International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 11 | Nov – 2025 DOI: 10.55041/ISJEM05219
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A Comprehensive Review of Blockchain Application across Multiple Domains: Current trends, Findings and Challenges.

Bhumi Lohar
Symbiosis Skills &
Professional University, Pune

Shreya Pardeshi
Symbiosis Skills &
Professional University, Pune

Aditya Mane
Symbiosis Skills &
Professional University, Pune

Dr. Parul Bhanarkar
Symbiosis Skills &
Professional University, Pune

Abstract- This survey paper presents a comprehensive examination of blockchain technology and its diverse applications across multiple domains. It begins by outlining the historical evolution and fundamental structure of blockchain systems, followed by an in-depth discussion of the core technologies that enable decentralized and secure operations. The study further explores the potential applications of blockchain, highlighting its transformative impact on various industries. Additionally, the paper analyzes the key challenges associated with blockchain adoption, offering insights into current limitations and areas requiring further research.

Keyword- Blockchain technology, Consensus mechanisms, Smart contracts, Cryptography, Distributed Ledger, Supply Chain Management, Healthcare Data Security, Identity Management, Asset Tokenization, Blockchain Applications

1. Introduction

Blockchain is a shared immutable ledger that facilitates the process of recording transactions and tracking assets across a business network. A Blockchain is a distributed database, which is shared over a computer network. Blockchain stores information electronically in a digital format to make transactions secure. It was created in 2008 by Satoshi Nakamoto to work as public distributed ledger for cryptocurrency transactions whose work was then done by work by Stuart Haber, W. Scott Stornetta, and Dave Bayer. This blockchain then solved the problem of double spending without the need of central authorities. Provided benefits such as better transparency, traceability, immutability and enhanced security.

This paper consists of: An overview of blockchain technology, its structure and implementation in Section 2. Technologies of blockchain covered in Section 3. Applications of blockchain in diverse domains in Section 4. Challenges that need to be overcome to utilize blockchain in its full potential in Section 5. Conclusion in Section 6.

2. Blockchain

2.1 History of blockchain-

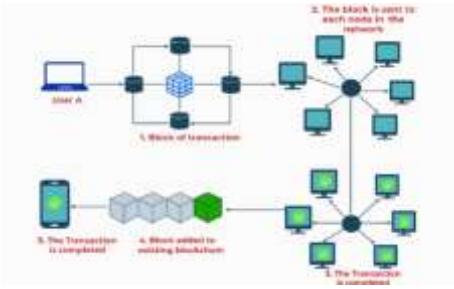
Blockchain technology began to take form in the early 1980s when David Chaum introduced the idea of a blockchain protocol [7]. In 1991, Stuart Haber and W. Scott Stornetta proposed a distributed timestamping system that used cryptographic methods to secure digital records [8]. Later, in the late 1990s, Nick Szabo expanded on this foundation by conceptualizing a digital currency that employed blockchain principles to ensure transaction security [9].A significant milestone occurred in 2008, when Satoshi Nakamoto published the Bitcoin white paper [10], presenting a peer-to-peer electronic cash system that relied on blockchain for transaction verification and security. The launch of Bitcoin in 2009 marked the beginning of a new era in digital currency [2].

In 2015, Vitalik Buterin introduced Ethereum, which extended blockchain's potential beyond digital currency to a general-purpose decentralized platform [11]. Ethereum enabled the creation of decentralized applications (dApps) that operate directly on the blockchain. These applications span various domains, including gaming, non-fungible tokens (NFTs), and decentralized finance (DeFi). To further improve the network's scalability, security,

and efficiency, the Ethereum Foundation announced the Ethereum 2.0 project in 2020, which remains under active development and is expected to reach full implementation by 2023.

2.2 Structure of blockchain-

The blockchain transaction operates, including its initiation, validation and ultimate confirmation via a distributed network. Block chain functions as a decentralized digital ledger that safely an openly records transactions across several computers. Every transaction is bundled into a block, which is subsequently added to a chain of earlier blocks after being validated by network nodes using consensus techniques. The data becomes unchangeable once it is uploaded, guaranteeing security and confidence without requiring a central authority. In digital systems, this procedure makes record-keeping secure, transparent, and impervious to tampering [20].



Followed steps are used:

1. Start the Transaction: Sending a transaction request (example., transferring digital assets) is how User A starts the process. The blockchain network receives this request for verification.
2. Verification of Transactions: A collection of linked database nodes receives the request. Before packing the transaction into a block, these nodes verify user credentials, digital signatures, and available balance.
3. Block Distribution: The transaction is sent to every node (computer) on the blockchain network when it is combined into a block. To verify the block's validity and correctness, each node examines it separately.
4. Method of Consensus: Using a consensus technique (such as Proof of Work or Proof of Stake) [21], all participating nodes concur that the transaction is legitimate. The Transaction is recognized as legitimate by the confirmed nodes, as shown by the green checkmarks.
5. Blockchain Added: The confirmed block is permanently added to the blockchain upon consensus, creating a sequential connection with earlier blocks while preserving immutability and transparency.
6. Verification of Transaction: At the end, the consumer receives the confirmation (displayed on the mobile device). The transaction is now finished, safely documented, and accessible to the blockchain ledger.

3. Technology of Blockchain

3.1 Distributed Ledger Technology –

DLT is a general protocol and structure for recording data in a distributed and secure fashion. It emphasizes the presence of a system that is controlled by a distributed network and has no central control. DLT secures data through cryptography and distributes them across the network for storage. This technology is designed to establish trust between parties that do not trust each other. Multiple copies of each record are kept and are linked together by a cryptographic algorithm, and all copies of data must be compromised for the intrusion to be successful[7].

Consists of components such as Nodes (individual devices that participate in DLT), Consensus (protocol used to achieve agreement on state of the ledger amongst nodes), Cryptography (used to secure data and ensure integrity) and Peer-to-Peer Network (decentralised network).

Distributed Ledger Technology (DLT) offers several transformative advantages over traditional centralized systems. It operates through decentralization, where multiple participants maintain synchronized copies of the ledger, minimizing the risks of data manipulation and single points of failure. With real-time updates, transactions are recorded and reflected instantly across all network nodes, ensuring accuracy and

immediate visibility into financial activities. The technology also enhances transparency by allowing authorized participants to access transaction records, thereby fostering trust and reducing the need for extensive audits. Through advanced cryptographic mechanisms, DLT ensures data integrity and security, making transaction histories immutable and resistant to cyberattacks. Additionally, by automating processes and eliminating intermediaries, DLT significantly reduces operational costs and enhances overall system efficiency.

3.2 Cryptography-

Cryptography is a method of securing data from unauthorized access. In the blockchain, cryptography is used to secure transactions taking place between two nodes in a blockchain network. In a blockchain there are two main concepts cryptography and hashing.

Cryptography is a collection of techniques and protocols designed to protect information from unauthorized access during communication. The term is derived from two Greek words *"Kryptos,"* meaning "hidden," and *"Graphein,"* meaning "to write." It ensures that data remains confidential and secure as it is transmitted or stored. In this process, encryption converts readable text (plaintext) into a random sequence of bits, known as ciphertext, making it unintelligible to unauthorized users. A key — a specific piece of information — is required to apply or reverse the cryptographic algorithm. Decryption is the reverse operation of encryption, transforming the random bit sequence back into its original plaintext form. The cipher refers to the mathematical algorithm used in this conversion process, enabling secure communication and data integrity.

In addition to blockchain technology, hash functions are widely used as fundamental encryption tools in various research, development, and application programs [8]. Hash functions output a fixed-size value regardless of the input length—a characteristic that this study aims to leverage. During the data-tracking process, exposing the actual values of the data poses a threat to security. Hence, this study applies the preimage resistance, collision resistance, and avalanche effect of hash functions. Furthermore, hash functions are advantageous for the rapid processing and validity verification of data in resource-constrained environments, preventing tampering with the original data. Therefore, in this study, the characteristics of hash functions are utilized to encrypt data and record them in the form of a hash chain.

3.3 Consensus Algorithm –

The Byzantine Generals Problem, proposed by Lamport, Shostak, and Pease (1982), illustrates the challenge of achieving consensus in unreliable or untrusted environments. In blockchain, this translates to the difficulty of maintaining consistent ledgers across decentralized nodes without relying on trust. To address this, Byzantine Fault Tolerance (BFT) mechanisms ensure that a distributed system can continue operating even if some nodes behave maliciously.[9]

Several consensus algorithms have been developed based on this principle:

- Proof of Work (PoW): Nodes compete to solve complex computational puzzles to add new blocks. The first node to find the correct solution receives a block reward.
- Proof of Stake (PoS): Nodes are chosen to validate blocks based on the amount of cryptocurrency they stake, reducing energy consumption compared to PoW.
- Proof of Capacity (PoC): Block creation rights are based on available storage capacity rather than computational power or stake.
- Delegated Proof of Stake (DPoS): A democratic model where nodes vote to elect delegates who validate transactions and create new blocks.
- Practical Byzantine Fault Tolerance (PBFT): A voting-based consensus ensuring network reliability even when up to one-third of nodes act maliciously.

The comparisons of the five consensus algorithms are listed -

	PoW	PoS	PoC	DPoS	PBFT
Setup	Public/private blockchain	Public/private blockchain	Public/private blockchain	Public/private blockchain	Private permissioned blockchain
Finality	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Immediate
Speed	Low	High	High	High	High
Energy Efficiency	Very low	High	High	High	Medium
Scalability	Good	Good	Good	Good	Bad
Resource Requirements	High	Medium	High	Medium	High
Example of use	Bitcoin Ethereum, Litecoin	Tezos, Ethereum2.0	NXT	EOS BitShares	Hyperledger, Chain

4. Application

1. Supply chain management

Supply chain management incorporates various blockchain techniques that can enhance traceability, security, and efficiency. It also allows supply chain finance to provide smooth processes of payment and builds trust in transactions between different parties. This blockchain technology makes it easier for compliance and auditing by recording regulatory data in a secure manner and prevents counterfeiting because the verification of goods' authenticity is obtained. Blockchain further enhances supplier management through the tracking of supplier reputations and allows collaboration by sharing data and enabling interoperability. It also contributes to sustainability and ethical sourcing since it guarantees transparency in material sourcing. By addressing key points, blockchain drives greater efficiency, accountability, and transparency across supply chains[10].

Blockchain techniques in supply chain management.

1. Detection of COVID-19 vaccines and supply chain traceability- ntegration of private and public blockchains helps to boost transaction capacity. Helping to standardize and govern the data flow could depend on blockchain technologies.

2. There is a requirement for more information about the provenance of the goods, lack of updated information, and hence, the difficulty of tracking the movement of the goods - Under a blockchain based supply chain, the data is verified and thereafter kept within the blockchain network. The immutability of the blockchain guarantees that the data stays unchangeable and unopposed to falsifying. As so, the recipient of such material might be quite confident in its accuracy and validity. Once the provider has kept data inside the blockchain network, it becomes accessible.

3. Capturing and storing substantial data with blockchain technology is a significant endeavour- The Inter Planetary File System (IPFS) provides an actual, real-world solution. IPFS is distributed file system that tries to connect all computational devices with a unified file system. IPFS allows people to use vast amounts of data and then add the immutable and permanent IPFS links into a transaction in a blockchain.

4. Issues with factory monitoring- IoT play a crucial role in generating and using digital data across the distribution process, intending to achieve enhanced transparency and traceability.

2. Healthcare

As far as healthcare is concerned, the urgency of development increases to more incredible speeds. Today the need is for quality health facilities supported by advanced and newer technologies. Here, Blockchain would play a critical role in transforming the healthcare sector. In addition, the landscape of the health system is moving towards a patient-centred approach focusing on two main aspects: accessible services and appropriate healthcare resources at all times. The Blockchain enhances healthcare organisations to provide adequate patient care and high-quality health facilities. Health Information Exchange is another time-consuming and repetitive process that leads to high health industry costs, quickly sorted out using this technology. Using Blockchain technology, citizens may take part in health study programs. In addition, better research and shared data on public wellbeing will enhance treatment for different communities. A centralised database is used to manage the entire healthcare system and organisations[3].

The Blockchain makes the entire prescription process transparent, from manufacturing to pharmacy shelves. Congestion, freight direction, and speed may all be tracked using IoT and Blockchain. It offers the chance to schedule acquisitions efficiently to prevent disruptions and shortages in clinics, pharmacies, and other medical facilities with a given medication. The deployment of digital frameworks built on Blockchain would help ensure that the logistics data avoid uncontrolled adjustments. It increases trust and prevents the illicit handling of records, payments, and medication

themselves by various people interested in purchasing drugs[3].

Significant applications Blockchain for healthcare.

1. Store information of an individual patient- Before and after the different clinical study phases, a significant amount of patient information and health data is generated. There are many people's blood tests, quality assessments, estimates, and wellness polls. It can provide results that show the existence of some document or record. Healthcare providers traverse the stored data and suspect its validity, and they will check this seamlessly by matching it to the original records stored on the Blockchain system. Blockchain is based on existing cryptographic techniques, which include the appropriate framework for cryptography for data sharing.

2. Validation- Transactions are validated in a Blockchain until they are linked to the chain and are done by algorithms. The authenticity is sealed until the material is encrypted, digitally signed and saved.

3. Safety and transparency- It provides excellent safety and transparency while enabling physicians to devote more time to treat patients. It would also allow supporting clinical trials and treatments for any rare disorder. Smooth data exchange among providers of medical solutions can contribute to diagnostic precision, efficient therapies and cost-effective ecosystems in a healthcare system.

4. Health record keeping- Blockchain can be a perfect technology for record-keeping in the medical world. Its applications include sharing healthcare data, keeping electronic healthcare records, managing insurance, and performing administrative tasks. Patients can send their health information via an app to a Blockchain network.

5. Display information- The Blockchain system will display information about the origins of the medication to ensure high quality and that the approved medicine's manufacturer supplies it. Blockchain provides better protection than ever for sensitive data, provided that it is appropriately used.

3. Digital identity management

Digital Identity is an online identity which is created by an individual in cyberspace. Just like the information on a passport identifies the owner for a specific purpose, the digital identity recognizes the holder of the identity with some digital identifiers like E-mail address, domain name or some URL[5].

The traditional IdM models have been designed effective for the service providers but not for the user because the users have to remember multiple passwords for accessing multiple web sites. A classification of various IdM strategies is given which includes the aspects like privacy and usability of IdM solutions. At the very basic level, IdM consists of service provider and the service consumer who can perform any kind of transaction without worrying about the security and the privacy associated with each transaction. By including an identity provider can help to establish the trust between the two. Traditional IdM systems were centralized and controlled by a single entity. The authentication and authorization was guaranteed by a “Trusted third party”. Several IdM models have been proposed in the past . The main function of any IdM system is to bind together the “identifier” and the “attributes” securely . According to poorly designed IdM systems can aggravate existing security problems and create opportunities to extract personal information from users. Security, Privacy and Anonymity are the major challenges while building a successful IdM system . Experts have considered Affordability, Integrity, Trustworthiness and Interoperability as important factors for a good IdM system[5].

4. Asset tokenization

The process of turning ownership rights or entitlements of both physical and intangible assets into digital tokens that are kept on a distributed ledger via blockchain technology is known as asset tokenization.

Tokenization allows real-world assets such as stocks, real estate, commodities, and artwork to be

represented, divided and safely exchanged on blockchain-based systems [15].

1. Fractional Ownership and Accessibility: By dividing valuable assets into smaller, tradeable units, tokenization makes it possible for retail investors to participate in the market and democratizes investment opportunities.
2. Automation of Smart Contract: By automating revenue sharing, dividend distribution, and compliance verification, blockchain-based smart contracts can minimize human error and oversight.
3. Immutability and Transparency: Every transaction involving tokenized assts is documented indefinitely, guaranteeing traceability and building investor confidence.
4. Increased Liquidity: Digital platforms make it possible to trade traditionally illiquid assts like infrastructure or real estate, allowing for round-the-clock secondary market trading.
5. Interoperability and Global Reach: Tokens can be traded internationally without the need for centralized middlemen, expanding market access and cutting expenses [15].

Implementation in Developing Economies and Emerging Markets [EMDEs]- It emphasizes how blockchain-based tokenization can transform infrastructure funding in EMDEs by bringing in international capital, enhancing transparency and lowering corruption through unchangeable records. Through tokenization, governments and private developers can diversify funding sources, draw in micro investments and use blockchain analytics to automate compliance reporting [16].

5. Smart contracts

A smart contract is a self-executing digital contract that is maintained on a blockchain. When certain conditions are satisfied, the contract's provisions are automatically carried out. Smart contract combines distributed consensus, automation and cryptographic security to do away with the need for intermediaries like banks, brokers or notaries. Once deployed, they become unchangeable parts of the blockchain ledger. They are developed in programming languages like Solidity, Chain code.

1. Autonomy: Once implemented, smart contracts operate autonomously, carrying out logic on their own without outside intervention.
2. Immutability: Contract code and execution history are unchangeable, guaranteeing dependability and integrity.
3. Transparency: The contract state is accessible to all nodes, which enhances stakeholder confidence and auditability.
4. Security: Smart contract is resistant to manipulation and illegal alteration since they are based on consensus procedures and cryptographic primitives.
5. Interoperability: By integrating with IoT systems, or APIs, smart contracts enable automation in the real world [21].

Blockchain benefits from Smart Contract:

- Automation of Transactions: By automating blockchain-based processes smart contract increase blockchain efficiency and trust while lowering the need for human intervention .
- Event Driven Execution: They provide event driven blockchain designs which enhance real-time blockchain interactions by enabling automated triggers when certain criteria are satisfied.
- Decentralized Applications [Dapps]: They make it possible to develop decentralized apps that operate on top of blockchain networks without the need for middlemen, extending the use of blockchain technology beyond financial transactions.
- Enhanced Trust in Multi-Party Systems: Smart contracts enable safe blockchain transactions between several parties without the requirement for a central authority or mutual trust.
- Decreased Transaction Costs: Smart contract reduces intermediary and enforcement costs by automating financial and legal agreements on blockchain.
- Improved Transparency and Auditability: A Smart contract's activities are all documented on the blockchain, offering complete traceability and transparency [21].

5. Challenges

Though blockchain has given strong support to manage security, still blockchain technology is facing challenges. Some of the challenges have been described here:

1. Scalability - There is an increase in blockchain usage volume and rise in the number of transactions occurring daily basis, blockchain has become huge in size. Transactions are stored in nodes for getting validation. First, the current transaction source needs to be validated before transaction itself. The block size restriction and time break required to produce new block plays a major role in not satisfying requirement for the simultaneous processing of millions of transactions in real time environment. In few cases, size of block may also create issue in delay of transaction [22]

2. Security- Security refers to the terms like integrity, availability and confidentiality. As all knows, confidentiality will be low in distributed networks, as well as integrity is also a major concern. In this case, availability will be not an issue as replication is there. Another major concern is 51% majority attack. In this case, one miner can get full control of the chain. Also there will be challenges like prevention from DDoS attack, Trojans and viruses from adware etc. [22]

3. Regulation problems The major challenge in case of blockchain implementation is rules and regulations of various countries. The concept of decentralized structure will make the control of central bank weak from the viewpoint of economic policy and money transactions amounts. Concerned authority need to pay attention on research on this issue and identify new strategy and formulating new policies.[22]

6. Conclusion

This research paper provides a comprehensive exploration of blockchain technology, outlining its core characteristics, structural components, and the mechanisms that enable trustless decentralized ecosystems. It examines major consensus algorithms and highlights their operational distinctions, offering clarity on how they influence blockchain performance and security. Additionally, the study emphasizes the transformative role of smart contracts in automating processes and reducing intermediaries across various sectors.

A detailed analysis of key application domains—supply chain management, healthcare systems, identity management, and asset tokenization—demonstrates the significant advantages that blockchain introduces in terms of transparency, traceability, data integrity, and efficiency. In supply chains, blockchain enhances product authenticity and real-time tracking; in healthcare, it strengthens data security and interoperability; in identity management, it supports secure, self-sovereign identities; and in asset tokenization, it enables fractional ownership and democratized access to digital and physical assets.

7. Reference

[1] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” Healthcare, vol. 7, no. 2, p. 56, 2019. doi: 10.3390/healthcare7020056.

[2] The Institution of Engineering and Technology, Blockchain in healthcare, 2018. [Online]. Available: https://www.theiet.org/media/9484/blockchain-in-healthcare.pdf

[3] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, “Blockchain technology applications in healthcare: An overview,” International Journal of Intelligent Networks, vol. 2, pp. 130–139, 2021. doi: 10.1016/j.ijin.2021.09.005.

[4] D. Elangovan et al., “The Use of Blockchain Technology in the Health Care Sector: Systematic Review,” JMIR Medical Informatics, vol. 10, no. 1, p. e25226, 2022. [Online]. Available: https://preprints.jmir.org/preprint/17278

[5] T. Rathee and P. Singh, “A systematic literature mapping on secure identity management using blockchain technology,” Journal of King Saud University – Computer and Information Sciences, 2021. doi: 10.1016/j.jksuci.2021.03.005.

[6] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, “Blockchain-based identity management systems: A review,” Journal of Network and Computer Applications, vol. 166, p. 102731, 2020. [Online]. Available:

https://www.sciencedirect.com/science/article/abs/pii/S1084804520302058

[7] A. Sunyaev, "Distributed ledger technology," in Internet Computing. Berlin/Heidelberg, Germany: Springer, 2020, pp. 265–299.

[8] S. Kim and D. Kim, "Data-Tracking in Blockchain Utilizing Hash Chain: A Study of Structured and Adaptive Process," [Journal/Publisher unspecified].

[9] J. Liu and J. Wu, "A Comprehensive Survey on Blockchain Technology and Its Applications," [Journal/Publisher unspecified].

[10] "Blockchain technology in supply chain management: Innovations, applications, and challenges," International Journal of Supply Chain Management, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772503025000192

[11] "Blockchain Technology for Global Supply Chain Management: A Survey of Applications, Challenges, Opportunities and Implications," IEEE Access, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10529266

[12] "Exploring Blockchain Research in Supply Chain Management: A Latent Dirichlet Allocation-Driven Systematic Review," Information, vol. 14, no. 10, p. 557, 2023. [Online]. Available: https://www.mdpi.com/2078-2489/14/10/557

[13] "Blockchain in Supply Chain Management," European Journal of Engineering and Technology Research, 2022. [Online]. Available: https://www.researchgate.net/publication/364580709_Blockchain_in_Supply_Chain_Management

[14] A. Buldas et al., "An Ultra-Scalable Blockchain Platform for Universal Asset Tokenization: Design and Implementation," IEEE Access, vol. 10, pp. 77284–77322, 2022. doi: 10.1109/ACCESS.2022.3192837.

[15] O. Ross, J. R. Jensen, and T. Asheim, "Assets under Tokenization," SSRN, 2019. doi: 10.2139/ssrn.3488344.

[16] Y. Tian et al., "Asset Tokenization: A Blockchain Solution to Financing Infrastructure in Emerging Markets and Developing Economies," SSRN, 2020. doi: 10.2139/ssrn.3837703.

[17] N. Afraz, F. Wilhelmi, H. Ahmadi, and M. Ruffini, "Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis," IEEE Access, vol. 11, pp. 95653–95666, 2023. doi: 10.1109/ACCESS.2023.3309423.

[18] Y. Li, "Emerging blockchain-based applications and techniques," Service Oriented Computing and Applications, vol. 13, pp. 279–285, 2019. doi: 10.1007/s11761-019-00281-x.

[19] R. Chatterjee and R. Chatterjee, "An Overview of the Emerging Technology: Blockchain," in Proc. 3rd Int. Conf. Computational Intelligence and Networks (CINE), Odisha, India, 2017, pp. 126–127. doi: 10.1109/CINE.2017.33.

[20] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," IEEE Access, vol. 9, pp. 43620–43652, 2021. doi: 10.1109/ACCESS.2021.3065880.

[21] B. K. Mohanta, S. S. Panda, and D. J. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," in Proc. 9th Int. Conf. Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018, pp. 1–4. doi: 10.1109/ICCCNT.2018.8494045.

[22] D. Meva, "Issues and Challenges with Blockchain: A Survey," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 12, 2018