BLOCKCHAIN UNCHAINED: APPLICATIONS OUTSIDE CRYPTOCURRENCY

Lakshmi Kumari* Neetu Mittal**

The blockchain technology, which first gained recognition for enabling cryptocurrencies such as Bitcoin, is now emerging as a transformative technology with applications extending far beyond digital currencies. Its decentralized, unchangeable, and transparent characteristics make it appropriate for a variety of fields, including as voting systems, healthcare, banking, supply chain management, identity verification, and intellectual property protection. In this research paper usage of blockchain technology in different areas is shown depicting the features such as operational efficiency, security, and transparency. It also explores the foundational role of blockchain in cryptocurrency, focusing on how the consensus mechanism, mining process, and cryptographic principles secure transactions and maintain decentralization. Through an analysis of real-life use cases, this paper identifies the possibilities, shortcomings, and emerging potential of blockchain technology. Blockchain's capacity to generate tamper-proof and decentralized digital accounts is perhaps its most groundbreaking feature. Blockchain's future will keep unfolding as industries pursue higher levels of security and efficiency, as its role will expand.

Keywords: *Blockchain, Cryptocurrency, Decentralization, Smart Contracts, Cryptography*

INTRODUCTION

In 2008, Satoshi Nakamoto introduced BTC as underpinning architecture for a secure, transparent, and decentralized payment platform. The principles of decentralization, immutability, and transparency introduce the blockchain in a distributed ledger. These core elements play a key role in facilitating financial transactions without the use of intermediaries like banks and centralized financial institutions. Blockchain has developed from cryptocurrency over time to facilitate

* Research Scholar, Amity University, Noida, Email: Lakshmi.kumari@iitmipu.ac.in

** Professor, Amity University, Noida

applications across various industries, such as logistics, data protection, and governance. Its potential to operate as an impenetrable, decentralized ledger system has promoted its extensive adoption across key sectors. The constantly evolving environment of blockchain technology has initiated innovations that transcend monetary uses. Governments and nongovernmental organizations are more and more turning to blockchain due to its capacity to transform data security and enhance transparency. As developments continue, blockchain is ready to have a major influence on world economies, facilitating transactions, protecting records, and redefining trust within digital environments.

Blockchain and Cryptocurrency

The first and foremost application of blockchain was the cryptocurrency itself. Bitcoin led the way with a peer-to-peer payment system to secure trustless transactions without financial institutions in between. This is achieved through decentralization, immutability, transparency, and security. Decentralization means that transactions are verified and recorded by a system and not a single central authority, which reduces the risks involved in centralized control. Immutability is the fact that when a matter is written over blockchain, after that it cannot be changed, providing veracity and security. Transparency enables all transactions to be written and made available to market participants, thus enhancing trust in the system.

Hashing is used to have security and the application of public-private key mechanisms, safeguarding transactions against unauthorized changes. Blockchain technique reduces the probability of deception and hacking, hence it is an opted method for safe monetary dealings across the globe. As use increases, blockchain is also a necessary technology for expanding digital finance and international trade.

Moreover, with more emergence of decentralized finance (DeFi) systems and non-fungible tokens (NFTs), blockchain is continuously being expanded beyond its initial use, demonstrating its versatility and resilience in the digital economy. As governments and financial institutions look to integrate blockchain into their current infrastructure, the technology will have a substantial part to show in determining the impending of secure, efficient, and transparent financial systems.

The building blocks laid by Bitcoin have led to the creation of supplementary cryptocurrencies such as Ripple and Litecoin, including transaction processing speeds, and specific functionalities designed for various applications. More importantly, Ethereum has brought about smart contracts, which broaden the use of blockchain beyond monetary transactions, allowing decentralized applications (DApps) and other automated services. Smart conventions executed automatically by predefined agreements, removing the prerequisite for intermediaries and providing trustless contract execution. Consequently, blockchain technology is increasingly being applied across different sectors, like real estate, supply chain management, healthcare, banking, and intellectual property protection. Outside these industries, blockchain has been applied to governance, where it is utilized for secure voting systems, and in identity authentication, providing improved privacy and security for digital identities. In this paper, the growth of blockchain from a cryptocurrency-supporting technology to a revolutionary tool that is transforming various industries by improving security, competence and transparency in digital transactions is discussed. Based on actual case studies and future trends, this research outlines the effect of blockchain on business models, regulation, and the overall economy.

Blockchain in Cryptocurrency

Cryptocurrency is the most significant and widespread application of blockchain technology. The fundamental components of blockchain's part in cryptocurrency comprise transaction validation, mining, cryptographic security, and trustlessness (Nakamoto, 2009). These features combine to advance the dependability of transactions and supply a robust basis for financial services. The distributed nature of blockchain assures no single entity manipulates the system, rendering it immune to fraud and external interference. In addition, the usage of cryptography ensures that transactions are innocuous and irreversible, minimizing risks associated with unauthorized access and data breaches. The trustless nature of cryptocurrency transactions enables parties to trade digital assets without the need for a trusted third party, greatly reducing transaction costs and making it accessible to users across the globe. Consequently, blockchain technology continues to revolutionize the financial sector by offering an alternative to traditional banking systems and facilitating borderless digital payments. Furthermore, the integration of blockchain into digital wallets and money applications boosts security and ease of use, which brings cryptocurrency closer to mainstream consumers. Governments and banks are also looking into central bank digital currencies (CBDCs) as a means of utilizing blockchain technology while still having regulatory control and monetary stability. The increasing use of cryptocurrency is pushing the development of blockchain protocols further, leading to innovative solutions for scalability, interoperability, and security.

Transaction Validation and Mining

Cryptocurrency transactions are validated and recorded on the blockchain with a consensus mechanism, which guarantees accuracy and avoids double-spending. The process is essential in maintaining the veracity of the blockchain network and that transactions are genuine. Different techniques are available, each tailored to ensuring security, efficiency, and decentralization. The most popular mechanisms are Proof of Work (PoW) and Proof of Stake (PoS), which both guarantee blockchain networks are secure and immune to fraudulent transactions. These mechanisms enable blockchain participants to verify and authenticate transactions collectively, thus furthering the decentralized nature of the system. The selection of an agreement can significantly influences the performance, scalability, and blockchain network's energy utilization efficiency, making it a core element of cryptocurrency technology. In addition to this, innovations like hybrid consensus mechanisms and sharding protocols are being researched for blockchain scalability and transaction velocity optimization. With development in blockchain networks, studies of innovative consensus algorithms like Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) are opening for cleaner and more efficient blockchain solutions.

Proof of Work (PoW)

Bitcoin shows that, whereby miners compete to solve complex mathematical equations with computational effort. The initial miner to solve the equation gets rewarded with cryptocurrency upon adding a new block to the blockchain. The process creates network security since it is computationally challenging for the bad guys to manipulate previous transactions. Nevertheless, PoW demands great usage of energy, which raises questions over its sustainability in the long run. Mass mining processes devour enormous amounts of electricity, evoking environmental alarm and sparking calls for more sustainable alternatives. Imperfect as it is, PoW is among the most secure and battle-proven consensus protocols, securing blockchain networks from malicious attacks and ensuring their integrity. Technologies like low-power consumption mining equipment and mining farms are being pursued to offset the environmental footprint of PoW. In addition, nations and organizations are investing in research on other PoW variations that decrease computational complexity without sacrificing security. With ongoing improvements in the efficiency of blockchain, PoW-based networks are attempting to balance security, decentralization, and sustainability (Wood, 2014).

Proof of Stake (PoS)

Ethereum is shifting to PoS, in which validators are chosen according to the amount of coins owned and will "stake." PoS requires less energy and less computational power necessary for mining, fixing the sustainability issues related to PoW. With decreased energy usage, PoS offers a sustainable option while not sacrificing network security or decentralization. PoS validators are motivated to be honest, as their assets staked may be cut due to dishonesty. PoS also allows for faster processing of transactions and reduced fees, the popular option for blockchain networks that require scalability. This shift is a big step in blockchain development, which encourages eco-friendly practices while guaranteeing strong security. (Antonopoulos, 2014). As PoS continues to gain traction, its variants like Delegated Proof of Stake (DPoS) and Liquid Proof of Stake (LPoS) are being formulated in order to improve governance schemes and transactional throughput. The trend towards PoS-based networks will be likely to further spur blockchain adoption with a simpler and cheaper alternative for developers and end- users.

Cryptographic Security

Cryptographic algorithms are used to protect transactions including hashing and digital signatures, to make them secure and immutable. Hashing is done to ensure every block contains a cryptographic hash of the previous one, and tamper-proof chain. Block information in Bitcoin is secured using SHA-256 (Secure Hash Algorithm), which maps input data to a fixed-length hash that is unique and irretrievable. Digital signatures increase transaction security by confirming that only official can authenticate transactions. Public and private key cryptography enables secure signing of transactions to preserve data integrity. The private key allows the owner to sign a transaction, while the public key permits others to validate its authenticity to preserve transaction security. Any attempt to manipulate transaction details would render the hash invalid, preserving immutability. Cryptographic security measures resist attacks like double-spending and fraud in transactions, ensuring blockchain as a solid foundation for safe digital interactions. Furthermore, sophisticated cryptographic methods like zero-knowledge proofs (ZKPs) and homomorphic encryption are on the rise, enhancing security and privacy within blockchain networks further.

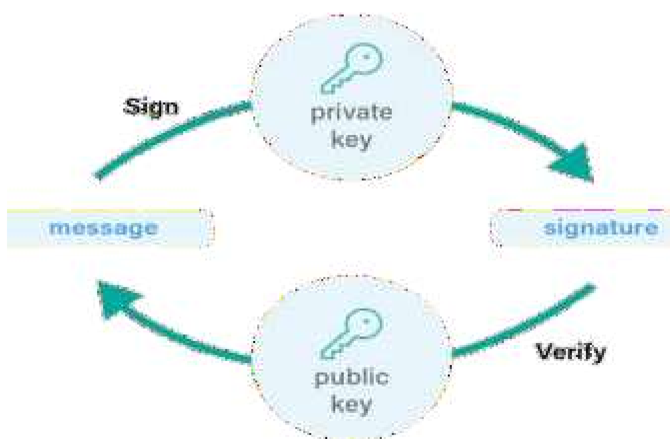

Figure 1 Cryptography Security

Decentralization and Trustlessness

Cryptocurrency is a system of nodes, whereby transactions are verified independently. The absence of centralized control decreases the menace of censorship, fraud, and only one points of failure. Decentralization has one of its fundamental characteristics in consensus mechanisms, including Proof of Work (PoW) and Proof of Stake (PoS), which verify transactions without requiring centralized authorities. (Treiblmaier, 2018). These techniques do not allow harmful actors from changing transaction history, ensuring integrity. Trustlessness implies that users do not have to trust mediators such as banks or governments; rather, the cryptographic rules of the system ensure transaction validity. Blockchain removes middlemen through the use of smart contracts, which carry out transactions automatically according to set rules. This lowers costs, improves efficiency, and eliminates the risk of human bias or manipulation. Decentralization also ensures resistance against interference or control by the government, and thus blockchain networks become more robust. Distributed ledger technology (DLT) allows all participants to maintain a ledger copy, minimizing the likelihood of data tampering or loss. The increased use of decentralized finance (DeFi) also highlights the trustless nature of blockchain, giving users financial independence.

Blockchain Applications Beyond Cryptocurrency

Supply Chain Management

Blockchain revolutionizes supply chain management by offering greater transparency, traceability, and efficiency. All supply chain transactions are placed on an unchangeable distributed ledger, which makes it hard for fraud and counterfeiting. Large corporations such as IBM and Walmart use blockchain technology to authenticate goods, protect against counterfeiting, and verify the origin of products. Blockchain enables real-time tracking of shipments so that products reach their destinations on schedule and in good condition. Companies can make payments and impose agreement automatically without the use of middlemen, saving administrative costs and delays (Kshetri & Voas, 2018). Better traceability enables companies to quickly track and recall defective or tainted products, increasing safety standards. Moreover, blockchain's ability to hold detailed records guarantees regulatory compliance, lowering legal risks. Anti-counterfeiting is also improved, as blockchain can verify product authenticity by holding unique digital signatures. Small businesses can also utilize blockchain technology to achieve clear and secure supply chains, thereby boosting consumer trust and operational performance (Mollah et.al. 2019). This technology can be combined with IoT devices further enhances tracking capability, optimizing logistics and warehouse management for a flawless supply chain experience.

Healthcare

Blockchain has life-changing applications in medicine by safeguarding private patient data across the health continuum and increasing interoperability. Automated medical documents that are put on a blockchain cannot be modified, and they cannot be deleted, providing data integrity. Providers and patients have secure access to records, avoiding duplicated tests and administrative burdens. Blockchain facilitates seamless sharing of data between hospitals, clinics, and research institutions while maintaining patient privacy through encryption. Pharmaceutical companies employ blockchain to monitor medicines from production to delivery, keeping fake drugs off the streets. Smart contracts allow insurance claims to be processed automatically, shutting down opportunities for fraud and efficient processes (Zhao, Fan & Yan, 2016). Medical supply chains also benefit from blockchain, verifying authenticity and origin of medicines. Blockchain supports clinical trials by securing research data, sealing it from tampering, and opening up medical studies to transparency. AI-driven analytics coupled with blockchain could improve patient treatment and diagnosis guidelines. As such, blockchain puts more trust in healthcare services due to reduced inefficiencies, improving patient outcomes, and improving security measures for the data in the medical sector.

Voting Systems

Blockchain secures elections through a verifiable, transparent, and tamper-proof voting mechanism. Conventional voting systems can be susceptible to fraud, hacking, and human mistakes, weakening election integrity. Blockchain voting assures that every vote is recorded safely on an indelible ledger, avoiding duplication or tampering. Voter identity is authenticated via cryptographic authentication to ensure only authentic voters cast votes. Decentralized counting enhances transparency since citizens and election observers can independently verify the results. Smart contracts make counting automatic and minimize the risk of manipulation as they guarantee agreed-upon election rules are applied. Blockchain-enabled voting alsoenhances remote and online voting, making it easier for citizens who may not be physically present at polling centers. The technology minimizes costs related to printing ballots, personnel to manage polling centers, and manual count.. Blockchain voting would end election fraud, improve voter trust, and ensure transparent and equitable elections globally if implemented extensively.

Intellectual Property and Copyright Protection

Blockchain provides a secure platform for protecting intellectual property (IP) and copyright by establishing permanent proof of ownership. Artists, writers, musicians, can have their work registered on blockchain, ensuring timestamped evidence of authorship (Crosby, 2016). The permanent record makes unauthorized use impossible and easy to prove ownership rights. Smart contracts enable automatic payment of royalties, ensuring fair compensation for creators and diminishing conflicts. Blockchain also supports anti-piracy efforts by authenticating content digitallyand preventing unauthorized sharing. The technology promotes IP management through safe licensing deals, whose terms are guaranteed through smart contracts without the requirement of intermediaries. Trade secrets and patents can be protected by keeping them on a secure blockchain system, which prevents intellectual property theft. Blockchain also enables fractional ownership of digital assets, which allows several parties to share revenue streams in an open format. The integration of non- fungible tokens (NFTs) has unveiled blockchain's potential for digital content ownership to tokenize and successfully monetize creators' work. Blockchain overall strengthens IP rights, promotes equitable remuneration, and enables secure content delivery.

Identity Verification

Blockchain enhances identity verification by providing self-sovereign identity management where individuals are in charge of their data. Conventional identity models use centralized databases and, thus, are at risk of being hacked, impersonated, and subject to identity fraud. Blockchain provides a decentralized identity system in which individuals hold and exchange identity credentials safely. Digitally stored identity on blockchain is unalterable and eliminates duplication and forgery. Governments and institutions can leverage blockchain for secure authentication, providing access to banking, insurance, and e-governance services. Identity verification across borders is simple with blockchain providing worldwide interoperability. Smart contracts provide real-time identity verification, shortening on boarding time for businesses and online services. Privacy is improved with selective disclosure mechanisms, where users provide only required information without revealing complete details. Decentralized identity technologies like Self-Sovereign Identity (SSI) and Verifiable Credentials (VCs) are picking pace with their capacity to deliver secure and user-managed identity systems. Blockchain-based identity verification strengthens security, improves trust, and makes digital interactions smoother across different industries, which will lead to a more secure and efficient identity management system.

Application	Key Benefit	Industry Impact	Technical Feature
Supply Chain Management	Transparency	High	Interoperability
Healthcare	Data Integrity	Critical	Drug Traceability
Voting Systems	Voter Verification	Essential	Immutable Record
Intellectual Property	Proof of Ownership	Moderate	Royalty Tracking
Identity Verification	Self-Sovereign Identity	High	Anti-Piracy Measures

Figure 2
Challenges Faced by Blockchain

Scalability

Blockchain networks are scalability-limited where many transactions have to be performed. Bitcoin processes up to seven transactions per second (TPS), whereas Visa is capable of processing 24,000 TPS. When the network gets congested, high fees are incurred and low processing speeds prevail. Solutions such as the Lightning Network and Plasma try to fix the scalability issues but are at a nascent stage of roll-out (Croman, 2016). Sharding is yet another solution being developed, where the blockchain is divided into multiple parallel chains in order to distribute the computational burden. Layer-2 solutions such as rollups batch groups of transactions together before adding them to the main chain, reducing traffic. Nevertheless, it is difficult to achieve these solutions and maintain it secure and decentralized. Blockchain scalability is required for widespread adoption as slow transaction speeds hinder its real-world application. Researchers continue to explore novel consensus algorithms, such as proof-of-history (PoH) and directed acyclic graphs (DAGs), to increase efficiency. Scaling constraints will determine whether block chain will be able to thrive in supporting global financial systems, smart contracts, and decentralized applications (dApps). Research and development continue to optimize speed, security, and de centralization.

Regulatory Uncertainty

Governments around the world are developing blockchain regulations, and this has introduced operational uncertainties. Different jurisdictions have varying rules, and cross-border operations are challenging. The regulatory challenges involve unclear tax codes, anti-money laundering (AML) compliance, and privacy concerns, which complicate wide blockchain adoption. Restrictive rules are imposed by some governments on cryptocurrency transactions as well, affecting businesses utilizing blockchain for financial services. Governance of such rules as the General Data Protection Regulation (GDPR) is challenging, as blockchain immutability challenges the "right to be forgotten." Governments also concern themselves with criminal activities such as money laundering and tax avoidance enabled by anonymous blockchain transactions. There is increased clarity in rules over time, however, through stablecoins, central bank digital currencies (CBDCs), and decentralized finance (DeFi) frameworks development. Establishing international regulatory norms will be key to fostering blockchain innovation without compromising consumer protection and financial stability. Policymakers, industry players, and blockchain creators need to collaborate to create a balanced regulatory approach that drives responsible blockchain adoption.

Energy Consumption

Blockchain networks are isolated, making cross-chain communication challenging. Various blockchains support varied protocols and consensus mechanisms, which prevent seamless data exchange across them. Non-standardization causes inefficiency for business firms requiring multi-blockchain integration. Solutions such as cross-chain bridges, atomic swaps, and interoperability protocols like Polka Dot and Cosmos are suggested to connect various blockchains. These technologies make it possible for assets and data to move from one network to another without requiring central intermediaries, ushering in a more integrated environment. Interoperability is, however, hampered by security vulnerabilities and the complexities of developing universal standards. Greater interoperability will spur blockchain usage across industries through allowing different blockchain platforms to communicate with one another and share data seamlessly.

Interoperability

The majority of blockchain networks, particularly those using Proof-of-Work (PoW), come with high energy demands. Bitcoin mining, for example, requires enormous computational power, posing challenges of environmental sustainability. The utilization of large quantities of energy produces carbon emissions, raising concerns regarding the long-term sustainability of blockchain. To address this, blockchain developers have been shifting towards energy-efficient consensus protocols such as Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS). Ethereum's switch from PoW to PoS with Ethereum 2.0 significantly reduced its energy consumption. Additionally, innovations like carbon- neutral blockchains and renewable energy-based mining centers aim to mitigate environmental concerns. Green blockchain techniques will play a critical role in gaining widespread adoption with keeping up with global climate initiatives.

Security Threats

Despite blockchain having the inherent security advantages, it is nevertheless vulnerable to attacks. 51% attacks arise when one gets in possession of most of the network's mining power and can therefore bully transactions around. Smart contract weaknesses also pose threats, with bugs in codes being exploited by attackers to take advantage. Hacking and exploitation in decentralized finance (DeFi) protocols have caused tremendous money losses. Formal verification, rigorous smart contract auditing, and multi-signature validation mechanisms are being implemented to enhance security for upgrading. Quantum-resistant cryptographic practices are also in the process of being developed in order to make blockchain security future-proof against attacks from quantum computing. High-security levels need to be ensured in order to make blockchain applications trusted.

Lack of Awareness and Adoption

To counteract blockchain's constraints, measures are being implemented. Layer-2 scaling technologies such as rollups and sidechains accelerate transactions while reducing base chain congestion. Regulative frameworks are also evolving to provide transparency and encourage sound usage. Efforts to develop interoperability via standardized protocols and cross-chain communication platforms are gaining momentum. Energy-saving consensus algorithms such as Proof-of-Stake and hybrid models are tackling environmental concerns. Security innovations, including AI-based threat detection and quant.um-resistant cryptography, further strengthen blockchain networks. Continuous innovation and cross- industry collaboration among developers, regulators, and companies will be essential in addressing these challenges and unlocking the potential of blockchain.

Figure 3

FUTURE SCOPE

Decentralized Finance (DeFi): DeFi revolutionizes financial services by enabling lending, borrowing, and insurance without traditional intermediaries. DeFi platforms leverage blockchain to offer trustless, transparent financial solutions.

Cross-Border Payments: **Blockchain facilitates fast, cost-effective international money transfers using stablecoins and central bank digital currencies (CBDCs). It eliminates reliance on traditional banking intermediaries, reducing fees and transaction times.**

AI and Blockchain Integration: **AI and blockchain integration enhances fraud detection, predictive analytics, and automated decision-making. Smart contracts powered by AI can execute complex agreements with increased efficiency and accuracy.**

Tokenization of Assets: **Real-world assets, including real estate and art, can be tokenized and traded on blockchain platforms. Tokenization enhances liquidity, allowing fractional ownership and easier asset transfers.**

Conclusion

Blockchain started as a technology to support cryptocurrency and gradually evolved into a disruptive technology that could be adopted into any industry. Its features of security, transparency, and decentralization have made it the backbone of financial systems, supply chains, healthcare and other industries. While scalability and regulatory uncertainty pose some challenges, future technological developments and rising adoption could drive growth in blockchain gradually assimilating into mainstream industries.

REFERENCES

Antonopoulos, A.B. (2014). *Mastering Bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media.

Apte, S. & Petrovsky, N. (2016). Will blockchain technology revolutionize excipient supply chain management?. *Journal of Excipients and Food Chemicals*.

Beck, R. & Müller-Bloch, C. (2017). Blockchain as radical innovation: A framework for engaging with distributed ledgers. In: Proceedings of the 50th Hawaii International Conference on System Sciences. 653.

Böhme, R. et.al. Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives*. 29(2): 213-238.

Bonneau, J. et.al. (2015). SoK: Research perspectives and challenges for Bitcoin and Cryptocurrencies. In: *IEEE Symposium on Security and Privacy,* San Jose*,* USA. 104-121, doi: 10.1109/SP.2015.14.

Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application Platform. *Whitepaper*. https//:www.ethereum.org.

Casino, F. Dasaklis, T.K. & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36: 58-61.

Catalini, C. & Gans, J.S. (2016). Some simple economics of the blockchain. *NBER Working Paper*. National Bureau of Economic Research, Cambridge.

Conti, M. et.al. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*. 20(4): 3416-3452.

Croman, K. et.al. (2016). On scaling decentralized blockchains. In: Financial Cryptography and Data Security International Workshop. Springer. 106-125.

Crosby, M. et.al. (2016) Blockchain technology: Beyond bitcoin. Applied Innovation Review. 2:71.

Dinh, T.T. & Thai, M.T. (2018). AI and blockchain: A disruptive integration. *Computer*. 51(9): 48-53.

Eyal, I. & Sirer E. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*. 61(7): 95–102. https://doi.org/10.1145/3212998

Gervais, A. et.al. (2016). On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, New York. 3-16.

Haber, S. & Stornetta, W.S. (1991). How to time stamp a digital document. *Journal of Cryptology*. 3: 99-111.

Kiayias, A. et.al. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Lecture Notes in Computer Science, Annual International Cryptology Conference.

Kim H.M. & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*. 25(1): 18-27.

Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South?. *Third World Quarterly.*38:1710-1738.

Kshetri, N. & Voas, J. (2018). Blockchain in developing countries. *IEEE IT Professional.* 20(2): 11-14.

Mollah, M.B. et.al. (2019). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing List*.

Narayanan, A. et.al. *Bitcoin and cryptocurrency technologies*. Princeton University Press. 2016.

O'Dwyer, K.J. & Malone, D. (2014). Bitcoin mining and its energy footprint. In: 25th IET Irish Signals and Systems Conference. 280-285.

Ølnes, S. Ubacht, J. & Janssen, M. (2018). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly.* 34(3): 355-364.

Pinna, A. & Ruttenberg, W.(2016). Distributed ledger technologies in securities post-trading. *European Central Bank Occasional Paper Series*.172.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*. 2(9).

Tapscott, D. & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin, New York.

Treiblmaier, H. (2018). The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. *Supply Chain Management: An International Journal*. 23(6): 545-559.

Tschorsch, F. & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*. 18(3): 2084-2183.

Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM.* 59(11): 15-17.

Vasek,M., Thornton, M. and Moore, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In: Lectures Notes in Computer Science at International Conference on Financial Cryptography and Data Security.8438: 57-71.

Wood, G., et al. (2014). Ethereum: A secure decentralized generalised transaction ledger. Ethereum Project Yellow Paper, 151.

Xu, X. et.al. (2016). The blockchain as a software connector. In: 13th Working IEEE/IFIP International Conference on Software Architecture. 182.191.

Yli-Huumo, J. et.al. (2016). Where is current research on blockchain technology?—A systematic review. *PLoS ONE.* 11(10): 0163477.

Zhao, J.L. Fan, S. & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*. 2(1): 28.

Zheng, Z. et.al.(2017). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*. 14(4): 352-375.

IITM JOURNAL OF MANAGEMENT and IT (ISSN: 0976-8629)
PUBLISHING POLICY & AUTHOR GUIDELINES

IITM Journal of Management & IT, a peer-reviewed, hybrid (print & online), bi-annual journal that publishes original research and review papers related to entire spectrum of Management, Commerce and its interdisciplinary areas. Typescript required for consideration in IITM Journal of Management and IT are: Research papers (max length: 5500 words or 15 typed pages of A4 size including figures, and references) containing original research findings in a clear and concise manner.

Submission: Article (s) should be submitted to the Editor, IITM Journal of Management and IT, through designated e-mail (**journal@iitmipu.ac.in**) along with Word ® attachment. The author (s) should obtain copyright clearance for materials used in the article. It will be assumed that submission of an article to this journal implies that all the foregoing conditions are applicable.

Review Process: Follows double blind peer-review process, IITMJMIT makes full confidentiality among authors and reviewers and does not take biased decision.

Language: All articles must be submitted in Standard English (preferably British). Authors for whom English is a second language are encouraged to seek assistance in writing from a native speaker. Manuscripts written in poor English will not be sent for review.

Confidentiality: IITM Journal of Management and IT treats the submitted manuscript and all communication with authors and referees as confidential. Authors must also treat communication with the Editor as confidential.

Plagiarism: As per the international standards, manuscripts, which have similarity, index less than 10 percentage will only be accepted. Author (s) must submit plagiarism report checked by internationally accepted plagiarism detection software along with the manuscript.

Referencing Style: The APA Style for referencing has to be used, for e.g.:

References should be indicated in the text by following the APA Style Alphabetically arranged in order. Some examples of various types of documents are given below:

- **Book (Printed) with Single Author:** Tolkien, J.R.R. (1954). Lord of the Rings. (2nd Ed.). England: Houghton Mifflin. In-text citation: (Tolkien, J.R.R., 1954).
- **Chapter/Article in an Edited Book:** Neilson, W. (2005). Physical Activity, Participation and Disability. In D. Fraser, R. Moltzen & K. Ryba (Eds.), Learners with Special Needs in Aotearoa New Zealand (3rd ed., pp. 411-422). Palmerston North, New Zealand: Dunmore Press. In-text Citation: (Neilson, 2005)
- **Article in a Journal** Reference for Printed Journal Article Pajunen, K. (2008). Institutions and inflows of foreign direct investment: a fuzzy-set analysis. Journal of International Business Studies, 39(4), 652-669.

  Reference for Online Journal Article El Gharras, H. (2009). Polyphenols: food sources, properties and applications - a review. International Journal of Food Science & Technology. 44(12), 2512-2518. Retrieved from doi:10.1037/rmh0000008 In-Text Citation for Off-line and On-line Journal Articles: (El Gharras, 2009)
- **Thesis/Dissertation** Shobhadevi, Y. J., & Bidarakoppa, G. S. (1994). Possession phenomena: As a coping behaviour. In G. Davidson (Ed.), Applying psychology: Lessons from Asia-Oceania(pp. 83-95). Carlton, Vic., Australia: Australian Psychological Society. In-Text Citation: (Shobhadevi and Bidarakoppa 1994)
- **For Online document** United States Environmental Protection Agency. (2007, May 4). Climate Change. Retrieved From the Environmental Protection Agency website: http://www.epa.gov/climatechange In-Text Citation: (United States Environmental, 2007)