Enhancing E-commerce Security: The Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions

Suresh Budha Dahal
School of Engineering, Kathmandu Tribhuvan University (TU)

Abstract

This study aims to investigate the effectiveness of blockchain technology in securing e-commerce transactions and protecting against fraud. The study examines the application of blockchain technology in various e-commerce platforms and identifies its potential to enhance transaction security and reduce the risk of fraud. The study found that blockchain technology offers several advantages in securing e-commerce transactions. One of the key findings is that the immutable nature of blockchain records ensures that transaction data cannot be tampered with once it has been recorded. This makes it almost impossible for fraudsters to manipulate e-commerce transactions, ensuring the authenticity and integrity of the data. The study also found that cryptographic security is a crucial aspect of blockchain technology that enhances e-commerce transaction security. The use of digital signatures, hash functions, and encryption algorithms ensure that transactions are secure and private, preventing unauthorized access to transaction data. Decentralized consensus is another key finding of this study. The study found that the validation and confirmation of transactions by a network of nodes rather than a central authority makes it difficult for fraudsters to manipulate or alter transactions since they would need to compromise a large number of nodes to do so. The study further discovered that the automation of e-commerce transactions using smart contracts enhances transaction security and reduces the risk of fraud. Smart contracts automate the execution of e-commerce transactions, ensuring that they are carried out according to pre-defined rules and conditions, eliminating the need for intermediaries and reducing the risk of fraud. The study identified that the traceability of transactions and their associated data using blockchain technology makes it easier to identify and investigate fraudulent activities. Blockchain technology allows for the tracking of transactions, providing a detailed record of all the associated data, which can be used to identify fraudulent activities and prevent them from happening in the future.

Keywords: Blockchain technology, E-commerce transactions, Fraud protection, Cryptographic security, Smart contracts

Introduction

In today's digital age, cybersecurity has become one of the most critical issues facing individuals, businesses, and governments. With the rise of the internet, the world has become more connected than ever before, and as a result, cyber threats have also increased in number and complexity. Cybersecurity is essential because it helps protect sensitive information, such as personal data, financial records, and intellectual

property, from falling into the wrong hands. It helps to prevent cybercrime, which can cause significant financial losses, reputational damage, and legal liability. Cybersecurity measures also play a crucial role in protecting national security, preventing espionage, and ensuring the safety of critical infrastructure. In short, cybersecurity is vital for safeguarding both personal and national interests in today's digital world.

One of the key reasons why cybersecurity is so important is the increasing reliance on technology in all aspects of our lives. From online banking and shopping to social media and healthcare, our personal data is constantly being shared and stored online. Cybersecurity measures are needed to protect this information from unauthorized access, theft, and misuse. Without adequate cybersecurity measures in place, our personal data is vulnerable to cybercriminals who can use it for identity theft, financial fraud, and other malicious purposes. Cybersecurity is also critical for businesses that collect and store customer data, as a data breach can result in severe reputational damage, financial losses, and legal liability. Therefore, businesses need to take cybersecurity seriously and implement robust cybersecurity measures to protect their data and their customers' data.

Moreover, cybersecurity is crucial for protecting national security and critical infrastructure. Governments around the world are increasingly relying on technology to deliver essential services, including healthcare, transportation, and utilities. A cyber attack on critical infrastructure, such as power grids or water systems, can have severe consequences, disrupting services and causing chaos. In addition, cyber espionage is a growing threat, with nation-states and other malicious actors seeking to steal sensitive information from other countries. Cybersecurity measures are critical for preventing these threats and protecting national security interests. As technology continues to advance, so do the threats and vulnerabilities associated with it. Therefore, it is essential to continue to develop and improve cybersecurity measures to protect against evolving threats and ensure that our personal data, businesses, and national security interests remain secure.

The emergence of ecommerce, or electronic commerce, can be traced back to the 1960s with the development of electronic data interchange (EDI), which allowed businesses to exchange documents and data electronically. However, it wasn't until the widespread adoption of the internet in the 1990s that ecommerce truly took off. Online retailers such as Amazon and eBay revolutionized the way people shopped, offering a convenient and efficient way to purchase goods without leaving their homes.

The growth of ecommerce was also facilitated by advances in technology such as secure payment systems, user-friendly website design, and reliable shipping and delivery options. These improvements made online shopping more accessible and appealing to a wider audience, and enabled ecommerce businesses to scale quickly and efficiently. Today, ecommerce has become an integral part of the global economy,

with sales reaching trillions of dollars annually and new technologies such as blockchain and AI paving the way for even more growth and innovation in the future.

However, the rise of ecommerce has also brought about significant changes in the way we shop and do business. Traditional brick-and-mortar retailers have had to adapt to the changing landscape or risk being left behind, while ecommerce businesses must constantly innovate and improve in order to stay competitive. Ecommerce has also raised concerns about privacy and security, as well as the impact on local communities and small businesses. Despite these challenges, the emergence of ecommerce has transformed the way we live, work, and shop, and will continue to shape the future of commerce and society as a whole. The emergence of ecommerce has been a remarkable and transformative phenomenon that has reshaped the way we buy and sell goods and services. From its early roots in electronic data interchange to the massive global industry it is today, ecommerce has revolutionized the way we do business, connect with one another, and interact with the world around us. As technology continues to evolve and new innovations emerge, the future of ecommerce looks bright, with endless opportunities for growth and development.

Effectiveness of Blockchain Technology in Protecting Against Fraudulent Transactions

Immutable records are a fundamental characteristic of blockchain technology. It is one of the defining features that make blockchain so appealing for businesses and individuals alike. The immutability of blockchain records means that once a transaction is recorded on the blockchain, it cannot be altered, deleted or tampered with. This level of security provides trust and transparency in transactions, making it ideal for industries that require high levels of security, such as finance, healthcare, and government.

One of the key benefits of immutable records is that it eliminates the need for intermediaries. Traditional financial transactions often require intermediaries, such as banks, to ensure that transactions are secure and that all parties involved are protected. With blockchain technology, the need for intermediaries is reduced or eliminated entirely, reducing the cost and complexity of transactions. This allows for faster and more efficient transactions, which can benefit both businesses and consumers.

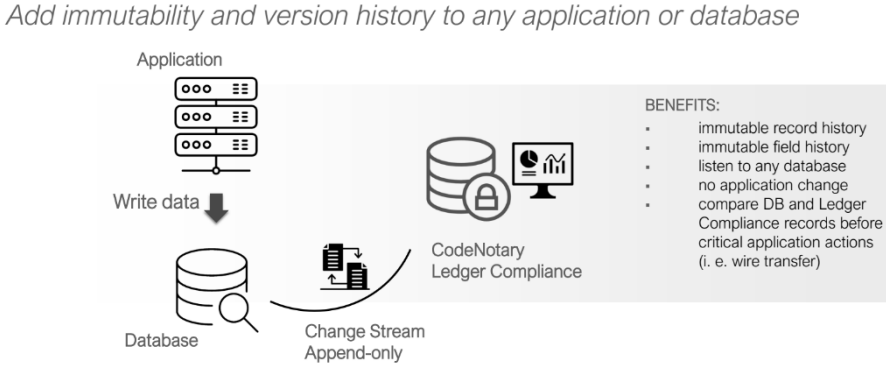
Another benefit of immutable records is that it helps to prevent fraud. Fraudulent activities, such as double-spending, are common in traditional financial transactions. Blockchain technology eliminates these fraudulent activities by ensuring that once a transaction is recorded on the blockchain, it cannot be altered or deleted. This makes blockchain an ideal solution for industries that are susceptible to fraud, such as insurance and real estate.

The immutability of blockchain records also provides a high level of transparency. This transparency allows individuals and businesses to track transactions and ensure that they are conducted fairly and transparently. This level of transparency can be particularly important in industries where trust and transparency are critical, such as

government, healthcare, and supply chain management. Finally, immutable records are critical for ensuring the security of e-commerce transactions. With the rise of e-commerce, security has become a primary concern for businesses and consumers. Immutable records provide a high level of security, making it impossible for anyone to tamper with transaction data once it has been recorded. This means that e-commerce transactions are secure and cannot be changed by anyone, providing businesses and consumers with peace of mind.

Immutable records are a fundamental characteristic of blockchain technology. The immutability of blockchain records provides numerous benefits, including eliminating the need for intermediaries, preventing fraud, providing transparency, and ensuring the security of e-commerce transactions. As blockchain technology continues to evolve and gain acceptance, it is likely that immutable records will become even more critical for ensuring the security and transparency of transactions across a wide range of industries.

Figure 1. Immutability



One of the primary strengths of blockchain technology is its robust cryptographic security. Blockchain uses advanced cryptographic techniques to ensure that transactions are secure and private. This security is achieved through a combination of digital signatures, hash functions, and encryption algorithms that ensure the authenticity and integrity of data.

Digital signatures are one of the core components of cryptographic security on the blockchain. Digital signatures are a way of verifying that a transaction has been

created by a specific individual and has not been tampered with during transmission. Digital signatures use a public and private key system, where the private key is used to sign the transaction and the public key is used to verify the signature.

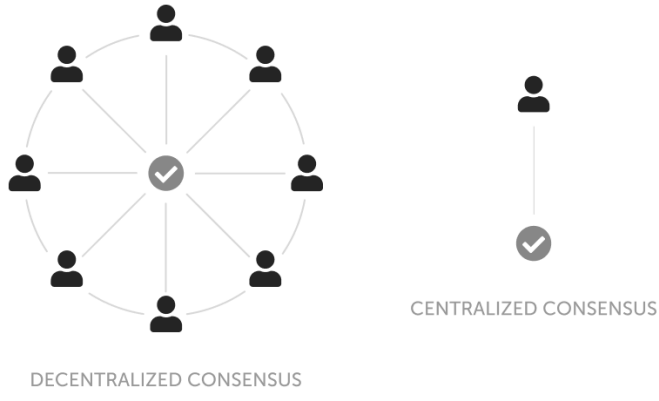
Hash functions are another critical component of cryptographic security on the blockchain. A hash function is a mathematical algorithm that takes an input and produces a fixed-length output. The output, known as a hash, is unique to the input and cannot be reversed. In the context of blockchain, hash functions are used to create a unique identifier for each transaction. This identifier is then used to verify the integrity of the transaction.

Encryption algorithms are also used to ensure the privacy and security of transactions on the blockchain. Encryption algorithms use complex mathematical algorithms to scramble data so that it is unreadable without a decryption key. Encryption is used to protect sensitive data, such as financial transactions or personal information, from unauthorized access or tampering.

Together, these cryptographic techniques provide a high level of security and privacy for transactions on the blockchain. By using digital signatures, hash functions, and encryption algorithms, blockchain technology ensures that transactions are secure and private. This security is particularly important for industries that require high levels of security, such as finance, healthcare, and government.

In addition to providing security and privacy, cryptographic security on the blockchain also provides transparency. Because transactions on the blockchain are publicly visible, anyone can verify the authenticity and integrity of the data. This transparency helps to build trust between parties and ensures that transactions are conducted fairly and transparently. Cryptographic security is a critical component of blockchain technology. Through the use of digital signatures, hash functions, and encryption algorithms, blockchain technology ensures the authenticity, integrity, privacy, and security of transactions. As blockchain technology continues to evolve, it is likely that cryptographic security will become even more critical for ensuring the security and privacy of transactions across a wide range of industries.

Figure 2. Decentralized consensus



Another key feature of blockchain technology is its decentralized consensus mechanism. Unlike traditional financial systems, where transactions are validated and confirmed by a central authority, transactions on the blockchain are validated and confirmed by a network of nodes. This decentralized consensus mechanism ensures that the blockchain remains secure and transparent.

Decentralized consensus on the blockchain is achieved through a process known as mining. Mining involves solving complex mathematical equations to validate transactions and create new blocks on the blockchain. The nodes that participate in mining are known as miners, and they are incentivized to participate through the reward of newly created cryptocurrency.

The decentralized nature of blockchain consensus makes it difficult for fraudsters to manipulate or alter transactions. In order to successfully alter a transaction, an attacker would need to compromise a large number of nodes, which is virtually impossible. This makes the blockchain a highly secure and tamper-proof system.

The decentralized consensus mechanism also provides transparency and trust in transactions. Since all nodes in the network participate in the validation and confirmation of transactions, there is no need for a central authority. This ensures that transactions are conducted in a fair and transparent manner, and that all parties have equal access to the network.

Another benefit of decentralized consensus is that it provides a high level of scalability. Unlike traditional financial systems that are limited by the capacity of their centralized infrastructure, the decentralized nature of blockchain technology allows for an unlimited number of nodes to participate in the network. This means that blockchain technology can support a vast number of transactions without sacrificing security or performance. The decentralized consensus mechanism is a critical feature of blockchain technology. By allowing transactions to be validated and confirmed by a network of nodes, rather than a central authority, blockchain technology provides a high level of security, transparency, and scalability. As blockchain technology continues to evolve, it is likely that decentralized consensus will become even more critical for ensuring the security and transparency of transactions across a wide range of industries.

Smart contracts are a powerful tool enabled by blockchain technology that allows for the automation of e-commerce transactions. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist on a decentralized blockchain network, making them transparent and tamper-proof.

Smart contracts can automate the execution of e-commerce transactions, ensuring that they are carried out according to pre-defined rules and conditions. This means that once the conditions of a smart contract are met, the transaction is automatically executed. This eliminates the need for intermediaries such as lawyers, brokers, or escrow agents and reduces the risk of fraud.

The use of smart contracts can also speed up the execution of transactions. Since the terms of the contract are pre-defined and the execution is automated, the transaction can be completed much faster than traditional contracts. This makes the use of smart contracts particularly attractive for industries that require fast and secure transactions, such as finance and supply chain management.

Another benefit of smart contracts is that they can reduce costs. Since smart contracts eliminate the need for intermediaries, the costs associated with these intermediaries are also eliminated. This can lead to significant cost savings for businesses that use smart contracts.

Smart contracts also provide a high level of transparency and trust in transactions. Since the terms of the contract are directly written into lines of code, the contract is transparent and tamper-proof. All parties can see the terms of the contract and can trust that the contract will be executed as intended. Smart contracts are a powerful feature of blockchain technology that can automate e-commerce transactions, reduce the need for intermediaries, speed up transaction times, reduce costs, and provide a high level of transparency and trust. As blockchain technology continues to evolve, the use of smart contracts is likely to become even more widespread, particularly in industries that require fast and secure transactions.

Traceability is a critical feature of blockchain technology that allows for the tracking of transactions and their associated data. This makes it easier to identify and investigate fraudulent activities, making blockchain technology a powerful tool for fighting fraud.

With blockchain technology, each transaction is recorded on a public ledger, which can be viewed by anyone on the network. This creates a transparent and tamper-proof record of all transactions, providing a high level of traceability. Since each block on the blockchain is linked to the previous block, it is virtually impossible to alter or delete a transaction once it has been recorded.

Traceability on the blockchain can be particularly useful for industries that require the tracking of goods or products, such as the food industry or supply chain management. With blockchain technology, each product can be assigned a unique identifier that is recorded on the blockchain. This allows for the tracking of the product from its origin to its final destination, making it easier to identify and investigate any issues that may arise.

Blockchain technology can also be used to combat fraud in the financial industry. By providing a transparent and tamper-proof record of all transactions, blockchain technology makes it more difficult for fraudsters to engage in activities such as money laundering or embezzlement. The use of blockchain technology can help to reduce the risk of fraud and increase transparency in financial transactions.

Another benefit of traceability on the blockchain is that it can help to increase consumer trust. With blockchain technology, consumers can be confident that the products they are purchasing are genuine and have not been tampered with. This can be particularly important in industries such as pharmaceuticals, where counterfeit products can pose a serious risk to public health. Traceability is a critical feature of blockchain technology that allows for the tracking of transactions and their associated data. By providing a transparent and tamper-proof record of all transactions, blockchain technology can help to combat fraud, increase transparency, and build consumer trust. As blockchain technology continues to evolve, it is likely that traceability will become even more important for ensuring the security and transparency of transactions across a wide range of industries.

Conclusion

The future of cybersecurity is likely to be shaped by emerging technologies and the increasing prevalence of cyber threats. One of the biggest trends in cybersecurity is the growing use of artificial intelligence (AI) and machine learning (ML) to detect and respond to cyber attacks. With the growing complexity of cyber threats, AI and ML can help to identify and mitigate these threats more quickly and accurately than human analysts. AI and ML can analyze vast amounts of data to detect patterns and anomalies, helping to identify potential threats before they can cause significant damage. Moreover, AI and ML can help to automate routine cybersecurity tasks, freeing up human analysts to focus on more complex and strategic issues.

Another significant trend in the future of cybersecurity is the growing importance of cloud security. With the increasing adoption of cloud computing, organizations are storing more and more sensitive data in the cloud, making cloud security a critical issue. As a result, cloud service providers are investing heavily in developing robust security measures to protect their customers' data. Additionally, organizations are looking to implement cloud security measures such as data encryption, multi-factor authentication, and identity and access management to protect their cloud-based data. Cloud security will continue to evolve as more organizations move their data and applications to the cloud, making it a crucial area of focus for the future of cybersecurity.

The future of cybersecurity will also be shaped by the increasing prevalence of the Internet of Things (IoT) devices. IoT devices, such as smart home devices and wearable technology, are becoming more common and are expected to increase in number in the coming years. However, IoT devices are often poorly secured, making them vulnerable to cyber attacks. As a result, there will be a growing need for robust security measures to protect IoT devices from cyber threats. This will require the development of new technologies and standards for securing IoT devices, as well as increased awareness and education for consumers to help them protect their IoT devices from cyber threats. The future of cybersecurity will be shaped by emerging technologies, the increasing importance of cloud security, and the growing prevalence of IoT devices. Organizations will need to continue to invest in cybersecurity measures to protect their data and their customers' data from cyber threats. Additionally, there will be a growing need for cybersecurity professionals with the skills and knowledge to develop and implement effective cybersecurity measures in this ever-evolving digital landscape. As technology continues to advance, the future of cybersecurity will be critical for protecting our personal data, businesses, and national security interests.

References

[1] B. V. Prasanthi and P. Kanakam, "Cyber forensic science to diagnose digital crimes-a study," *International Journal of*, 2017.

[2] K. Jaishankar, "Cyber criminology: Evolving a novel discipline with a new journal," *International Journal of Cyber Criminology*, 2007.

[3] T. F. Gayed, H. Lounis, and M. Bari, "Cyber forensics: Representing and (im) proving the chain of custody using the semantic web," in *COGNITIVE 2012: The Fourth International Conference on Advanced Cognitive Technologies and Applications*, 2012, pp. 19–23.

[4] M. Mnyakin, "Investigating the Impacts of AR, AI, and Website Optimization on Ecommerce Sales Growth," *RRST*, vol. 3, no. 1, pp. 116–130, Dec. 2020.

[5] C. M. Karat, J. O. Blom, and J. Karat, *Designing personalized user experiences in eCommerce*, 2004th ed. New York, NY: Springer, 2004.

[6] J. Telo, "ANALYZING THE EFFECTIVENESS OF BEHAVIORAL BIOMETRICS IN AUTHENTICATION: A COMPREHENSIVE REVIEW," *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, vol. 2, no. 1, pp. 19–36, 2019.

[7] J. Telo, "Web Traffic Prediction Using Autoregressive, LSTM, and XGBoost Time Series Models," *Web Traffic Prediction Using Autoregressive, LSTM, and XGBoost Time Series Models*, vol. 3, no. 1, pp. 1–15, 2020.

[8] C. Cho, S. Chin, and K. S. Chung, "Cyber forensic for hadoop based cloud system," *International Journal of Security and its Applications*, vol. 6, no. 3, pp. 83–90, 2012.

[9] L. Luciano, I. Baggili, M. Topor, P. Casey, and F. Breitinger, "Digital Forensics in the Next Five Years," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, Hamburg, Germany, 2018, pp. 1–14.

[10] A. J. Marcella and F. Guillossou, *Cyber forensics: From data to digital evidence*. Nashville, TN: John Wiley & Sons, 2012.

[11] J. Telo, "Intrusion Detection with Supervised Machine Learning using SMOTE for Imbalanced Datasets," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 5, no. 1, pp. 12–24, 2021.

[12] R. Santanam, M. Sethumadhavan, and M. Virendra, *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*. Hershey, PA: Information Science Reference, 2010.

[13] I. V. Kotenko, M. Kolomeets, A. Chechulin, and Y. Chevalier, "A visual analytics approach for the cyber forensics based on different views of the network traffic," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 9, no. 2, pp. 57–73, 2018.

[14] R. Y. Patil and S. R. Devane, "Unmasking of source identity, a step beyond in cyber forensic," in *Proceedings of the 10th International Conference on Security of Information and Networks*, Jaipur, India, 2017, pp. 157–164.

[15] G. S. Dardick, "Cyber Forensics Assurance," 2010.

[16] J. Telo, "Supervised Machine Learning for Detecting Malicious URLs: An Evaluation of Different Models," *Sage Science Review of Applied Machine Learning*, vol. 5, no. 2, pp. 30–46, 2022.
[17] J. Stirland, K. Jones, H. Janicke, T. Wu, and Others, "Developing cyber forensics for SCADA industrial control systems," in *Proceedings of the International Conference on Information Security and Cyber Forensics*, 2014.
[18] S. Nirkhi and R. V. Dharaskar, "Comparative study of Authorship Identification Techniques for Cyber Forensics Analysis," *arXiv [cs.CY]*, 24-Dec-2013.
[19] E. Cornelius and M. Fabro, "Recommended practice: Creating cyber forensics plans for control systems," Idaho National Lab. (INL), Idaho Falls, ID (United States), INL/EXT-08-14231, Aug. 2008.
[20] J. Telo, "Understanding Security Awareness Among Bank Customers: A Study Using Multiple Regression Analysis," *Sage Science Review of Educational Technology*, vol. 6, no. 1, pp. 26–38, 2023.
[21] A. Marcella Jr and D. Menendez, "Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes," 2010.
[22] I. Baggili and F. Breitinger, "Data sources for advancing cyber forensics: What the social world has to offer," 2015. [Online]. Available: https://cdn.aaai.org/ocs/10227/10227-45279-1-PB.pdf.
[23] G. Shrivastava, K. Sharma, M. Khari, and S. E. Zohora, "Role of Cyber Security and Cyber Forensics in India," in *Handbook of Research on Network Forensics and Analysis Techniques*, IGI Global, 2018, pp. 143–161.
[24] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington, "A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later," *Comput. Secur.*, vol. 57, pp. 1–13, Mar. 2016.
[25] J. Telo, "A Comparative Analysis of Network Security Technologies for Small and Large Enterprises," *International Journal of Business Intelligence and Big Data Analytics*, vol. 2, no. 1, pp. 1–10, 2019.
[26] B. V. Prasanthi and Vishnu Institute of Technology, "Cyber Forensic Tools: A Review," *Int. J. Eng. Trends Technol.*, vol. 41, no. 5, pp. 266–271, Nov. 2016.
[27] H. Park, S. Cho, and H.-C. Kwon, "Cyber Forensics Ontology for Cyber Criminal Investigation," in *Forensics in Telecommunications, Information and Multimedia*, 2009, pp. 160–165.
[28] A. Brinson, A. Robinson, and M. Rogers, "A cyber forensics ontology: Creating a new approach to studying cyber forensics," *Digital Investigation*, vol. 3, pp. 37–43, Sep. 2006.
[29] J. Telo, "PRIVACY AND CYBERSECURITY CONCERNS IN SMART GOVERNANCE SYSTEMS IN DEVELOPING COUNTRIES," *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, vol. 4, no. 1, pp. 1–13, 2021.
[30] N. Shetty, G. Schwartz, and M. Felegyhazi, "Competitive cyber-insurance and internet security," *of information security and …*, 2010.
[31] K. Kioskli, T. Fotis, and H. Mouratidis, "The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, Vienna, Austria, 2021, pp. 1–9.

[32] J. Telo, "Blockchain Technology in Healthcare: A Review of Applications and Implications," *Journal of Advanced Analytics in Healthcare Management*, vol. 1, no. 1, pp. 1–20, 2017.
[33] M. Mainelli and M. Smith, "Sharing Ledgers For Sharing Economies: An Exploration Of Mutual Distributed Ledgers (aka Blockchain Technology)," *Journal of financial perspectives*, 01-Dec-2015.
[34] M. Avital, R. Beck, J. L. King, M. Rossi, and R. Teigland, "Jumping on the blockchain bandwagon: Lessons of the past and outlook to the future," *ICIS Chem. Bus.*, 2016.
[35] D. Shrier, W. Wu, and A. Pentland, "Blockchain & Infrastructure (Identity, Data Security)," 2016. [Online]. Available: https://www.getsmarter.com/blog/wp-content/uploads/2017/07/mit_blockchain_and_infrastructure_report.pdf.
[36] F. Milani, L. García-Bañuelos, and M. Dumas, "Blockchain and business process improvement," *BPTrends newsletter (October 2016)*, 2016.
[37] J. Telo, "AI for Enhanced Healthcare Security: An Investigation of Anomaly Detection, Predictive Analytics, Access Control, Threat Intelligence, and Incident Response," *Journal of Advanced Analytics in Healthcare Management*, vol. 1, no. 1, pp. 21–37, 2017.
[38] M. Swan, "Blockchain Thinking : The Brain as a Decentralized Autonomous Corporation [Commentary]," *IEEE Technol. Soc. Mag.*, vol. 34, no. 4, pp. 41–52, Dec. 2015.
[39] J. Zhang, N. Xue, and X. Huang, "A Secure System For Pervasive Social Network-Based Healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016.
[40] A. Ekblaw and A. Azaria, "MedRec: Medical Data Management on the Blockchain," 2016.
[41] M. Swan, *Blockchain: Blueprint for a new economy*. O'Reilly Media, 2015.
[42] J. Telo, "Smart City Security Threats and Countermeasures in the Context of Emerging Technologies," *International Journal of Intelligent Automation and Computing*, vol. 6, no. 1, pp. 31–45, 2023.
[43] H. Kayhan, "Ensuring trust in pharmaceutical supply chains by data protection by design approach to blockchains," *Blockchain Healthc. Today*, vol. 5, Sep. 2022.
[44] D. Immaniar, A. A. Aryani, and S. Z. Ula, "Challenges Smart Grid in Blockchain Applications," *B-FronT*, vol. 2, no. 2, pp. 1–9, Sep. 2022.