Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

The Intersection of Blockchain Technology and Data Security in e-Business

Nikos Kostopoulos

Department of Management Science and Technology

University of Patras, Greece

nikolaoskostop@gmail.com

Hera Antonopoulou*

Department of Management Science and Technology

University of Patras, Greece

hera@upatras.gr

*Corresponding Author: E-mail: hera@upatras.gr

Abstract

This paper investigates the integration of blockchain technology and data security within an e-business context, articulating the transformative potential of this integration across various key sectors: financial transactions, supply chain operations, digital healthcare, and product authenticity verification. Other important attributes of blockchain, such as decentralization, immutability, and transparency, coupled with powerful security measures, are explored. This indicates the importance of ensuring data security in e-business, especially against cyber threats and insider threats. This paper therefore will explore specific blockchain applications in e-business, focusing especially on smart contracts, supply chain management, and data security. It also accepts challenges, including high development costs and integration problems, but it highlights opportunities according to potential operational efficiencies and overall improvement in transparency. Convergence of blockchain with AI and machine learning is discussed as part of future trends, which sets higher demand for continued research and development to maximize the benefits while at the same time mitigating the risks linked to blockchain technology in e-business. The references cited provide an essential overview of the current research landscape, which spans various digital technologies and their implications in multiple domains.

Keywords: *Blockchain Technology, Data Security, E-business, Decentralization, Immutability, Transparency, Cyber Threats, Smart Contracts, Supply Chain Management, Operational Efficiency, Financial Transactions*

1. Introduction

Background Blockchain technology has not only reshaped the global IT landscape but also changed the operational methods of economies, social systems, and civilizations worldwide. The Internet began to develop rapidly in the 1990s and gradually integrated with various areas of society, and a great deal of data began to accumulate as well. It was soon discovered, however, that although the Internet could circulate and issue a great variety of resources, it could not solve the transaction problem caused by different types of irreparable property. Hence, double spending threats derived from currency transactions emerged. Blockchain technology originated to solve these problems. A blockchain is a continuously growing list of records (called blocks),

which are linked and secured using cryptography. It is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way [1-6]. Economically speaking, the function of blockchain technology is to use a new conception created by the Internet to design an online currency system. Bitcoin was the first decentralized digital currency system founded based on blockchain technology, which was officially launched in January 2009. Blockchain technology is very important in the transaction process. Its basic operation consists of four processes—issuing, transmitting, handling, and trading. This technology benefits many parties since everyone has a ledger to check [7-10].

Definition and Basic Concepts

A blockchain is a data structure that allows the creation of a "digital ledger" to encode financial and non-financial transactions, mainly web based. The blockchain is a distributed ledger consisting of a chain of blocks. As in any ledger, a block contains a list of transactions, each signed by the party that wants to execute it. The structure of the block also allows the computerized nodes on the network to agree on the order of the transactions, collecting them in groups that are unchangeable. A hash function, which is extremely fast to compute, is a mathematical function that receives as input a set of data of any size and produces its "hash" - typically a string of characters that represents the cryptographic footprint of the original data. Any change in the data (even minimal) will cause a significant change in the output hash. This idea can be applied recursively on the blocks themselves to create a secure block sequence [11-14]. A node is network-aware and can be an individual computer, device, or cloud-based system that participates in the blockchain process. A block is a data structure that houses the data about transactions. The term "hash" comes from the physical action of chopping up a bunch of data, turning everything into a few points of data, but it's more about the function of simplification. One main activity within blockchains is the maintenance of the integrity between computers present in the network through the consensus mechanism. There are many consensus methods, such as proof of work, proof of stake, Byzantine fault tolerance, and delegated proof of stake, among others. The type and method of implementing the consensus mechanism can generate very different results and can reveal a blockchain that is maintained through a public management of its details. In this case, the term public blockchain is used. Instead, in a private blockchain, every node can be managed and controlled by the owner of it [15-19].

Key Features and Components

Blockchain's architecture design and important application of decentralized features are described in the key features of blockchain. Decentralization not only makes electronic transactions in financial information processes realize peer-to-peer without intermediate links, but also can effectively decentralize management and reduce the space of a central platform as a single point of failure, to support the sustainable development of the relevant ecosystem. Immutability, which discovers the value of historical data, does not rely on any special means of trust or a single center to ensure the authenticity of electronic transaction behavior data. Once written, a kind of electronic transaction behavior record is unable to be modified or reversed. After the transaction data is affirmed, the two entities involved in the transaction must reach a consensus through a special mechanism of verification and ensure that the data cannot be tampered with. It has strong traceability and can lay the foundation for the identification and always tracking of the source of the goods. Transparency refers to the openness of electronic transaction behavior data, which can be checked and traced by any online nodes through the network. Each node holds a full copy of the transaction behavior data and concurrently updates it in real time, ensuring the consistency and transparency of the data. In addition, the system must implement better security and protection, certificate and key technology, to effectively support the trusted identification and confirmation of the information and transaction characteristics of the relevant personnel in the electronic transaction process. It effectively prevents denial of service attacks and protects electronic transaction information systems. The components of a blockchain include block, chain, and node. Cryptographic techniques are essential in the field of blockchain. The digital signature algorithm allows users in the blockchain to verify the transaction characteristics and safety, effectively supporting asymmetric encryption, hash algorithms, certificate technology, and digital signatures to further enhance the protection of transaction characteristics and promote information security. Public Key Infrastructure allows users participating in electronic transactions to more effectively promote the secure identification and legal value of

Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

transaction data. This trust model based on cryptographic techniques helps nodes of the entire transaction network verify that they are indeed interacting with the correct party to prevent the occurrence of counterfeiting. Thus, the implementation of these features ensures the trustworthiness of the business to a very large extent [20-27].

2. Data Security in e-Business

Data security is of paramount importance in e-business. As businesses are increasingly becoming digitized, data will be touched almost every time a customer or a client buys, or end-users engage with businesses. In view of this, the protection of sensitive data is important and essential. However, data security for e-business should make use of the data security controls that can protect the data from unauthorized access and loss. This also means that a framework is required to be in place to ensure that the rules and regulations related to data protection and organization, which includes data handling and its governance, are respected and maintained. Data security should focus on the strength of the security culture, which can be a deciding factor for business success. The measures that the organization takes to protect sensitive data are also a suitable test for their efficient system administration. In the case of any kind of data breach or loss, the decline of this company's credibility is faster, which depends on the interval and the severity of the loss. The various declared data security breaches due to threats like application intrusion, configuration errors, and authentication breaches show that large enterprises consist of several threads tied together by backend data. Companies these days not only want to conduct digital transactions over the Internet, but they also want to secure them from threats. This could be possible only by integrating security capabilities into the transactions. There are certain inherent vulnerabilities present in various digital transactions, and it becomes hard to trace the threats present in every digital transaction and to counteract them. So, it should lie in the best interest of customers or clients to tailor the security risk according to the needs of the business. This can be achieved by proactively securing the networks and systems to counter the attacks and threats before they pose their danger [28-36].

Importance of Data Security in e-Business

e-Business is the pivot of commercial activities wherein the data of users or customers is a core asset. It is therefore necessary to ensure that the data assets are well secured to gain confidence and encourage transactions between the concerned parties. There are various types of commercially sensitive information that e-Businesses often deal with, such as personal user data, business strategy data, customer databases, payment details, etc. Sharing any sensitive data with anyone who does not need it can possibly cause severe damage to the e-Business. A loss of credit card details would cause a considerable reputational loss and probably a financial loss to the company responsible for the data. With the increasing complexities of systems and data, it becomes more important not just to find out who accessed the data, but what the intended use was [37-44]. The risk of a data breach entails several serious consequences for any business, not just from a financial viewpoint. There is a huge reputational impact when personal or financial information is disclosed, which can discourage users from engaging with the e-Business. The public loss of confidence in fully digital systems can have cascading effects that can trigger regulation, which comes with considerable cost and inconvenience. Costs could range from system upgrades due to changes in legislation to compensation for individuals related to data protection operations. This is a risk even if the business is not in violation of any laws but was itself the victim of a compromise. Many market sectors that handle data are now under regulatory pressure due to personal data scandals, leading to new statutory instruments. These regulatory approaches forensically investigate what data was exposed or compromised, and it is increasingly likely that confidential data will be the target of future regulatory checks. Reputational and financial loss in e-Business provides a strong need to not take the chance with untrustworthy data. Non-reputable data, such as customer review systems that allow for fraud, may in themselves create additional harm to public trust, with wider effects [45-52].

Common Threats and Vulnerabilities

The advancement of technology certainly has facilitated the occurrence of certain risks. There are several primary threats that occur in businesses today, and these threats are becoming more complex and widely distributed. Cyber threats are now some of the biggest issues in businesses, with more than a quarter of

Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

businesses reporting that it was their biggest risk. Some common cyber threats include: • Phishing. • Malware such as viruses, Trojans, and worms. • Denial-of-service. • Advanced persistent threats. • Insider threats [53-58]. The unreliability of e-business is due primarily to vulnerabilities in three key areas, including technology, employee weaknesses, and the business supply chain. The growing reliance on e-business has attracted more outsiders with malevolent intent. The conflicts between profitability and security have led managers to implement constantly changing technological components in the internal network of many businesses. Many businesses are not aware of the technologies running in their internal network infrastructure, nor are they aware of the current software patch application in their organization. Therefore, businesses today are subject to known, unknown, and potential risk vulnerabilities that have not been detected. The most dangerous risk vulnerability is the one that has not been detected, as it poses an inherent danger to the data, information, and/or intellectual property that flows through the network infrastructure. Moreover, as new vulnerabilities arise, so do new threats. Consequently, businesses are constantly upgrading their boundaries and internal network security protocols [59-64]. Thus, the common threats and vulnerabilities that affect e-businesses undermine their integrity and can therefore crush the confidence of potential customers. Business managers are not only expected to identify the potential threats and vulnerabilities that surface due to technological advancement, but they are also expected to find an effective method of dismantling these risks [65-66].

3. Blockchain Applications in e-Business

Blockchain, as an underlying technology of cryptocurrencies, has recently drawn much attention from academia and industry. Thanks to its standout features, blockchain can innovate and transform e-business. Several leading companies have built their business ecosystems based on blockchain from scratch, while some other companies are currently proactively pursuing blockchain-driven transformation. So far, there are a variety of ways and contexts where blockchain technology is applied in business. For instance, it can be engaged in processing financial transactions, managing supply chain operations, authenticating digital assets, and much more [67-71]. To date, blockchain technology has shown its strong potential in numerous e-business usage scenarios, and we introduce some of them with related use cases as follows. These examples of the latest uses of blockchain technology cover different usages such as payment processing, digital identity, product authenticity, digital healthcare, and supply chain management. These uses provide considerable scale, among several benefits. One use case showed an example of 1.6 billion transactions in 2021. One further use case, and future research, is to investigate the role of blockchain in enabling new models of supply chain financing. Blockchain is significantly transformative, helping to enhance effectiveness and efficiencies in operations. The role of this technology is explored in many ventures, emphasizing impact and future economies in business. The technological underpinning, in this context, as a permissioned distributed ledger, has commoditized computing and transactional capabilities. All the use cases mentioned above illustrate that blockchain can potentially be used to improve transparency, security assurance, and operational efficiency in a variety of e-business areas. These blockchain use cases in e-business are introduced and discussed with relevant blockchain technology features, as a foundation to understand how blockchain can be adopted to secure e-business data. Blockchain in supply chain management is currently experiencing a significant uptick; for example, some companies are piloting blockchain in the apparel supply chain, while others have built a blockchain-based product provenance and recall solution and have a B2B solution for product authenticity in the pharmaceutical industry, providing sensor-equipped blockchain-to-IoT communication devices. These platforms manage tracking and tracing along the chain and in some cases use the blockchain-based product passport [72-78]. Smart contracts are computer protocols that can automatically validate contractual clauses and execute obligations. Since smart contracts can operate with no intermediation and enable safe fair trading between unacquainted e-business organizations, they can be effectively applied to automatic contractual processes in various scenarios. At present, there are already existing smart contract platforms. Each smart contract is hosted by a modified node in a mainstream decentralized distributed ledger system. Supply chain management approaches based on the permissioned blockchain variant can assure the supply chain data and information transparency and security, thereby motivating inter-enterprise cooperation. In other words, blockchain technology can assign each participant in a supply chain, such as suppliers, manufacturers, logistics, retailers, and consumers, their own private and public key pair. Only if it is coordinated and accepted by all the other participants can one participant join the block. In that way, blockchain technology makes it feasible to keep

Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

unfalsified supply chain data records. Besides, blockchain technology also makes it infeasible for any other participant to deny transactions or disagree on the state of the transaction [79-84].

Smart Contracts

The most prominent application of blockchain in the e-business field is smart contracts. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller directly written into lines of code. The best way to describe them is to compare them to a vending machine. Normally, a buyer would buy items directly from a seller, especially paper assets. Smart contracts protect investors, enhance security, and reduce reliance on intermediaries. Smart contracts enable contracts and transactions to be enforced even when the parties are strangers or in free domains [85-89]. The maturation of several technologies has enabled smart contracts to flourish. First, the fixed rules prevent disputes, so smart contracts in nature have less litigation value. Second, innovation in blockchain facilitates companies to be run digitally and securely without auditors. Therefore, smart contracts have been widely adopted in the settlement of various financial contracts. Finally, certain real estate transactions have evolved to a point where they do not value the possible conflicts between landlords and sub-secure tenants. Smart contracts play a role in facilitating this group of transactions. However, smart contracts are never a remedy for all economic and request requirements. In the absence of an experienced expert in the original topic and in the information of a reputable losing company in terms of law, there may not be the same confidence [90-94]. When you write a piece of computer code, you are easily skeptical of unexpected errors. This is a problem because smart contracts are for the code. They control high stakes and technically cost the owner nothing for non-compliance, with digitally encoded penalties in such cases. Obligations to implement a study are minimal. Finally, the performance of smart contracts is uncertain. There are few texts that only talk about a smart contract. The work mainly examines the legal implications of blockchain. So far, blockchain-supported smart contracts have not been well researched. There is a lack of information about the essential legal implications of blockchain technology. There are two groups present—firstly, early blockchain and conceptual articles, and second, professional writings [95-100].

Supply Chain Management

The biggest impact and value creation through blockchain will be seen in the supply chain and logistics industries. One of the most impactful applications of blockchain is the ability to enhance data transparency and traceability, enabling real-time tracking of food products from farm to plate and from origin to destination for other sorts of physical products. Such a real-time tracking system can effectively reduce fraudulent activities in the supply chain process and improve inventory control, as well as the management of logistics and transportation. Beyond the food sector, blockchain implementation can also be credited to retail and luxury goods. Blockchain can also lower costs due to operational efficiencies that come from it. Specifically for the supply chain, by using blockchain's smart contracts, one possible application could be the automation of supply chain transactions, including processing orders and shipments [101-106]. Challenges of blockchain technology consist of a protracted implementation process, high entry development costs, difficulties in system integration, and inherent security weaknesses. However, several companies have implemented blockchain technology to enhance the transparency, traceability, and resiliency of their supply chain logistics operations. Already, a leading company in blockchain technology has launched its blockchain network for testing the global food supply chain traceability. The main function of blockchain is to track the movement of food from farm to plate. The aim of the case companies involved in the project is to ensure that a quality control system is being adopted, validate the authenticity of the food that flows across the border, and provide consumers with assurance of food safety [107-112].

4. Integration of Blockchain and Data Security in e-Business

The synergy of the features inherently present in blockchain technology with the needs of data security defines its potential to integrate data security in existing e-business frameworks. The decentralization of the computing model advocates for data security systems to provide a multi-layered protective barrier against both outsider and insider threats. Verifiability, transparency, and immutability of the signed records embed great potential for ensuring the provenance of the authentic data owner. The blockchain's capability to deliver

Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

tamper-resistant affiliate or registration services will always provide authentic and secure data interaction infrastructure. One of the most striking advantages of introducing blockchain technology in the sphere of data interchange systems is its ability to effectively challenge cyberattacks aiming to hijack the authorization and authentication processes in business operations. The innovative algorithms are expected to foster secure and authenticated interactions between business processes, software agents, Internet of Things objects, clients, and business stakeholders. The integration of enhanced business data security based on the decentralized attributes of blockchain is appealing, particularly because of the potential to introduce solutions that significantly reduce system unavailability, communication issues, and illegal data access procedures [113-118]. On the other hand, the process of integrating business procedures and data protection through the support of blockchain technology is associated with issues that should be discussed and will also benefit from research and development. Technically, blockchain technology, due to its current limitations in terms of storage and large transaction time latency, would always advocate for collaboration with traditional security paradigms and infrastructure. It would aid in developing more diverse systems composed of trusted and traditional security components along with emerging blockchain-based security processes. It should be noted that an end-to-end data security system, including external data interchange, may always be more secure. In some cases, the rise of blockchain technology in e-business can lead to a stronger push by attackers to falsify or take down the blockchain infrastructure through distributed denial of service attacks or similar actions causing unavailability of data and log records. Therefore, completely relying only on blockchain technology for data security, considering its resistance to powerful attacks, can lead to trust issues. This mindset of an organization's approach towards the integration of blockchain in data security can be a good directive for strategic planning of future research and the development of the entire spatial e-business framework. These new features and systems should always be developed or inspire more secure environments but not rely upon complex structures. Research and development on the integration of blockchain and data security should focus on hybridization of existing technical and blockchain processes to ensure that a breach of one system can be identified while the blockchain system is used for ensuring provenance and security of the compromised system. Additionally, research and development for IT services, such as the integration of technology, information, and security compliance, always requires a global mindset and better collaboration, particularly between business, cyber, and blockchain domain stakeholders [119-121].

Challenges and Opportunities

Without question, the integration of blockchain and data security involves significant obstacles for e-business. Firstly, blockchain is an emerging technology and accounts for a high initial investment. Blockchain projects are not merely an extension of existing businesses, but rather have the potential to initiate innovative business ventures that will lead to the future of businesses. Secondly, blockchain technologies inherently consist of cryptographic algorithms and have an underlying P2P system. If an organization lacks in-house expertise in this emerging technology, it may entail hiring professional staff or training courses in the adaptation of this technology. In addition, despite the benefits of blockchain, there are regulatory developments that need to be taken into consideration, as there is uncertainty about how existing regulation applies to blockchain. Accordingly, investment in blockchain technology is not expected to increase unless organizations can assure and accept this level of risk [122-125]. Over time, blockchain regulation is expected to adapt to facilitate the use of the technology while still protecting users from criminal activity. However, while challenges exist, this analysis balances the opportunities that the integration of blockchain and data security can bring to e-business. Increased data security is a primary benefit, mitigating potential risks from traditional digital security-based approaches by using blockchain to package data, data transmission, etc. via blockchain and encrypting custom data in the blockchain. In relation to data transmission, it is possible to create smart materials, process or contract papers that are encrypted on a blockchain. It improves data management and is cost-effective, given this process can be automated via technology. Finally, it is possible to limit control with advanced permissions, which reduces administrative overhead and increases network efficiency [126-130].

5. Future Trends and Innovations

The blockchain industry is evolving at a rapid rate to enhance current capabilities and improve existing features. In the present era, blockchain is a slow distributed database that suffers from scalability issues, but in

Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

the coming years, blockchain is expected to be scalable. Blockchain can be a more meaningful technology if it enables developers to create new e-business models, decentralize digital identity and supply chain management, provide consumer protection, protect against cyber-attacks, ensure secure voting, support a decentralized internet, and facilitate identity for the internet provided by the government and IoT applications. It also provides opportunities across advanced supply chains, IoT, and other verticals and industries. The future generations of blockchains are expected to focus on innovation in blockchain operations, along with digital contracts and multi-party computing. The future blockchain for supply chain management is expected to be based on side-chain technology. It involves 5G and blockchain features founded on different criteria to improve connection, interaction, and security [131-136]. Artificial Intelligence and Machine Learning are also expected to strengthen the blockchain industry's security capabilities. Recently, algorithms have been built with the aid of AI and ML to detect vulnerabilities and threats in blockchain platforms. AI discovers malicious programs that cause significant data breaches. AI-based deep learning models are also developed to detect network anomalies, such as distributed denial-of-service attacks that aim to make a network or website unavailable to users. These networks would be very unsafe without the aid of artificial intelligence, especially as the system becomes more deeply involved. From various perspectives of blockchain, the wellbeing of blockchain is determined by a minimum of 4.67. Furthermore, due to new and unanticipated applications, blockchain is recognized as serious in various industries, as this scenario expands rapidly throughout the world and may disrupt many business processes. Any decision-maker in an unexpected industry should continuously evaluate the latest impacts and trends to be fully aware of blockchain technology's capabilities and stay competitive in their current e-business environment. In comparison, regulatory authorities and governments must continuously modify and review current regulatory frameworks as a complement to emerging issues. These must be anticipated and acknowledged as the current cryptocurrency landscape evolves. The journey of blockchain is unpredictable, but potential opportunities are immense [137-142].

6. Conclusion

The Fourth Industrial Revolution has accelerated the growth of e-business, which in turn has intensified the ferocious competition and spate of value chain as an extension of data activities. This has also created inherent vulnerabilities, visible and invisible, that may potentially be exploited by adversaries. A thorough contemplation reveals blockchain as an apparatus that can take e-business enterprises a step closer to a state of invincibility against possible attacks. The spike in Ransomware as a Service is indicative of a surmounting volume of threats in cyberspace. E-businesses can't hesitate in maintaining the status quo; the use of exploding cryptocurrencies in these transactions indicates that this is something more than it should be. Coined as a disruptive technology, blockchain and cryptocurrencies being heralded for the same can bring us to a conclusion indicating that we need a paradigm shift to get rid of this whirlpool. The faster coordinated efforts are made to use data security technologies that connect the data manager and data owner while providing secure code and real-time process integrity to deal with evolving threat models, the more businesses shall be able to counter quota-busting tactics thrown at them. There are, therefore, several implications associated with e-business being secured with the use of blockchain. E-business operational efficacy improves because of data security in hostage or trap situations. Business-customer trust is established and magnified due to the assistance delivered in maintaining the confidentiality of transactions. A competitive edge is established owing to operational prudence. The agony of e-businesses is quite clearly visible; they lack this cog in their security framework. Also, the composition of this cog has become quite clear, and future e-business environments may significantly witness blockchain firms operating equally with the cryptocurrency blooming companies because of this cog. The best moves for organizations would be to think about a security culture now instead of dealing with their accountants and reporting their losses in the account books later. It can come into the image now or after all current security technologies have been defeated. This raises the impetus such that investment should be prudent, and this investment, by the virtue of blockchain, can't be questioned even in unquantifiable terms.

7. References

[1] Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J. (2020). A survey on blockchain technology concepts, applications, and issues. SN Computer Science. https://doi.org/10.1007/s42979-020-00123-0

[2] Laroiya, C., Saxena, D., & Komalavalli, C. (2020). Applications of blockchain technology. In Handbook of research on blockchain technology (pp. 213-243). Academic Press. https://doi.org/10.1016/B978-0-12-819816-2.00009-5
[3] Garcia-Teruel, R. M. (2020). Legal challenges and opportunities of blockchain technology in the real estate sector. Journal of Property, Planning and Environmental Law, 12(2), 129-145. https://doi.org/10.1108/JPPEL-07-2019-0039
[4] Amadi-Echendu, A. P. (2021). Using blockchain technology to facilitate property transactions. South African Journal of Information Management, 23(1), 1-7. https://doi.org/10.4102/sajim.v23i1.1421
[5] Luo, L. (2022). Application of blockchain technology in intellectual property protection. Mathematical Problems in Engineering. https://doi.org/10.1155/2022/4641559
[6] Gousteris, S., Stamatiou, Y. C., Halkiopoulos, C., Antonopoulou, H., & Kostopoulos, N. (2023). Secure Distributed Cloud Storage based on the Blockchain Technology and Smart Contracts. Emerging Science Journal, 7(2), 469–479. https://doi.org/10.28991/esj-2023-07-02-012
[7] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of blockchain technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073
[8] Albayati, H., Kim, S. K., & Rho, J. J. (2020). Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach. Technology in Society. https://doi.org/10.1016/j.techsoc.2020.101320
[9] Zhu, P., Hu, J., Li, X., & Zhu, Q. (2021). Using blockchain technology to enhance the traceability of original achievements. IEEE Transactions on Engineering Management, 70(5), 1693-1707. https://doi.org/10.1109/TEM.2021.3066090
[10] Rijanto, A. (2021). Blockchain technology adoption in supply chain finance. Journal of Theoretical and Applied Electronic Commerce Research, 16(7), 3078-3098. https://doi.org/10.3390/jtaer16070168
[11] Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In Handbook of research on blockchain technology (pp. 349-371). Academic Press. https://doi.org/10.1016/B978-0-12-819816-2.00014-9
[12] Antonopoulou, H., Theodorakopoulos, L., Halkiopoulos, C., & Mamalougkou, V. (2023). Utilizing Machine Learning to Reassess the Predictability of Bank Stocks. Emerging Science Journal, 7(3), 724–732. https://doi.org/10.28991/esj-2023-07-03-04
[13] Saini, K. (2021). Blockchain foundation. In Essential Enterprise Blockchain Concepts and Applications (pp. 1-14). Auerbach Publications. https://doi.org/10.1201/9781003097990-1
[14] Deshmukh, A., Tyagi, A. K., Hansora, H., & Menon, S. C. (2023). Applications of distributed ledger (blockchain) technology in e-healthcare. In The Internet of Medical Things (IoMT) and Telemedicine Frameworks and Applications (pp. 248-261). IGI Global. https://doi.org/10.4018/978-1-6684-3533-5.ch013
[15] Hashmi, S. A., Ali, C. F., & Zafar, S. (2021). Internet of things and cloud computing-based energy management system for demand side management in smart grid. International Journal of Energy Research, 45(1), 1007-1022. https://doi.org/10.1002/er.6141
[16] Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain-based cloud computing: Architecture and research challenges. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3036812
[17] Sharma, P., & Kantha, P. (2020). Blynk'cloud server based monitoring and control using 'NodeMCU. International Research Journal of Engineering and Technology (IRJET), 7(10), 1362-1366.
[18] Stamatiou, Y., Halkiopoulos, C., & Antonopoulou, H. (2023). A Generic, Flexible Smart City Platform focused on Citizen Security and Privacy. Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics. https://doi.org/10.1145/3635059.3635095
[19] Awaisi, K. S., Hussain, S., Ahmed, M., Khan, A. A., & Ahmed, G. (2020). Leveraging IoT and fog computing in healthcare systems. IEEE Internet of Things Magazine, 3(2), 52-56. https://doi.org/10.1109/IOTM.0001.1900096
[20] Vergne, J. P. (2020). Decentralized vs. distributed organization: Blockchain, machine learning, and the future of the digital platform. Organization Theory. https://doi.org/10.1177/2631787720977052
[21] Hsieh, Y. Y. & Vergne, J. P. (2023). The future of the web? The coordination and early-stage growth of decentralized platforms. Strategic Management Journal. https://doi.org/10.1002/smj.3455
[22] Zarrin, J., Wen Phang, H., Babu Saheer, L., & Zarrin, B. (2021). Blockchain for decentralization of internet: Prospects, trends, and challenges. Cluster Computing. https://doi.org/10.1007/s10586-021-03301-8
[23] Theodorakopoulos, L., & Theodoropoulou, A. (2024). Leveraging Big Data Analytics for Understanding Consumer Behavior in Digital Marketing: A Systematic Review. Human Behavior and Emerging Technologies, 2024(1). Portico. https://doi.org/10.1155/2024/3641502
[24] Baninemeh, E., Farshidi, S., & Jansen, S. (2023). A decision model for decentralized autonomous organization platform selection: Three industry case studies. Blockchain: Research and Applications, 4(2), 100127. https://doi.org/10.1016/j.bcra.2023.100127

[25] Mueller-Bloch, C., Andersen, J. V., Spasovski, J., & Hahn, J. (2024). Understanding decentralization of decision-making power in proof-of-stake blockchains: An agent-based simulation approach. European Journal of Information Systems, 33(3), 267-286. https://doi.org/10.1080/0960085X.2022.2125840
[26] Rahardja, U., Ngadi, M. A., Budiarto, R., Aini, Q., Hardini, M., & Oganda, F. P. (2021). Education exchange storage protocol: Transformation into decentralized learning platform. Frontiers in Education. https://doi.org/10.3389/feduc.2021.782969
[27] Leng, J., Chen, Z., Huang, Z., Zhu, X., Su, H., Lin, Z., & Zhang, D. (2022). Secure blockchain middleware for decentralized IIoT towards industry 5.0: A review of architecture, enablers, challenges, and directions. Machines. https://doi.org/10.3390/machines10100858
[28] Bolek, V., Romanová, A., & Korček, F. (2023). The information security management systems in E-business. Journal of Global Information Management, 31(1), 1-29. https://doi.org/10.4018/JGIM.316833
[29] Esmaeilpour Ghouchani, B., Jodaki, S., Joudaki, M., Balali, A., & Rajabion, L. (2020). A model for examining the role of the Internet of Things in the development of e-business. VINE Journal of Information and Knowledge Management Systems, 50(1), 20-33. https://doi.org/10.1108/VJIKMS-04-2019-0058
[30] Halkiopoulos, C., Antonopoulou, H., Gkintoni, E., Aroutzidis, A. (2021). Neuromarketing as an Indicator of Cognitive Consumer Behavior in Decision Making Process of Tourism Destination. In: Katsoni, V., Șerban, A.C. (eds) Transcending Borders in Tourism Through Innovation and Cultural Heritage. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-030-92491-1_41
[31] Setyowati, W., Widayanti, R., & Supriyanti, D. (2021). Implementation of e-business information system in Indonesia: Prospects and challenges. International Journal of Cyber and IT Service Management, 1(2), 180-188. https://doi.org/10.34306/ijcitsm.v1i2.49
[32] Kala, E. M. (2023). The impact of cyber security on business: How to protect your business. Open Journal of Safety Science and Technology. https://doi.org/10.4236/ojsst.2023.132003
[33] Sumaryanti, L., Kusuma, D. H., Widijastuti, R., & Muzaki, M. N. (2021). Improvement security in e-business systems using hybrid algorithm. TELKOMNIKA (Telecommunication Computing Electronics and Control), 19(5), 1535-1543. https://doi.org/10.12928/telkomnika.v19i5.20403
[34] Bakalis, A., Halkiopoulos, C., & Antonopoulou, H. (2024). The Digital Transformation of Tourism. Case Study of Greek Tourism. Springer Proceedings in Business and Economics, 121–157. https://doi.org/10.1007/978-3-031-54338-8_9
[35] El-Ebiary, Y. A. B., Almandeel, S., Ghanem, W. A. H., Abu-Ulbeh, W., Al-Dubai, M. M. M., & Bamansoor, S. (2020). Security issues and threats facing the electronic enterprise leadership. 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). https://doi.org/10.1109/ICIMCIS51567.2020.9354330
[36] Eltweri, A., Faccia, A., Roxana Moțteanu, N., Sawan, N., & Pio Leonardo Cavaliere, L. (2020). The role of risk management in auditing e-business. 2020 4th International Conference on Software and e-Business. https://doi.org/10.1145/3446569.3446584
[37] Antonopoulou, H., Halkiopoulos, C., Barlou, O., Beligiannis, G. (2019). Transition from Educational Leadership to e-Leadership: A Data Analysis Report from TEI of Western Greece. International Journal of Learning, Teaching and Educational Research, 18 (9), pp.238-255. DOI:10.26803/ijlter.18.9.13
[38] Ethan, O., & Umar, H. (2024). Comparative analysis of e-commerce database technologies: Blockchain, scalable storage, and cyber defense strategies. Unpublished. https://doi.org/10.13140/RG
[39] Bibhu, V., Kumar, A., Lohani, B. P., & Kushwaha, P. K. (2021). Robust secured framework for online business transactions over public network. 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). https://doi.org/10.1109/ICIEM51511.2021.9445380
[40] Theodorakopoulos, L., Theodoropoulou, A., & Halkiopoulos, C. (2024). Enhancing Decentralized Decision-Making with Big Data and Blockchain Technology: A Comprehensive Review. Applied Sciences, 14(16), 7007. https://doi.org/10.3390/app14167007
[41] Ma, X., & Wang, Z. (2024). Computer security technology in e-commerce platform business model construction. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e28571
[42] Taherdoost, H. (2023). Legal, regulatory, and ethical considerations in e-business. In E-Business Essentials: Building a Successful Online Enterprise (pp. 379-402). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-39626-7_15
[43] Taherdoost, H. (2023). Introduction to E-Business. In E-Business Essentials: Building a Successful Online Enterprise (pp. 1-24). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-39626-7_1
[44] Gopinath, N., & Padmaja, D. S. (2025). Ethical and legal issues in e-business. In Business Transformation in the Era of Digital Disruption (pp. 293-300). IGI Global. https://doi.org/10.4018/979-8-3693-7056-8.ch011
[45] Gkintoni, E., Halkiopoulos, C., Antonopoulou, H., & Togias, P. (2016). Emotional Intelligence in Social Network Consumers. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4312266

[46] Hu, Z., Wu, G., Wu, H., & Zhang, L. (2022). Cross-sectoral preparedness and mitigation for networked typhoon disasters with cascading effects. Urban Climate. https://doi.org/10.1016/j.uclim.2022.101140
[47] Bikhchandani, S., Hirshleifer, D., Tamuz, O., & Welch, I. (2024). Information cascades and social learning. Journal of Economic Literature, 62(3), 1040-1093. https://doi.org/10.1257/jel.20241472
[48] Fereshtehnejad, E., Gidaris, I., Rosenheim, N., Tomiczek, T., Padgett, J. E., Cox, D. T., ... & Peacock, W. (2021). Probabilistic risk assessment of coupled natural-physical-social systems: Cascading impact of hurricane-induced damages to civil infrastructure in Galveston, Texas. Natural Hazards Review, 22(3), 04021013. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000459
[49] Semakula, H. M., Liang, S., Mukwaya, P. I., & Mugagga, F. (2023). Application of a Bayesian network modeling approach to predict the cascading effects of COVID-19 restrictions on the planting activities of smallholder farmers. Agricultural Systems. https://doi.org/10.1016/j.agsy.2023.103733
[50] Schemmer, M., Heinz, D., Baier, L., Vössing, M., & Kühl, N. (2021). Conceptualizing digital resilience for AI-based information systems. ECIS.
[51] Halkiopoulos, C., Antonopoulou, H., Gkintoni, E., & Aroutzidis, A. (2022). Neuromarketing as an Indicator of Cognitive Consumer Behavior in Decision-Making Process of Tourism destination—An Overview. Springer Proceedings in Business and Economics, 679–697. https://doi.org/10.1007/978-3-030-92491-1_41
[52] Thakur, M. (2024). Cyber security threats and countermeasures in the digital age. Journal of Applied Science and Education (JASE).
[53] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. https://doi.org/10.1016/j.egyr.2021.08.126
[54] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208. https://doi.org/10.1080/23270012.2020.1731721
[55] Almeida, F., Santos, J. D., & Monteiro, J. A. (2020). The challenges and opportunities in the digitalization of companies in a post-COVID-19 world. IEEE Engineering Management Review, 48(3), 97-103. https://doi.org/10.1109/EMR.2020.3013206
[56] Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2021b). Associations between Traditional and Digital Leadership in Academic Environment: During the COVID-19 Pandemic. Emerging Science Journal, 5(4), pp.405–428. DOI:10.28991/esj-2021-01286
[57] Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., Egerson, J., ... & Egerson, J. (2024). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. World Journal of Advanced Research and Reviews, 23(1), 81-96. https://doi.org/10.30574/wjarr.2024.23.1.1900
[58] Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and privacy issues. 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). https://doi.org/10.1109/TPSISA52974.2021.00032
[59] Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460. https://doi.org/10.3390/electronics9091460
[60] Gkintoni, E., Halkiopoulos, C., Antonopoulou, H., & Togias, P. (2016). Emotional Intelligence in Social Network Consumers. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4312266
[61] Theodorakopoulos, L., Karanikola, Z., Katsonis, N., & Papadopoulos, D. (2018). The Use of New Information and Communication Technologies In The Learning Process: A Case Study of Secondary Education In The Prefecture of Aitoloakarnania. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4209722
[62] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
[63] Rodrigues, M., Franco, M., Sousa, N., & Silva, R. (2021). COVID-19 and the business management crisis: An empirical study in SMEs. Sustainability. https://doi.org/10.3390/su13115912
[64] Gkinton, E., Telonis, G., Halkiopoulos, C., & Boutsinas, B. (2023). Quality of Life and Health Tourism: A Conceptual Roadmap of Enhancing Cognition and Well-Being. Springer Proceedings in Business and Economics, 651–666. https://doi.org/10.1007/978-3-031-26829-8_41
[65] Lyngdoh, S. W., & Chhering, M. (2025). Cybersecurity threats and legal responsibilities in e-business: An Indian perspective. In Business Transformation in the Era of Digital Disruption (pp. 259-292). IGI Global. https://doi.org/10.4018/979-8-3693-7056-8.ch010
[66] Odokuma, E. E., & Musa, M. O. (2022). Internet threats and mitigation methods in electronic businesses post-COVID-19. International Journal of Computer Applications. https://doi.org/10.5120/ijca2022922195
[67] Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: A framework for salient research topics. Electronic Commerce Research and Applications, 48, 101054. https://doi.org/10.1016/j.elerap.2021.101054

[68] Papadopoulos, D., Gkintoni, E., Halkiopoulos, C., & Antonopoulou, H. (2023). e-Tourism and Online Reservation Systems in Electronic Business. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4319582
[69] Sestino, A., Giraldi, L., Cedrola, E., Zamani, S. Z., & Guido, G. (2022). The business opportunity of blockchain value creation among the Internet of value. Global Business Review. https://doi.org/10.1177/09721509221115012
[70] Cheng, H. K., Hu, D., Puschmann, T., & Zhao, J. L. (2021). The landscape of blockchain research: Impacts and opportunities. Information Systems and e-Business Management, 19(3), 749-755. https://doi.org/10.1007/s10257-021-00544-1
[71] Marikyan, D., Papagiannidis, S., Rana, O., & Ranjan, R. (2021). Blockchain in a business model: Exploring benefits and risks. In Responsible AI and Analytics for an Ethical and Inclusive Digitized Society: 20th IFIP WG 6.11 Conference on e-Business, e-Services and e-Society (pp. 555-566). Springer. https://doi.org/10.1007/978-3-030-85447-8_46
[72] Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2021a). Transformational Leadership and Digital Skills in Higher Education Institutes: During the COVID-19 Pandemic. Emerging Science Journal, 5(1), pp.1–15. DOI:10.28991/esj-2021-01252
[73] Abdulkareem, M., & Sami, T. M. G. (2024). Cloud-web principles-based blockchain technology for sustainable and secure enterprise systems integrating AI and IoT for transparency and traceability.
[74] Wang, Z., Li, M., Lu, J., & Cheng, X. (2022). Business innovation based on artificial intelligence and blockchain technology. Information Processing & Management. https://doi.org/10.1016/j.ipm.2021.102759
[75] Faccia, A., De Lucia, C., Eltweri, A., Sawan, N., & Cavaliere, L. P. (2020). Extended audit report: Enhancing trust and reputation in IT processes and across e-business industries. 2020 2nd International Conference on E-Business and E-commerce Engineering, 23-27. https://doi.org/10.1145/3446922.3446927
[76] Ji, F., & Tia, A. (2021). The effect of blockchain on business intelligence efficiency of banks. Kybernetes. https://doi.org/10.1108/K-10-2020-0668
[77] Nodehi, T., Zutshi, A., Grilo, A., & Rizvanovic, B. (2022). EBDF: The enterprise blockchain design framework and its application to an e-procurement ecosystem. Computers & Industrial Engineering, 171, 108360. https://doi.org/10.1016/j.cie.2022.108360
[78] Antonopoulou, H., Giannoulis, A., Theodorakopoulos, L., & Halkiopoulos, C. (2022). Socio-Cognitive Awareness of Inmates through an Encrypted Innovative Educational Platform. International Journal of Learning, Teaching and Educational Research, 21(9), 52–75. https://doi.org/10.26803/ijlter.21.9.4
[79] Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654. https://doi.org/10.1016/j.cose.2019.101654
[80] Hamledari, H., & Fischer, M. (2021). Role of blockchain-enabled smart contracts in automating construction progress payments. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 13(1), 04520038. https://doi.org/10.1061/(ASCE)LA.1943-4170.0000442
[81] Stamatiou, Y. C., Halkiopoulos, C., Giannoulis, A., & Antonopoulou, H. (2022). Utilizing a Restricted Access e-Learning Platform for Reform, Equity, and Self-development in Correctional Facilities. Emerging Science Journal, 6, 241–252. https://doi.org/10.28991/esj-2022-sied-017
[82] Tolmach, P., Li, Y., Lin, S. W., Liu, Y., & Li, Z. (2021). A survey of smart contract formal specification and verification. ACM Computing Surveys (CSUR). https://doi.org/10.1145/3464421
[83] Permenev, A., Dimitrov, D., Tsankov, P., Drachsler-Cohen, D., & Vechev, M. (2020). Verx: Safety verification of smart contracts. 2020 IEEE Symposium on Security and Privacy (SP), 1661-1677. https://doi.org/10.1109/SP40000.2020.00024
[84] Sirena, P., & Patti, F. P. (2022). Smart contracts and automation of private relationships. In Constitutional Challenges in the Algorithmic Society (pp. 315-330). Cambridge University Press. https://doi.org/10.1017/9781108914857.017
[85] Panas, G., Thrasidi, N., Halkiopoulos, C., & Gkintoni, E. (2022). Consumer Behavior and Cognitive Factors in Relation to Gastronomic Tourism and Destination Marketing in Greece. Springer Proceedings in Business and Economics, 655–677. https://doi.org/10.1007/978-3-030-92491-1_40
[86] Dolat-abadi, H. M., Rasi, M., & Sadat, S. A. (2024). Smart contracts as a third-party coordinator: Tools for implementing agreements in e-business management. In Building Smart and Sustainable Businesses With Transformative Technologies (pp. 123-151). IGI Global. https://doi.org/10.4018/979-8-3693-0210-1.ch008
[87] Gómez, C., Pérez Blanco, F. J., Vara, J. M., De Castro, V., & Marcos, E. (2021). Design and development of smart contracts for e-government through value and business process modeling. Hawaii International Conference on System Sciences (HICSS). https://doi.org/10.24251/HICSS.2021.254
[88] De Andrés, J., & Lorca, P. (2021). On the impact of smart contracts on auditing. International Journal of Digital Accounting Research. https://doi.org/10.4192/1577-8517-v21_6

[89] Halkiopoulos, C., Giotopoulos, K., Antonopoulou, H., & Theodorakopoulos, L. (2020). E-Business and Cloud Computing Services in Greek Companies during Economic Recession. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4153968
[90] Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Networking and Applications, 14, 2901-2925. https://doi.org/10.1007/s12083-021-01127-0
[91] Nanayakkara, S., Perera, S., Senaratne, S., Weerasuriya, G. T., & Bandara, H. M. N. D. (2021). Blockchain and smart contracts: A solution for payment issues in construction supply chains. Informatics, 8(2), 36. https://doi.org/10.3390/informatics8020036
[92] Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., ... & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. Renewable and Sustainable Energy Reviews, 158, 112013. https://doi.org/10.1016/j.rser.2021.112013
[93] Panas, G., Thrasidi, N., Halkiopoulos, C., Gkintoni, E. (2021). Consumer Behavior and Cognitive Factors in Relation to Gastronomic Tourism and Destination Marketing in Greece. In: Katsoni, V., Şerban, A.C. (eds) Transcending Borders in Tourism Through Innovation and Cultural Heritage. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-030-92491-1_40
[94] Rathnayake, I., Wedawatta, G., & Tezel, A. (2022). Smart contracts in the construction industry: A systematic review. Buildings, 12(12), 2082. https://doi.org/10.3390/buildings12122082
[95] Li, G., Xue, J., Li, N., & Ivanov, D. (2022). Blockchain-supported business model design, supply chain resilience, and firm performance. Transportation Research Part E: Logistics and Transportation Review, 163, 102773. https://doi.org/10.1016/j.tre.2022.102773
[96] Yeh, T. Y., & Kashef, R. (2020). Trust-based collaborative filtering recommendation systems on the blockchain. Advances in Internet of Things. https://doi.org/10.4236/ait.2020.104004
[97] Gkintoni, E., Kakoleres, G., Telonis, G., Halkiopoulos, C., & Boutsinas, B. (2023). A Conceptual Framework for Applying Social Signal Processing to Neuro-Tourism. Springer Proceedings in Business and Economics, 323–335. https://doi.org/10.1007/978-3-031-26829-8_20
[98] Saleh, M. A., Khatri, S. P., Ghrayeb, A., & Refaat, S. S. (2024). A review on the applications of blockchain-based smart contracts in the smart grid. 2024 4th International Conference on Smart Grid and Renewable Energy (SGRE). https://doi.org/10.1109/SGRE59715.2024.10428798
[99] Theodorakopoulos, L., Theodoropoulou, A., & Stamatiou, Y. (2024). A State-of-the-Art Review in Big Data Management Engineering: Real-Life Case Studies, Challenges, and Future Research Directions. Eng, 5(3), 1266–1297. https://doi.org/10.3390/eng5030068
[100] Zhu, Q., Kouhizadeh, M., & Sarkis, J. (2022). Formalizing product deletion across the supply chain: Blockchain technology as a relational governance mechanism. International Journal of Production Research, 60(1), 92-110. https://doi.org/10.1080/00207543.2021.1987552
[101] Hader, M., Tchoffa, D., El Mhamedi, A., Ghodous, P., Dolgui, A., & Abouabdellah, A. (2022). Applying integrated blockchain and big data technologies to improve supply chain traceability and information sharing in the textile sector. Journal of Industrial Information Integration, 28, 100345. https://doi.org/10.1016/j.jii.2022.100345
[102] Halkiopoulos, C., & Giotopoulos, K. (2022). Tourism's Use of Web-Based Information Systems and the Influence of Tourism Trends. Springer Proceedings in Business and Economics, 407–426. https://doi.org/10.1007/978-3-030-92491-1_25
[103] Raja Santhi, A., & Muthuswamy, P. (2022). Influence of blockchain technology in manufacturing supply chain and logistics. Logistics, 6(1), 15. https://doi.org/10.3390/logistics6010015
[104] Antonopoulou, H., Giannoulis, A., Theodorakopoulos, L., & Halkiopoulos, C. (2022). Distance Education Opportunities in the Fields of Social Justice, Equality, and Human Rights for Inmates During Pandemic. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4019002
[105] Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021). On blockchain integration with supply chain: Overview on data transparency. Logistics, 5(3), 46. https://doi.org/10.3390/logistics5030046
[106] Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., & Secundo, G. (2022). Blockchain technology for bridging trust, traceability, and transparency in circular supply chain. Information & Management, 59(7), 103508. https://doi.org/10.1016/j.im.2021.103508
[107] Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation Research Part E: Logistics and Transportation Review, 142, 102067. https://doi.org/10.1016/j.tre.2020.102067
[108] Gkintoni, E., Halkiopoulos, C., Antonopoulou, H. (2022). Neuroleadership an Asset in Educational Settings: An Overview. Emerging Science Journal. Emerging Science Journal, 6(4), 893–904. DOI:10.28991/esj-2022-06-04-016

Technium Business and Management (TBM)
Vol. 10, pp.109-122 (2024)
ISSN: 2821-4366
www.techniumscience.com

[109] Al-Zaqeba, M., Jarah, B., Ineizeh, N., Almatarneh, Z., & Jarrah, M. A. A. L. (2022). The effect of management accounting and blockchain technology characteristics on supply chains efficiency. Uncertain Supply Chain Management, 10(3), 973-982. https://doi.org/10.5267/j.uscm.2022.2.016
[110] Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. Sustainability, 13(4), 1726. https://doi.org/10.3390/su13041726
[111] Giotopoulos, K., Halkiopoulos, C., Papadopoulos, D., Antonopoulou, H., (2019). Towards Bring Your Own Device Marketing Policy. International Journal of Technology Marketing, 13(2). Inderscience Publishers: IJTMKT-10313. DOI:10.1504/ijtmkt.2019.10023906
[112] Rawat, R. (2022). A systematic review of blockchain technology use in e-supply chain in internet of medical things (IoMT). International Journal of Computations, Information and Manufacturing (IJCIM), 2(2). https://doi.org/10.54489/ijcim.v2i2.119
[113] Desai, B., Patil, K., Mehta, I., & Patil, A. (2024). A secure communication framework for smart city infrastructure leveraging encryption, intrusion detection, and blockchain technology. Advances in Computer Sciences, 7(1).
[114] Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing zero-trust models in the financial industry through blockchain integration: A proposed framework. Electronics, 13(5), 865. https://doi.org/10.3390/electronics13050865
[115] Akanfe, O., Lawong, D., & Rao, H. R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. International Journal of Information Management, 76, 102753. https://doi.org/10.1016/j.ijinfomgt.2024.102753
[116] Kandukuri, V. (2024). The effectiveness of blockchain technology in detecting, mitigating and securing cyber threats. Asian Journal of Information Technology.
[117] Dave, C. (2024). Security challenges with blockchain: Navigate blockchain security challenges, unveil vulnerabilities, and gain practical strategies for secure application.
[118] Antonopoulou, H. (2024). Personality Traits and the Growth of Emotional Intelligence. A Systematic Evaluation. Technium Education and Humanities, 6, 173–184. https://doi.org/10.47577/teh.v6i.9442
[119] Zawaideh, F. H., Abu-Ulbeh, W., Mjlae, S. A., El-Ebiary, Y. A. B., Al Moaiad, Y., & Das, S. (2023). Blockchain solution for SMEs cybersecurity threats in e-commerce. 2023 International Conference on Computer Science and Emerging Technologies (CSET). https://doi.org/10.1109/CSET58993.2023.10346628
[120] Belghith, A. (2022). Investigation on e-commerce platforms for tackling e-business security challenges. International Journal on Engineering Applications, 10(6). https://doi.org/10.15866/irea.v10i6.20649
[121] Blancaflor, E., Aquino, J. P. J., Bravo, P. B., Pallarca, R. H., & Pascua, J. G. (2022). A review on cryptocurrency (a blockchain technology) scams in the Philippines. 6th International Conference on E-Business and Internet. https://doi.org/10.1145/3572647.3572674
[122] Du, J., Shi, Y., Li, W., & Chen, Y. (2023). Can blockchain technology be effectively integrated into the real economy? Evidence from corporate investment efficiency. China Journal of Accounting Research. https://doi.org/10.1016/j.cjar.2023.100292
[123] George, K., & Patatoukas, P. N. (2021). The blockchain evolution and revolution of accounting. In Information for Efficient Decision Making: Big Data, Blockchain and Relevance (pp. 157-172). https://doi.org/10.1142/9789811220470_0006
[124] Giannoulis, A., Theodorakopoulos, L., & Antonopoulou, H. (2022). Learning in Second-Chance Schools during COVID-19 Case Study: Legal Framework and Distance Learning Platforms in Greek Prison. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4132811
[125] Pimentel, E., & Boulianne, E. (2020). Blockchain in accounting research and practice: Current trends and future opportunities. Accounting Perspectives. https://doi.org/10.1111/1911-3838.12239
[126] Ani, N., Millah, S., & Sunarya, P. A. (2024). Optimizing online business security with blockchain technology. Startupreneur Business Digital (SABDA Journal), 3(1), 67-80. https://doi.org/10.33050/sabda.v3i1.488
[127] Al Khaldy, M., Alshdifat, G., Almalahmeh, T., & Aldweesh, A. (2024). Blockchain as a resilient infrastructure for e-business transactions. 2nd International Conference on Cyber Resilience (ICCR). https://doi.org/10.1109/ICCR61006.2024.10532913
[128] Halkiopoulos, C., & Gkintoni, E. (2024). Leveraging AI in E-Learning: Personalized Learning and Adaptive Assessment through Cognitive Neuropsychology—A Systematic Analysis. Electronics, 13(18), 3762. https://doi.org/10.3390/electronics13183762
[129] Xuan, T. R., & Ness, S. (2023). Integration of blockchain and AI: Exploring application in digital business. Journal of Engineering Research and Reports, 25(8), 20-39. https://doi.org/10.9734/jerr/2023/v25i8955
[130] Vetrivel, S. C., Arun, V. P., Sowmiya, K. C., & Sabareeshwari, V. (2024). Personalized healthcare in the era of e-business 5.0: Harnessing the power of big data. In Smart Technologies and Innovations in E-Business (pp. 186-203). IGI Global. https://doi.org/10.4018/978-1-6684-7840-0.ch010
[131] Sanka, A. I., & Cheung, R. C. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis, and future research. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2021.103232

[132] Giannoulis, A., Antonopoulou, H., & Halkiopoulos, C. (2022). EDUCATIONAL LEARNING METHODS WITH GAMIFICATION ASPECTS FOR INMATES DURING PANDEMIC. EDULEARN22 Proceedings, 1, 5746–5751. https://doi.org/10.21125/edulearn.2022.1351
[133] Alghamdi, T. A., Khalid, R., & Javaid, N. (2024). A survey of blockchain-based systems: Scalability issues and solutions, applications, and future challenges. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3408868
[134] Zulkifli, A. (2023). Accelerating database efficiency in complex IT infrastructures: Advanced techniques for optimizing performance, scalability, and data management in distributed systems. International Journal of Information and Cybersecurity, 7(12), 81-100.
[135] Alrehaili, A., Namoun, A., & Tufail, A. (2021). A comparative analysis of scalability issues within blockchain-based solutions in the Internet of Things. International Journal of Advanced Computer Science and Applications, 12(9). https://doi.org/10.14569/IJACSA.2021.0120955
[136] Antonopoulou, H. (2024). The Value of Emotional Intelligence: Self-Awareness, Self-Regulation, Motivation, and Empathy as Key Components. Technium Education and Humanities, 8, 78–92. https://doi.org/10.47577/teh.v8i.9719
[137] Antonopoulou, H. (2023). Evolutionary Features of Personality Research and Leadership Traits. A Comprehensive Analysis. Technium Business and Management, 6, 58–69. https://doi.org/10.47577/business.v6i.9717
[138] Antonopoulou, H. (2023). Building up Leadership Skills in Vulnerable Social Groups. Case Study in Bipolar Disorder and Psychoeducation Contribution. Technium Business and Management, 6, 70–79. https://doi.org/10.47577/business.v6i.9718
[139] Hussain, A. A., & Al-Turjman, F. (2021). Artificial intelligence and blockchain: A review. Transactions on Emerging Telecommunications Technologies, 32(9), e4268. https://doi.org/10.1002/ett.4268
[140] Antonopoulou, H. (2024). The Contribution of Mental Capacity to Personality Formulation. An Overview. Technium Education and Humanities, 7, 101–114. https://doi.org/10.47577/teh.v7i.9720
[141] Mansour, R. F. (2022). Artificial intelligence-based optimization with deep learning model for blockchain-enabled intrusion detection in CPS environment. Scientific Reports. https://doi.org/10.1038/s41598-022-17043-z
[142] Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Network. https://doi.org/10.1109/MNET.021.1900629