www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-**12**, Issue-**6**, December **2024**
Research Paper

Int. J. Sc. Res. in Network Security and Communication

E-ISSN:2321-3256

Exploration of Blockchain Technology for Enhanced Data Security in Small and Medium Enterprises

Mani Arora

Assistant Professor, Khalsa College, Amritsar, India

Author's Mail Id: maniarora@khalsacollege.edu.in

Received: 18/Oct/2024, Accepted: 20/Nov/2024, Published: 31/Dec/2024

Abstract— Small and Medium Enterprises (SMEs) constitute a significant portion of the global business landscape, yet they often face challenges in fortifying their data security infrastructure. This research paper investigates the integration of blockchain technology to enhance data security in Small and Medium Enterprises (SMEs). SMEs, often constrained by limited resources, face significant challenges in securing sensitive information. The study assesses the current data security landscape in SMEs, identifying vulnerabilities and exploring the potential of blockchain as a robust solution. Emphasizing decentralization and tamper resistance, the paper highlights how blockchain can fortify data security, offering benefits such as improved integrity and transparent audit trails. Practical considerations, including integration challenges and user adoption, are addressed, providing actionable insights for SMEs seeking to fortify their data security through blockchain implementation. The research contributes to the evolving discourse on cybersecurity in SMEs, offering a foundation for practical applications in blockchain technology for enhanced data protection.

Keywords— Blockchain, Data Security, Small and Medium Enterprises (SMEs), Cyber Threats, Information Protection

I. INTRODUCTION

Small and medium-sized enterprises (SMEs) make up most global businesses, playing a vital role in driving economies and encouraging innovation. The criteria for categorizing SMEs vary widely from country to country, with different regions using factors such as the number of employees, annual turnover, capital investment, or a combination of these. For instance, the International Finance Corporation (IFC) and the European Commission consider firms with fewer than 250 employees as SMEs, with additional criteria like annual turnover and balance sheet total. In India, micro, small, and medium enterprises (MSMEs) are classified based on turnover and machinery investment, with businesses falling within the MSME category if their turnover is below INR 250 crores and their investment in plants and machinery is not more than INR 50 crores.

Data security is a critical concern for Small and Medium Enterprises (SMEs) as they increasingly rely on digital technologies to conduct business. SMEs face unique challenges in safeguarding their data, including limited resources, expertise, and awareness compared to larger enterprises. In numerous enterprises engaged with data providers, collectors, and processors, effective data management has emerged as a key priority. The conventional approach adopted by SMEs is insufficient to maintain current global business operations [4].

Blockchain technology represents one of the most recent approaches to decentralized data storage, minimizing unauthorized access to stored data through the establishment of trust. In the realm of blockchain, information is stored in a distributed ledger. The integrity and availability essential for participants to write, read, and verify transactions within the blockchain network are provided by blockchain technology. Notably, this technology prohibits deletion and modification operations on transactions and other ledger-stored information. The cryptographic primitives and protocols supporting the blockchain system, such as digital signatures and hash functions, ensure that ledger-recorded transactions are protected in terms of integrity, authenticity, and non-repudiation. Additionally, as a distributed network, blockchain relies on a consensus protocol, a set of rules followed by all participants to achieve a globally unified perspective on the recorded transactions.

In an environment where trust is not assumed, blockchain offers users desirable features including decentralization, autonomy, integrity, immutability, verification, fault-tolerance, anonymity, auditability, and transparency [[1], [2], [3]]. These advanced features have garnered significant attention from both academic and industrial sectors in recent years. Previous research has explored the theoretical foundations and the international expansion of SMEs [5]. Despite the importance of these studies, there are gaps in understanding the connection between processes aimed at strategizing, synergizing, and standardizing, and the overall business performance of SMEs [6]. Furthermore, these studies have identified a knowledge gap in the application of Blockchain Technology (BCT). Consequently, there is a suggestion for additional academic research to address these gaps and enhance BCT-driven global market operations.

Protecting information and controlling data access is essential for organizations handling large amounts of company and employee data. Managing this data has become a major challenge for organizations that collect, provide, and process information. Blockchain technology is a modern solution for decentralized data storage, designed to reduce unauthorized access and build trust. Some studies [7] [8] have explored how to address privacy concerns in big data. Several systems have been created to secure personal data, including methods like anonymizing data to protect sensitive information, using differential privacy to add random noise during data sharing, and encryption techniques that allow processing without revealing the original data [9]. This study focuses on exploring how blockchain technology can solve privacy issues in data management. It will cover common data privacy problems, explain how blockchain works, and analyze how this technology can effectively protect sensitive information.

II. AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain technology represents a distributed, decentralized, and duplicated record-keeping system. It can take different shapes, including public or private structures, and can be either permissioned or permissionless. It may also function with or without the involvement of tokenized crypto-economics. This cohesive framework ensures the permanence of data, security through cryptography, accurate time-stamping, and thorough auditability. These features together create a transaction record that is pure and unalterable [10]. The fundamental characteristics of this system create an environment resistant to censorship and manipulation, thus preserving the integrity of transactions. Initially gaining prominence with the emergence of Bitcoin (Blockchain 1.0), this technology has since broadened its scope. It introduced the concept of smart contracts (Blockchain 2.0) and extended its applications to various fields (Blockchain 3.0), including healthcare, education, and governance. Originally emerging from a 2008 paper called “Peer-to-peer electronic cash transfer” by an individual or group under the pseudonym Satoshi Nakamoto, blockchain technology has since achieved considerable recognition [11]. Moving away from the conventional centralized client-server approach, it adopts a decentralized peer-to-peer structure, providing a range of uses beyond just digital currency [12]. The evolution of blockchain is characterized by distinct stages, highlighted by its integration into various industries and the development of consensus mechanisms, smart contracts, and blockchain-based tokens. Blockchain networks depend on consensus algorithms for establishing consensus about the validity and order of transactions among participants [13]. These algorithms cater to varied objectives. Some notable examples are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). Bitcoin employs PoW, which confirms transactions by solving complex mathematical problems, a process that is resource-intensive. PoS and DPoS present less energy-intensive alternatives, though they pose issues such as the potential for wealth concentration. PBFT, used in permissioned blockchains, ensures agreement among verified nodes.

Smart contracts represent automated contracts embedded in the blockchain, executing themselves when certain conditions are met. They function by activating predefined rules in response to specific events, thereby removing the need for middlemen and ensuring secure and reliable contract fulfilment [13]. Crafted in specialized programming languages tailored for blockchain, such as Solidity for Ethereum, smart contracts provide efficiency, security, transparency, and unchangeability. Their uses span various sectors, including finance, supply chain management, and real estate. Continuous improvements are being made in smart contract security, focusing on formal verification methods, and enhancing interoperability among different blockchain systems.

Blockchain tokens represent digital assets with either value or utility within a blockchain environment [14]. These encompass cryptocurrencies and utility tokens. Cryptocurrencies, like Bitcoin and Ethereum, are used as digital money, whereas utility tokens grant access to specific features in decentralized applications. Tokens enable smooth transactions, enhance transparency, and support innovative business models, including decentralized finance. The introduction of new token standards such as ERC-20, ERC-721, and ERC-1155 broadens opportunities for distinctive assets and intricate token ecosystems. The ongoing development of blockchain has led to its application in various fields, offering decentralized alternatives to conventional challenges. Through mechanisms like consensus algorithms, smart contracts, and blockchain tokens, this technology fosters a new framework of trust, transparency, and efficiency across different digital domains.

III. RELATED WORK

Data security has emerged as a critical concern for SMEs, given the increasing frequency and sophistication of cyber threats and data breaches [15]. According to the "2019 Data Breach Investigations Report" by Verizon, 43% of cyber-attacks target small businesses, emphasizing the vulnerability of SMEs in the digital landscape. The literature survey suggests that the lack of robust data security infrastructure and limited resources often leave SMEs susceptible to various cyber threats, including malware, phishing attacks, and data breaches.

In response to these challenges, researchers and industry experts have increasingly turned to blockchain technology as a potential solution for enhancing data security. Blockchain, originally developed as the underlying technology for crypto currencies, has gained attention for its potential applications beyond finance [16]. In the context of data security, blockchain's decentralized and immutable ledger offers the promise of enhanced data

integrity and security, making it an attractive option for SMEs looking to bolster their cyber security measures.

Studies have highlighted the key features of blockchain that make it particularly suitable for addressing data security challenges. The immutability of data stored on the blockchain ensures that once information is recorded, it cannot be altered retroactively without the alteration being readily apparent. This characteristic significantly reduces the risk of unauthorized data tampering, providing a more secure data storage and transaction environment.

Moreover, the decentralized nature of blockchain eliminates the single point of failure, making it inherently more resilient against cyber-attacks. The literature emphasizes that by distributing data across a network of computers rather than storing it in a centralized database, blockchain minimizes the risk of data breaches and unauthorized access, thereby enhancing the overall security posture of SMEs.

Several case studies and pilot projects have demonstrated the practical application of blockchain in data security for SMEs. For instance, a case study conducted by the International Data Corporation (IDC) showcased how a blockchain-based data security solution enabled an SME in the retail sector to secure its customer data effectively [17]. By implementing blockchain, the company was able to ensure the integrity and confidentiality of sensitive customer information, thereby enhancing customer trust and loyalty [18]. Examining the dataset on blockchain vulnerabilities reveals a rise in attacks with the introduction of new blockchains over the years (Fig. 2). However, Figure 1. distinctly illustrates that once the cause is identified, subsequent blockchain research has actively enhanced security measures [19].

Additionally, the literature highlights the importance of considering the scalability and interoperability of blockchain solutions in the context of SMEs. As SMEs often operate with limited resources and technical expertise, the scalability and compatibility of blockchain technology with existing systems are crucial factors to ensure a smooth integration process without disrupting daily operations.

Overall, the existing literature underscores the potential of blockchain technology in addressing the data security challenges faced by SMEs. By leveraging blockchain's inherent security features, SMEs can establish a robust and resilient data security framework, thereby mitigating the risks associated with data breaches and cyber-attacks.

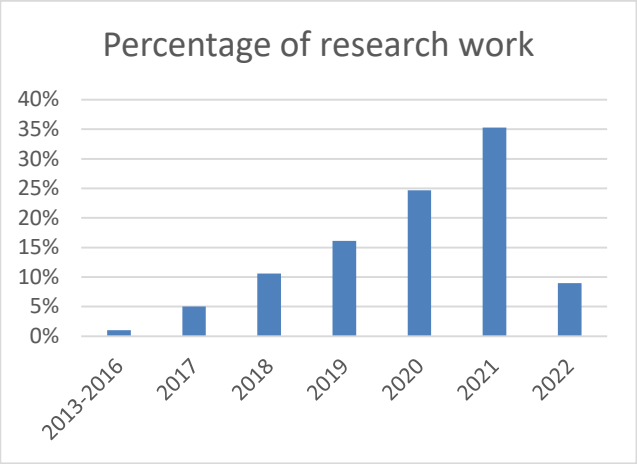

Fig1. Research work done towards blockchain in cyber security

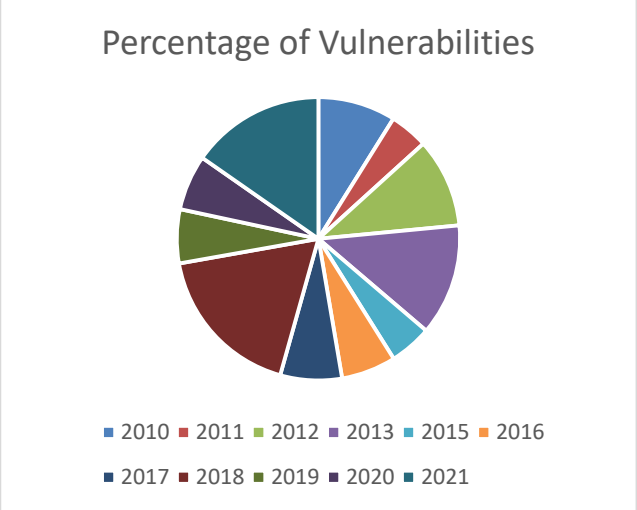

Fig 2. Different vulnerabilities discovered in blockchain domain

IV. BLOCKCHAIN DRIVEN SME GLOBAL OPERATIONS

In the aftermath of the COVID-19 pandemic, the speed at which Small and Medium-sized Enterprises (SMEs) operate internationally has become a critical aspect of their global strategic planning, significantly influencing their expansion into overseas markets. This is particularly relevant for Indian SMEs, which, despite their potential, often lack a strong technological foundation. To thrive in a competitive landscape, these enterprises must find ways to enhance their operational efficiency. Blockchain Technology (BCT) presents a viable solution, potentially bolstering the correlation between the rapidity of SMEs' international activities and their overall integrated business performance (IBP). Some of the SME global operations that blockchain is driving are:

1. **Enhanced Supply Chain Transparency:** Blockchain provides an immutable ledger, enabling SMEs to trace the origin, quality, and journey of products with absolute certainty. This transparency is crucial for businesses dealing with international supply chains, ensuring the authenticity and compliance of goods [20].

2. **Streamlined Payments and Remittances:** Cross-border transactions are often a challenge for SMEs due to high fees and slow processing times. Blockchain facilitates faster and more cost-effective international payments, bypassing traditional banking systems and their associated costs [21].
3. **Smart Contracts for Efficient Operations:** Smart contracts automate and enforce agreements between parties, reducing the need for intermediaries. This automation is particularly beneficial for international trade, where legal and compliance issues can be complex and varied across borders [22].
4. **Access to Global Markets:** Blockchain platforms can connect SMEs directly with trade. Blockchain's inherent characteristics like international buyers and suppliers, opening new market opportunities. This direct connection reduces reliance on middlemen, which can be cost-prohibitive for smaller businesses [23].
5. **Improved Assets Data Security and Privacy:** For SMEs handling sensitive data, blockchain offers advanced security features. The decentralized nature of blockchain makes data less vulnerable to cyber-attacks, a critical consideration in the digital age [24].
6. **Facilitating Trust in Transactions:** Trust is a significant factor in international immutability and transparency help in building trust among parties who do not have established relationships [25].
7. **Tokenization of Assets:** SMEs can leverage blockchain to tokenize their assets, making it easier to raise capital by selling digital tokens representing ownership or investment in the company [26].
8. **Compliance and Record Keeping:** Blockchain can simplify compliance with international regulations by providing a secure and unchangeable record-keeping system. This feature is particularly useful for SMEs that may not have extensive resources to dedicate to compliance management [27].
9. **Intellectual Property Protection:** For SMEs in creative industries or with proprietary technologies, blockchain can provide robust protection of intellectual property rights on a global scale [28].
10. **Decentralized Finance (DeFi) for SME Funding:** Blockchain opens new avenues for SME financing through DeFi platforms, offering alternatives to traditional banking and lending systems [29].

So blockchain is empowering SMEs in their global operations by offering solutions that are secure, efficient, and cost-effective, thereby levelling the playing field with larger corporations and opening new growth opportunities in the global market.

V. DATA SECURITY ISSUES IN SMES

The realm of IT security threats is extensive and constantly changing. These threats include activities like reconnaissance, collecting information, executing phishing schemes, creating fake websites, generating fraudulent certificates, and introducing malware into internal information systems. These varying threats present substantial obstacles in ensuring the security and integrity of information systems. Some of the major data security issues are due to following reasons:

1. **Cybersecurity Challenges**: SMEs often grapple with cybersecurity issues due to limited resources and expertise [30].
2. **Resource Constraints**: Unlike larger enterprises, SMEs typically have fewer financial and technical resources to allocate towards comprehensive cybersecurity [31]. Limited investment in advanced cybersecurity infrastructure leaves SMEs vulnerable.
3. **Vulnerability to Cyber Attacks**: SMEs are increasingly targeted by cybercriminals due to perceived weaker security systems [32]. Many SMEs lack specialized IT staff, leaving them more susceptible to cyber threats. Poor data management and inadequate backup solutions are common in SMEs, leading to potential data loss.
4. **Compliance and Regulatory Challenges**: SMEs struggle to keep up with changing data protection regulations, such as GDPR [33]. Employees in SMEs often do not receive adequate training on cybersecurity best practices
5. **Lack of Information Security Policy**: Numerous small and medium-sized enterprises aim to attain comprehensive information security, yet often fall short in establishing a clear information security policy. This absence not only obscures their broader security objectives but also hinders their ability to recognize and address immediate threats.

VI. INTEGRATION OF DATA PRIVACY AND BLOCKCHAIN IN SME

The concept of data privacy is multifaceted and lacks a universally accepted, comprehensive definition due to the varying perspectives from which researchers assess privacy concerns. The interpretation of data privacy issues often depends on the standpoint of the individual or entity involved. For individual users, data privacy pertains to the protection of their personal and private information, which becomes a concern when such data is revealed to unentitled parties without the user's permission. In the context of an organization, data privacy involves safeguarding sensitive information about the business from competitors. A breach in this context, where confidential information is leaked, signifies a compromise in the organization's data privacy.

Data privacy concerns the regulation and management of how consumer information is disseminated and utilized. This includes, but is not limited to, demographic details like age and income, which can be used for individual identification, as well as search history and personal profile data [34] [35].

Privacy is a complex issue that demands a thorough exploration of various aspects to fully grasp its significance. The way database managers implement

privacy controls often reflects their understanding of privacy concerns. In the realm of data privacy, there are four technical dimensions to consider: data providers, who are individuals or organizations that supply data for storage; data collectors, who initially gather, use, and store data from providers; data users, who are individuals or organizations requesting the acquired data as third parties; and the data warehouse itself, which serves as the central repository of data and plays a crucial role in data privacy matters.

The governance of data privacy revolves around fundamental principles. These include the necessity to clearly state the purpose of data collection, obtaining explicit consent from data subjects, ensuring that data collection and usage are restricted only to what is essential, and limiting data disclosure and retention as much as possible. Additionally, it is crucial to maintain the accuracy of the collected data, implement robust security measures, and provide transparency to data providers, allowing them to verify adherence to these principles.

They pinpointed four key aspects to comprehend data privacy: purpose, visibility, granularity, and retention [36]. This includes the clear delineation of data usage responsibilities, access, and the provision of robust security measures to ensure data protection. Data collectors are also instructed on the duration for which they can retain data and the entities to which they can disclose it, based on the consent provided by the data provider. Frequently, data sources or owners lack control over their data, such as its usage and retention period. Many data controllers often distribute data at their disposal with little or no regard for privacy regulations. Technologies that empower data owners with control over their data – determining how it is used by businesses and authorities without sacrificing security and their ability to offer personalized services – are crucial in providing technical solutions to data privacy challenges.

Many organizations are utilizing smart devices that gather personal data and store it in databases. These Internet of Things (IoT) objects are interconnected and equipped with internet capabilities. They collect vast amounts of information from their environment and exchange it with one another over software systems. This results in the generation of extensive data, which is utilized by dependent services like online marketing. However, this raises significant data privacy concerns, as these devices disseminate personal information that could potentially disclose the identities of their users [37].

The practice of aggregating information from diverse sources, amalgamating and altering it through sophisticated software, and then marketing it as a product, often violates the fundamental principle of obtaining consent from data providers. This situation has prompted calls for enhanced privacy protection measures from governments. The unauthorized disclosure and misuse of personal user data are now central concerns in the realm of information security within organizations. Companies are increasingly worried about the potential damage to their business caused by data theft, as well as the misuse of such data to undermine their business operations. Illegitimately obtained data can tarnish the reputation of individuals or organizations, leading to loss of public image and business relationships. Addressing and securing this data is therefore a top priority for governments, businesses, and individuals alike.

While there are various legal, ethical, and policy measures proposed for data privacy protection, they fall outside the purview of this paper. Instead, this paper aims to explore privacy protection through technical initiatives, with a particular focus on Blockchain technology, as previously mentioned, forming the core of the discussion.

To protect data privacy on the blockchain, sensitive information is converted into a hashed format, which links to a secure data storage system outside the blockchain. Blockchain provides pseudonymity, meaning users have a virtual identity to perform transactions. The security of the blockchain relies on the proof-of-work mechanism and the trustworthiness of miners. Effective data privacy management involves spreading data across decentralized systems that are designed to be private. One key benefit of blockchain is its decentralized nature, where no single authority controls the data, and transactions are permanent and unchangeable. These recorded and verified transactions help identify and prevent data misuse or tampering. This is made possible through peer-to-peer networks, which are a core feature of blockchain technology [37] .

Blockchain operates as a decentralized, peer-to-peer system, employing the proof-of-work consensus algorithm that depends on the collaboration of individual nodes for the transmission of information. To improve security and ensure information integrity on the blockchain, cryptographic public keys are used for authentication. This reduces the need for third parties and enhances transaction security and privacy. For example, Bitcoin uses cryptographic Proof of Work (PoW) and a series of hashed addresses, making it secure and private even when dealing with unknown users. Similarly, Bit-message is an application that ensures anonymity in a trustless network by sending encrypted messages within message streams. In these systems, the identities and profiles of data owners remain private, ensuring confidentiality without relying on trust [38] [39]. Blockchain technology can be leveraged to automate the control over the collection, storage, and distribution of sensitive information, utilizing the ledger as a binding confirmation for data access or storage due to its immutable nature. In parallel, researchers are developing a protocol intended to overlay existing blockchain infrastructure. This new protocol introduces the concept of 'secret contracts', differing from 'smart contracts', by enabling nodes within the blockchain to process data without accessing or 'seeing' it. This innovation would empower users to retain control over their personal data,

thwarting its exploitation by online platforms. As a result, this approach could significantly bolster the trustworthiness of these systems without necessitating individual users to provide access to their specific personal information.

VII. POTENTIAL OF BLOCKCHAIN AS A SOLUTION

The increasing frequency and sophistication of cyberattacks highlight the critical need for robust data security solutions. Blockchain technology emerges as a promising and innovative approach to addressing these concerns, offering a range of features like immutable data ledger, cryptographic security, decentralization and resilience**,** Smart Contracts for Automated Security Measures that can significantly enhance data security for SMEs.

Blockchain's cryptographic nature offers enhanced security features [40] using advanced cryptographic techniques. Blockchain employs cryptographic hash functions to secure data. Each block in the chain contains a unique hash, which is a fixed-size string of characters generated from the block's data. Any change in the block's data, even a minor one, will result in a completely different hash. This makes it extremely difficult for anyone to alter past blocks without changing all subsequent blocks, thereby ensuring the integrity of the entire chain. Also, Blockchain utilizes asymmetric cryptography, where each participant in the network has a pair of cryptographic keys: a public key and a private key. The public key is visible to everyone, while the private key is kept secret. Transactions are signed with the private key, and the corresponding public key is used to verify the authenticity of the signature. This ensures secure and verifiable transactions.

The decentralized structure of blockchain can prevent common cyber-attacks. Blockchain operates on a decentralized network of nodes, where each node has a copy of the entire blockchain. This distributed nature adds a layer of security as there is no central point of failure. Hacking or compromising a single node would not grant unauthorized access to the entire network or alter the entire blockchain. Also Blockchain relies on consensus mechanisms to agree on the state of the ledger. Popular mechanisms include Proof of Work (PoW) and Proof of Stake (PoS). In PoW, participants (miners) solve complex mathematical problems to validate transactions and create new blocks, while in PoS, validators are chosen to create new blocks based on the amount of cryptocurrency they hold. These mechanisms prevent malicious actors from taking control of the network.

Blockchain's immutability ensures data integrity, making it difficult to tamper with stored data [41]. Once a block is added to the blockchain, it is nearly impossible to alter its contents due to the cryptographic links between blocks and the consensus mechanism in place. This immutability ensures a tamper-resistant record of transactions.

Blockchain provides transparency in transactions, which is beneficial for auditing purposes [42]. It enables all participants in the network to access a shared and synchronized version of the ledger. This transparency enhances accountability and facilitates auditing processes. SMEs can benefit from a more transparent system that allows them to trace the flow of data and transactions within their networks. Blockchain platforms often support smart contracts, self-executing contracts with the terms of the agreement directly written into code. Smart contracts automatically enforce the agreed-upon rules, eliminating the need for intermediaries and reducing the risk of fraud.

VIII. CONCLUSION

Recently, blockchain technology has emerged as a highly regarded disruptive innovation, heralded as a potential ultimate solution for information security and data privacy breaches. Despite being in its nascent stages, various governments and prominent organizations are actively researching how this technology could safeguard critical data, including land records, patient health records, supply chain data, and online platform data privacy. However, the implementation of blockchain remains limited, indicating its early developmental phase. This paper primarily aims to assess blockchain's efficacy as a data privacy solution.

Blockchain technology offers promising avenues for enhancing data security in SMEs. However, the implementation of such technology must be carefully considered, considering the specific challenges and needs of SMEs. Further research and development in this area could make blockchain solutions more accessible and effective for SMEs in the future.

REFERENCES

[1] M.S. Ali, M. Vecchio, M. Pincheira, *et al.*, "Applications of blockchains in the internet of things: a comprehensive survey " IEEE Communications Surveys and Tutorials, Vol.**21**, Issue 2 pp.**1676-1717, 2019.**

[2] I.-C. Lin, T.-C. Liao "A survey of blockchain security issues and challenges" Int. J. Netw. Secur., Vol.19, Issue.5, pp**.653-659,2017.**

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang " Blockchain challenges and opportunities: a survey " Int. J. Web Grid Serv., Vol.14 Issue.4 , pp.**352-375, 2018.**

[4] de Villiers, C., Kuruppu, S., Dissanayake, D., 2020. "A (new) role for business—promoting the United Nations' Sustainable Development Goals through the internet-of-things and blockchain technology". J.Busres., Nov **2020.**

[5] Merugula, S., Dinesh, G., Kathiravan, M., Das, G., Nandankar, P., Karanam, S.R., 2021. "Study of Blockchain Technology in Empowering the SME. Proceedings - International Conference on Artificial Intelligence and Smart Systems" ICAIS 2021, pp.**758–765, 2021.**

[6] Paul, J."SCOPE framework for SMEs: a new theoretical lens for success and internationalization." Eur. Manag. J. Vol.38, Issue.2, pp.**219–230, 2020.**

[7] S. Yu, "Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data," in IEEE Access, Vol. 4, pp. **2751-2763, 2016.**

[8] Soria-Comas, J., Domingo-Ferrer, J. "Big Data Privacy: Challenges to Privacy Principles and Models. Data Sci" Eng. 1, pp.**21–28, 2016.**
[9] Zyskind, G., & Nathan, O. "Decentralizing privacy: Using blockchain to protect personal data." IEEE Security and Privacy Workshops. pp.**180-184, 2015.**
[10] Chabani, Z., Hamouche, S. and Said, R., "Is blockchain technology applicable in small and medium-sized enterprises?", in Motahhir, S. and Bossoufi, B. (Eds), Digital Technologies and Applications. ICDTA 2021. Lecture Notes in Networks and Systems, Springer, Cham, Vol.**211, 2021.**
[11] Nakamoto, S., "Bitcoin: a peer-to-peer electronic cash system", **2008**.
[12] Yang, J., Yu, H. and Pan, J. , "Research on the optimization of the financial system of SMEs based on blockchain technology", Proceedings- 2021 International Conference on Intelligent Blockchain based SME finance JTS Computing, Automation and Applications, ICAA 2021, pp.**623-627, 2021.**
[13] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., "An overview of blockchain technology: architecture, consensus, and future trends", 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, pp.**557-564, 2017.**
[14] Ante, L. , "Blockchain-based tokens as financing instruments: capital market access for SMEs?", Fostering Innovation and Competitiveness with FinTech, RegTech, and SupTech, pp. **129-141, 2020.**
[15] Swan, M." Blockchain: Blueprint for a New Economy". O'Reilly Media, **2015.**
[16] Tapscott, D., & Tapscott, A., "Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin", **2016.**
[17] Huang, D., O'Neill, J., & Parlikad, A. K. "Exploring the adoption of blockchain technology in the construction industry." In Proceedings of the Creative Construction Conference 2018 pp.**258-264, 2018.**
[18] Mougayar, W." The business blockchain: promise, practice, and application of the next internet technology". John Wiley & Sons,**2016**
[19] Ravi Prakash, V.S. Anoop, S. Asharaf. "Blockchain technology for cybersecurity: A text mining literature analysis" in International Journal of Information Management Data Insights, **2022.**
[20] Kshetri N " Blockchain's roles in meeting key supply chain management objectives " International Journal of Information Management Vol 39 pp.**80-89, 2018.**
[21] Maurer, Bill & Nelms, Taylor & Swartz, Lana. "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. Social Semiotics. 2013.
[22] Christidis, K. and Devetsikiotis, M.,"Blockchains and smart contracts for the internet of things." IEEE Access, Vol.4, pp.**2292-2303, 2016**
[23] Tapscott, D. and Tapscott, "A. Blockchain Revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World". Penguin, New York, **2016.**
[24] Pilkington, M. "Blockchain technology: principles and applications". Research Handbook on Digital Transformations, 2016.
[25] Primavera De Filippi, Morshed Mannan, Wessel Reijers. "Blockchain as a confidence machine: The problem of trust & challenges of governance, Technology in Society" Volume 62,101284, 2020.
[26] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis "A systematic literature review of blockchain-based applications: Current status, classification and open issues,Telematics and Informatics" Vol.36, pp.**55-81, 2019.**
[27] Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär, Ameen Soleimani "Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium" Blockchain: Research and Applications, 100176, **2023.**
[28] De Filippi, P., and Wright, A." Blockchain and the Law: The Rule of Code." Harvard University Press, **2018**.
[29] Wang, S., et al. . "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." Federal Reserve Bank of St. Louis Review, **2020**.
[30] Gordon, L. A., Loeb, M. P., & Sohail, T.." A framework for using insurance for cyber-risk management". Communications of the ACM, 53(3), pp.**81-85, 2010.**
[31] Anderson, R., & Stettler, "A.. SMEs and cybersecurity: risks and challenges". Information Security Journal: A Global Perspective, Vol 25 Issue 5-6, pp.**210-217, 2016.**
[32] Symantec.. Internet Security Threat Report, **2019**
[33] European Commission.. "GDPR and SMEs: Challenges and opportunities", **2018**.
[34] Foxman, E. R., & Kilcoyne, P.. Information technology, marketing practice, and consumer privacy: Ethical issues. Journal of Public Policy & Marketing, Vol 12 Issue 1, pp 106-119,**1993**.
[35] Martin, K. D., & Murphy, P. E.." The role of data privacy in marketing". Journal of the Academy of Marketing Science, Vol.45 Issue.2, pp.**135-155, 2017.**
[36] Barker, K., Askari, M., Banerjee, M., Ghazinour, K., Mackas, B., Majedi, M., ... & Williams, A. "A data privacy taxonomy". In British National Conference on Databases. Springer, Berlin, Heidelberg, pp.**42-54, 2009.**
[37] Conoscenti, Marco; Vetrò, Antonio; De Martin, Juan Carlos. "Blockchain for the Internet of Things: a Systematic Literature Review",IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir (MAR),. pp.1-6, **2016**.
[38] J. Warren, "Bitmessage "A peer-to-peer message authentication and delivery system," white paper, 27 November **2012.**
[39] Aitzhan, N. Z., & Svetinovic, D. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams". IEEE Transactions on Dependable and Secure Computing, **2016**.
[40] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H.. "An overview of blockchain technology: Architecture, consensus, and future trends." IEEE International Congress on Big Data (BigData Congress), pp.**557-564, 2017.**
[41] Bayer, D., Haber, S., & Stornetta, W. S.. "Improving the Efficiency and Reliability of Digital Time-Stamping. " Sequences II: Methods in Communication, Security, and Computer Science, pp.**329-334.1992.**
[42] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K." Where is current research on blockchain technology?—a systematic review". PloS one, Vol.**11**, Issue.**10, 2016.**

