms more suitable than others.

In conclusion, consensus mechanisms are pivotal to the operation of blockchain networks. They ensure that all participants agree on the state of the ledger, enabling

secure and trustworthy transactions without the need for intermediaries. The choice of consensus mechanism is a critical decision in designing a blockchain system, and understanding the nuances of each mechanism is essential for building robust and efficient networks.

Cryptography in Blockchain:

- **Introduction to Cryptographic Security:** **[5] [6]** Cryptography is a cornerstone of blockchain technology, ensuring the confidentiality, integrity, and authenticity of transactions and data within the network. By harnessing cryptographic techniques, blockchain achieves a high level of security and trustworthiness, enabling participants to engage in transactions without the need for intermediaries or centralized control.
- **Hash Functions:** Hash functions play a vital role in maintaining the integrity of blockchain data. A hash function takes an input of any size and produces a fixed-length string of characters, known as a hash. Crucially, even a slight change in the input results in a significantly different hash, making it nearly impossible to reverse-engineer the original data from the hash. Hash functions are used to represent transaction data in a condensed form, forming the basis of blocks in the blockchain. This technique ensures that even a small alteration to a transaction would result in a change to the block's hash, alerting participants to potential tampering.
- **Digital Signatures:** Digital signatures are another critical application of cryptography in blockchain. A digital signature combines a message (such as a transaction) with the private key of the sender to create a unique signature. This signature is attached to the transaction and can be verified using the sender's public key. The verification process confirms the authenticity of the transaction and the identity of the sender. Digital signatures enable secure and tamper-proof transactions while preserving the privacy of participants' private keys.
- **Public and Private Keys:** Blockchain relies on asymmetric cryptography, which involves the use of pairs of keys: a public key and a private key. Public keys are widely distributed and serve as addresses to which transactions can be sent. Private keys, on the other hand, remain confidential and are used to sign transactions, confirming the sender's authorization. The security of blockchain lies in the mathematical relationship between these keys, which ensures that only the possessor of the correct private key can produce valid digital signatures.
- **Encryption and Privacy:** Cryptography also plays a role in preserving privacy within blockchain networks. While blockchain data is transparent and accessible to all participants, specific transactions can be encrypted using cryptographic techniques. This encryption ensures that only authorized parties can access the content of the transaction, maintaining confidentiality while still benefiting from the transparency of the network.
- **Immutable Security:** The application of cryptography within the blockchain imparts an immutable layer of security. Once transactions are recorded and validated, they become practically irreversible due to the cryptographic hashing used to link blocks. Attempting to alter a transaction would require recalculating the hash for the affected block and all subsequent blocks, making tampering infeasible and evident.

In summary, cryptography serves as the linchpin of security in blockchain technology. By employing techniques such as hash functions, digital signatures, and asymmetric key pairs, blockchain systems ensure the integrity, authenticity, and confidentiality of transactions, establishing an environment of trust and accountability in the digital realm.

Decentralization and Trust:

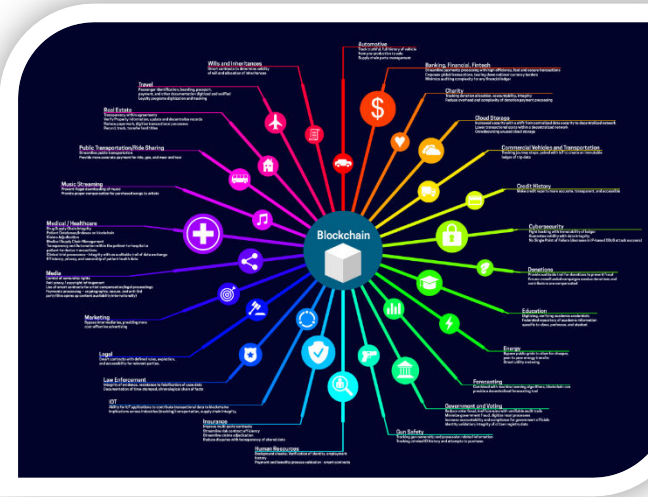
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

- **Introduction to Decentralization:** Decentralization stands as a cornerstone principle of blockchain technology, reshaping traditional paradigms of centralized control. In contrast to conventional systems where a single entity holds authority over data and transactions, blockchain achieves decentralization by distributing these responsibilities across a network of participants. This architecture has far-reaching implications, fostering transparency, accountability, and a new model of trust in digital interactions.
- **Eliminatin Central Authorities:** Traditional systems often require intermediaries or central authorities to validate and record transactions, introducing potential points of failure and vulnerability. Blockchain eliminates this need by enabling peer-to-peer interactions where participants directly transact with one another. The distributed nature of the network ensures that no single point can compromise the entire system.
- **Trust Through Consensus:** Decentralization redefines trust. In traditional systems, trust relies on centralized entities maintaining data accuracy and transaction validity. In a decentralized blockchain network, trust emerges through consensus mechanisms. Transactions are validated and confirmed by multiple participants in the network, eliminating the need to place blind faith in a single entity. The cryptographic verification of transactions and the immutability of the blockchain enhance the reliability and transparency of the network.
- **Removing Single Points of Failure:** Decentralization enhances the robustness of blockchain networks. In a centralized system, a single point of failure, such as a server outage or data breach, can cripple the entire system. In contrast, a decentralized network distributes data across numerous nodes, making it resilient to attacks and ensuring that even if some nodes fail or are compromised, the network remains operational and secure.
- **Transparency and Accountability:** Blockchain's decentralized architecture promotes transparency by providing all participants with access to the same ledger. Transactions are visible to all network participants, reducing the possibility of hidden manipulations. This transparency encourages accountability as participants are aware that their actions are open to scrutiny by others, discouraging fraudulent or dishonest behavior.
- **Challenges and Considerations:[3]** While decentralization offers numerous benefits, it also presents challenges. Achieving consensus in a distributed network can be computationally intensive and may result in slower transaction processing compared to centralized systems. Additionally, maintaining decentralized networks demands active participation from participants to validate transactions and secure the network, which can pose scalability challenges.
- **Building New Levels of Trust:** The decentralization of blockchain engenders a paradigm shift in how trust is established in digital interactions. Trust is no longer vested in single entities but emerges from the collective efforts of participants to maintain a transparent and secure network. This novel form of trust extends beyond individuals, encompassing the technology itself. The transparency, immutability, and consensus-driven nature of blockchain build new levels of trust in the digital realm.

In conclusion, decentralization redefines trust and introduces a new era of secure, transparent, and accountable digital interactions. By distributing authority and responsibility across a network of peers, blockchain technology provides a framework where participants can confidently engage in transactions without relying on intermediaries or centralized control.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Blockchain Applications:



- **Introduction to Diverse Applications: [8]** C. Patsakis Beyond its roots in cryptocurrencies, blockchain technology has ushered in a new era of innovation across a multitude of industries. The inherent features of transparency, security, and decentralization make blockchain a versatile solution with the potential to transform traditional processes, enhance security, and streamline operations. In this section, we explore some of the key industries and domains that have embraced blockchain technology.
- **Supply Chain Management:** Blockchain's transparency and immutability make it an ideal solution for supply chain management. By recording every stage of a product's journey on the blockchain, stakeholders gain a clear view of the origin, manufacturing, transportation, and delivery processes. This enhances traceability, reduces fraud, and provides consumers with reliable information about the products they purchase.
- **Healthcare and Medical Records:** In healthcare, the secure and interoperable nature of blockchain is leveraged to manage electronic health records. Patients can control access to their data and grant permission for medical professionals to view specific records securely. This ensures data integrity, reduces administrative complexities, and enhances patient privacy.
- **Identity Verification and Authentication:** Blockchain provides a decentralized and tamper-proof method for identity verification. Individuals can store their identity credentials on the blockchain, eliminating the need for multiple verification processes across different platforms. This can simplify access to services while enhancing data security.
- **Financial Services and Cross-Border Payments:** Blockchain's ability to facilitate secure and near-instant transactions has garnered significant interest from the financial sector. Cross-border payments, traditionally plagued by delays and fees, can benefit from blockchain's efficiency and reduced intermediaries, potentially revolutionizing international remittance processes.
- **Smart Contracts and Decentralized Applications (dApps):** Smart contracts, self-executing code that automatically enforces terms of an agreement, are a testament to blockchain's programmability. These contracts enable trustless automation of processes in various sectors, from real estate to insurance. Decentralized applications (dApps) built on blockchain platforms expand this concept, offering new ways to interact with digital services without intermediaries.
- **Intellectual Property and Copyright Protection:** Blockchain's immutability and timestamping features are harnessed to establish the ownership and provenance of digital assets, including intellectual property. By recording copyright information on the blockchain, creators can protect their work from unauthorized use and prove ownership in legal disputes.

Challenges and Considerations:

While blockchain applications offer significant promise, they are not without challenges. Scalability, regulatory compliance, and interoperability are areas that require careful consideration and innovative solutions. Additionally, introducing blockchain to existing systems may demand shifts in organizational processes and mindsets.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Unveiling Potential and Future Directions: The adoption of blockchain applications across various sectors highlights the technology's versatility. As industries continue to experiment and integrate blockchain solutions, new use cases are likely to emerge. However, it is crucial to acknowledge that not all problems necessitate blockchain's unique attributes, and careful evaluation is needed before implementation.

In summary, blockchain applications extend beyond cryptocurrencies, promising transformative changes in industries ranging from supply chain management to healthcare and beyond. The adaptability and trust-enabling features of blockchain open doors to innovative solutions that address real-world challenges and reshape traditional practices.

Challenges and Future Directions:

- ✓ **Scalability Concerns:** [3]T. Varvarigou One of the prominent challenges facing blockchain technology is scalability. As more transactions are added to the blockchain, the network's performance may degrade due to limitations in processing capacity and bandwidth. This challenge is particularly pronounced in public blockchains where numerous participants engage in transactions simultaneously. Addressing scalability is crucial for blockchain's widespread adoption, and various solutions, such as off-chain scaling and sharding, are being explored to enhance network throughput.
- ✓ **Energy Consumption:** Proof-of-Work (PoW) consensus mechanisms, while secure, have drawn attention due to their energy-intensive nature. The computational puzzles miners solve to validate transactions demand substantial computational power, resulting in high energy consumption. As blockchain networks grow, so does their carbon footprint. The search for energy-efficient consensus mechanisms and sustainable blockchain models is an essential step towards minimizing environmental impact.
- ✓ **Regulatory and Legal Considerations:** [11] K. Wüst, V. Glykantzis, H. Ritzdorf Blockchain's decentralized and borderless nature often collides with regulatory frameworks that were designed for centralized systems. The intersection of blockchain and existing legal systems poses challenges related to data privacy, jurisdiction, taxation, and compliance. Striking a balance between technological innovation and regulatory adherence is a complex task that requires cooperation between industry stakeholders, policymakers, and legal experts.
- ✓ **Interoperability and Standardization:** The proliferation of blockchain platforms and networks has led to a lack of interoperability between them. Different blockchains often operate in silos, limiting the seamless transfer of assets and data. Establishing standards and protocols for interoperability is essential to enable the fluid exchange of information across disparate blockchain networks and enhance their overall utility.
- ✓ **User Experience and Adoption:** Blockchain applications must provide a user experience that is intuitive and comparable to centralized alternatives. Overcoming the steep learning curve associated with blockchain, including managing private keys and interacting with decentralized applications, remains a hurdle for mainstream adoption. Improving user interfaces and enhancing accessibility are critical to lowering barriers to entry.
- ✓ **Identity and Security:** [12] S. Capkun While blockchain enhances security in many aspects, it also introduces new challenges. The immutable nature of the blockchain means that any data stored on it is permanent, potentially leading to privacy concerns if sensitive information is exposed. The management of cryptographic keys and the balance between privacy and transparency are ongoing considerations in blockchain design.
- ✓ **Future Directions:** Looking ahead, blockchain technology continues to evolve and adapt to meet emerging needs. Hybrid consensus mechanisms that combine the strengths of existing methods are gaining traction, aiming to provide a balance between security, energy efficiency, and scalability. Moreover, advancements in quantum computing pose both a challenge and an

opportunity for blockchain, as they threaten current cryptographic methods while inspiring the development of quantum-resistant algorithms. Interdisciplinary research is essential for blockchain's future growth. Collaboration between computer scientists, economists, legal experts, and policymakers will shape regulations, standards, and innovative use cases. As blockchain matures, industries are likely to find new ways to leverage its capabilities, and exploring novel domains, such as Internet of Things (IoT) integration and blockchain-based governance, will contribute to the technology's expansion.

In conclusion, while blockchain technology holds significant promise, it also faces critical challenges that require careful consideration and innovative solutions. The future of blockchain lies in its ability to address these challenges while continuously adapting to the evolving landscape of technology and society.

Conclusion:

Blockchain technology has transcended its origins as the foundation for cryptocurrencies and evolved into a transformative force with the potential to reshape industries and redefine digital interactions. Through this comprehensive exploration of blockchain's fundamental components, including distributed ledgers, consensus mechanisms, cryptographic security, decentralization, and trust, we have gained insights into its unique attributes and potential implications. Blockchain's distributed ledger architecture and consensus mechanisms offer a novel solution to the age-old challenge of achieving agreement in decentralized networks. Whether through the energy-intensive but secure Proof-of-Work (PoW), the energy-efficient and stake-based Proof-of-Stake (PoS), or other emerging hybrid models, consensus mechanisms ensure that participants can transact and communicate in a trustless manner. Cryptography stands as the bedrock of blockchain's security, guaranteeing the confidentiality, integrity, and authenticity of data. Hash functions, digital signatures, and asymmetric encryption collectively create an environment where transactions are tamper-proof, data is verifiable, and participants can trust the integrity of the information on the blockchain. Decentralization and trust are redefined by blockchain. The removal of central authorities and the shift towards peer-to-peer interactions foster transparency, reduce vulnerabilities, and enhance accountability. Trust emerges through the consensus of multiple participants rather than reliance on single entities, and the immutability of the blockchain instills confidence in the integrity of transactions. As we have explored diverse applications across supply chain management, healthcare, identity verification, financial services, and more, it becomes evident that blockchain has the potential to reshape traditional processes, enhance security, and open avenues for innovation. However, challenges like scalability, energy consumption, regulatory compliance, and interoperability demand continuous research and collaboration to unlock blockchain's full potential. The future of blockchain lies in its adaptability. It adapts to meet the changing needs of industries, societies, and technological advancements. The journey forward involves finding solutions to current challenges, developing sustainable and efficient models, and fostering interdisciplinary cooperation to shape regulations and standards. In conclusion, blockchain technology represents a paradigm shift in the way we interact with data and engage in transactions. Its decentralized, secure, and transparent nature offers the promise of greater efficiency, reduced intermediaries, and enhanced trust in digital interactions. As we continue to explore, innovate, and refine this technology, we usher in an era where the potential for positive transformation is boundless.

References:

[1]Aste, P. Tasca, and T. D. Matteo, ‘‘Blockchain technologies: The foreseeable impact on society and industry,’’ Computer, vol. 50, no. 9,
pp. 18–28, Jan. 2017.

[2] S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System.
Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[3] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha,
‘‘Blockchain for AI: Review and open research challenges,’’ IEEE
Access, vol. 7, pp. 10127–10149, 2019.

[4] A. Litke, D. Anagnostopoulos, and T. Varvarigou, ‘‘Blockchains for supply chain management: Architectural elements and challenges towards a

global scale deployment,'' Logistics, vol. 3, no. 1, p. 5, Jan. 2019.

[5] M. Kouhizadeh and J. Sarkis, ''Blockchain practices, potentials, and

[6]G. Peters, E. Panayi, and A. Chapelle, ''Trends in cryptocurrencies and

J. Financial Perspect., vol. 3, no. 3, pp. 1–25, Nov. 2015.

[7] J. Al-Jaroodi and N. Mohamed, ''Blockchain in industries: A survey,''

IEEE Access, vol. 7, pp. 36500–36515, 2019.

[8] F. Casino, T. K. Dasaklis, and C. Patsakis, ''A systematic literature review

of blockchain-based applications: Current status, classification and open

issues,'' Telematics Inform., vol. 36, pp. 55–81, Mar. 209.

[9] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ''Blockchain chal lenges and opportunities: A survey,'' Int. J. Web Grid Services, vol. 14,

no. 4, pp. 352–375, 2016.

[10] S. Bano, M. Al-Bassam, and G. Danezis, '' The road to scalable

blockchain designs,'' USENIX, Login, Mag., Dec. 2017, pp. 1–6.

[11] A. Gervais, G. O. Karame, and K. Wüst, V. Glykantzis, H. Ritzdorf, And S. Capkun, '' On the security and performance of proof of work

blockchains,'' in Proc. ACM SIGSAC Conf. Comput. Commun . Secur.

Oct. 2016, pp. 3–16.

[12] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, ''Is bitcoin a decentralized currency?'' IEEE Security Privacy, vol. 12, no. 3, pp. 54–60,

May/Jun. 2014.