IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 November 2023, accepted 19 December 2023, date of publication 1 January 2024,
date of current version 10 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3349019

SURVEY

On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security

OLEKSANDR KUZNETSOV[1,2,3], (Member, IEEE), PAOLO SERNANI[4], LUCA ROMEO[5], EMANUELE FRONTONI[2], (Member, IEEE), AND ADRIANO MANCINI[6]

[1]Department of Information and Communication Systems Security, Faculty of Computer Science, V. N. Karazin Kharkiv National University, 61022 Kharkiv, Ukraine
[2]Department of Political Science, Communication and International Relations, University of Macerata, 62100 Macerata, Italy
[3]Department of Information Management and Business Systems, Comenius University Bratislava, 820-05 Bratislava, Slovakia
[4]Department of Law, University of Macerata, 62100 Macerata, Italy
[5]Department of Economics and Law, University of Macerata, 62100 Macerata, Italy
[6]Department of Information Engineering, Marche Polytechnic University, 60131 Ancona, Italy

Corresponding author: Oleksandr Kuznetsov (kuznetsov@karazin.ua)

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme through the Marie Skłodowska-Curie, Project title "TRUST-digital TuRn in EUrope: strengthening relational reliance through Technology," under Grant 101007820.

ABSTRACT As reliance on disruptive applications based on Artificial Intelligence (AI) and Blockchain grows, the need for secure and trustworthy solutions becomes ever more critical. Whereas much research has been conducted on AI and Blockchain, there is a shortage of comprehensive studies examining their integration from a security perspective. Hence, this survey addresses such a gap and provides insights for policymakers, researchers, and practitioners exploiting AI and Blockchain's evolving integration. Specifically, this paper analyzes the potential benefits of the integration of AI and Blockchain as well as the related security concerns, identifying possible mitigation strategies, suggesting regulatory measures, and describing the impact it has on public trust.

INDEX TERMS AI, artificial intelligence, blockchain, distributed ledger technology, security.

I. INTRODUCTION

This research aims to investigate and offer a comprehensive review of the intersection of two transformative technologies - Artificial Intelligence (AI) and Blockchain Technology (BCT) - with a particular focus on the security implications of their integration. Situated within the broader context of the EU-funded TRUST project,[1] this study seeks to contribute to a more nuanced understanding of how trust in the digital transformation of society can be enhanced and fostered.

AI refers to a branch of computer science that involves the development of computer systems capable of performing tasks that normally require human intelligence, such as understanding natural language, recognizing patterns, and making decision [1]. It is a multidisciplinary field that draws from various areas including machine learning, deep learning, natural language processing, and robotics [2].

Blockchain, on the other hand, is a type of distributed ledger technology. It is essentially a decentralized and distributed digital ledger that records transactions across many computers in such a way that the registered transactions cannot be altered retroactively [3]. This technology underpins cryptocurrencies [4] like Bitcoin [5] but is increasingly being used in various other sectors, due to its potential for ensuring transparency, traceability, and security [6].

AI and BCT are being integrating in different applications domain, such as power distribution [7], business and finance [8], supply chain management [9], IoT [10], and many others. The rapid advancement and increasing ubiquity

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Saleem.

[1]https://trust-rise.eu/

of AI and BCT raise significant questions around security, ethics, and trust [11]. Understanding the challenges and opportunities inherent in the integration of these technologies is critical to leveraging their benefits while minimizing potential risks.

This research is particularly timely given the accelerated digital transformation of many aspects of society and the economy in recent years. As reliance on digital technologies grows, the need for secure, trustworthy solutions becomes ever more important. Furthermore, while much research has been conducted on AI and Blockchain individually, as well as about their potential integration in specific domains (such as healthcare, agriculture, and business [12], [13]) and in general [14], [15], there is a dearth of comprehensive studies examining their integration from a security perspective. This survey thus addresses such significant gap in the literature and provides valuable insights for policymakers, researchers, and practitioners navigating the evolving digital landscape. Furthermore, this survey, rather than being based on a systematic literature review i.e., a systematic collection of primary studies to provide a rigorous map of a research area [16], [17], is a targeted literature review, being more narrative, descriptive and rooted on articles selected by the authors from their point of view about the integration of AI and BCT. In this regard, our manuscript uniquely contributes to the literature about the integration of Blockchain and AI as follows:

- It provides a detailed analysis of the integration of Blokchain and AI in distinct fields, namely Neural Networks, Deep Learning, Machine Learning, Natural Language Processing (NLP), providing industrial level examples of successful applications of such integration.
- It presents an in-depth analysis of the impact of such integration from a security perspective, in terms of data, models, and network. As such, it describes the mitigation strategies available in the literature and their application in different domains.
- It depicts the current regulatory environment involving AI and Blockchain and their impact on public trust as derivable from the current literature, highlighting the emerging proactive and inclusive approach based on the need of transparency, accountability, and the engagement of the relevant stakeholders.

The rest of the paper is organized as follows. Section II provides an overview about the principles of Blockchain and AI, including an overview of existing applications. Section III describes the integration of Blockchain and AI, with examples of successful applications in different domains. Section IV focuses on the security issues of Blockchain and AI, proposing mitigation strategies. Section V includes a comprehensive analysis of the implications on data, models, and network security of the integration of Blockchain and AI. Section VI presents the current regulatory environment concerning Blockchain and AI. Section VII the implication of the integration of Blockchain and AI for public trust. Finally, Section VIII draws the conclusions of this review.

II. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE

Blockchain and AI are two groundbreaking technologies that have the potential to radically transform numerous industries and facets of everyday life. As such, a deep understanding of their principles and characteristic is essential because it enables the design and implementation of more effective systems. Therefore, in this section the characteristics of Blockchain (Subsection II-A) and AI (Subsection II-B) are described in details, and an overview of their application is provided (Subsection II-C).

A. PRINCIPLES AND CHARACTERISTICS OF BLOCKCHAIN TECHNOLOGIES

Blockchain technology, a decentralized and distributed digital ledger system, has emerged as a groundbreaking technology due to its unique attributes that ensure data integrity, transparency, and security [5]. Each block in the Blockchain contains a list of transactions which are linked and secured using cryptographic principles. The principal characteristic of Blockchain is its decentralized nature, removing the need for a central authority or intermediary [18]. Transactions are verified by nodes within the network, and once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks. This immutability feature is one of the key security advantages of Blockchain technology.

Blockchain can operate on different levels of access: public Blockchains, where everyone can join the network, and private Blockchains, where only a specific group of participants has access. Additionally, consensus mechanisms, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), are used to validate transactions and produce new blocks [19].

Smart contracts, self-executing contracts with the terms of the agreement directly written into code, represent another notable feature of some Blockchain implementations [20]. These contracts, which are source code written and executed on the Blockcahin, automatically execute transactions following predetermined rules when certain conditions are met [21].

The categorization of Blockchain types for AI applications can be outlined as follows:

- **Public Blockchains**: Public Blockchains are permissionless systems that allow users to download the Blockchain code, make modifications, and utilize it according to their individual requirements [5].
- **Private Blockchains**: Private Blockchains are managed by a single organization. Unlike public Blockchains, they are designed as permissioned systems where users and participants are pre-approved for read/write operations and are always identifiable within the network [22].
- **Consortium Blockchains**: Consortium Blockchains, also known as federated Blockchains, are operated by group of organizations working together [23].
- **Blockchain as a Service (BaaS)**: Cloud service providers are increasingly focusing on Blockchain

technologies due to their widespread adoption and acceptance by governments and large enterprises [24].

When it comes to the Blockchain infrastructure for AI applications, it can be categorized as follows [25]:

- **Linear Blockchain Architectures**: In linear Blockchain architectures, new blocks are appended at the end of the chain. While early decentralized systems operated on single chains, they encountered various issues such as slow scalability and compromised real-time performance of decentralized applications.
- **Nonlinear Blockchain Architectures**: Nonlinear Blockchain architectures are implemented using multichain structures, incorporating parent-child chains, main-side chains, and parallel chains. These architectures offer alternatives to the limitations of linear systems.

While originally created for the digital currency Bitcoin, Blockchain's potential extends far beyond cryptocurrency. It has shown promise in a variety of sectors, including supply chain management [26], [27], healthcare [28], and finance [29]. However, the technology is not without challenges, such as scalability issues, energy consumption concerns, and regulatory uncertainties [30], which require robust solutions for Blockchain to reach its full potential.

B. PRINCIPLES AND CHARACTERISTICS OF ARTIFICIAL INTELLIGENCE

AI, in its most fundamental sense, is a branch of computer science that aims to build systems capable of performing tasks that would require human intelligence, such as image recognition, decision-making, or natural language processing [31]. The concept of AI dates back to the mid-20th century with the first attempts to model the functioning of a single neuron in 1943 [32], and, most important, with the *Dartmouth Summer Research Project on Artificial Intelligence* [33] that gave birth to the AI term, After more than 60 years, the advancements in computing power and, specifically in GPUs [34], data availability, and algorithmic innovation, such as AlexNet [35], have ignited significant breakthroughs in the field.

AI systems can broadly be classified into two categories: narrow (or weak) AI, which is designed to perform a specific task, such as voice recognition; and general (or strong) AI, that can theoretically perform any intellectual task that a human being can do. The latter remains largely theoretical and represents the 'holy grail' of AI research [36].

Machine Learning (ML), a subset of AI, involves the use of statistical methods to enable machines to improve with experience. ML algorithms build a model based on inputs and use that to make predictions or decisions without being explicitly programmed to perform the task. Deep learning, a further subset of ML, involves neural networks with several layers (''deep'' structures) enabling even more complex patterns to be discerned [37], [38].

The presence of multiple Blockchain platforms can greatly aid AI by facilitating the execution of machine learning algorithms and enabling the tracing of data stored on decentralized peer-to-peer (P2P) storage systems [39]. These data sources originate from various smart connected products, including IoT devices, swarm robots, smart cities, buildings, and vehicles [40]. The features and services of the cloud can be also harnessed for off-chain machine learning analytics and intelligent decision making, and for data visualization.

AI presents numerous opportunities across various fields, from healthcare [41] to transportation [42], finance [43], and beyond. However, the characteristics of AI also pose significant challenges in terms of security, privacy, ethics, and governance [44]. These challenges must be robustly addressed to realize the full potential of AI technologies.

C. OVERVIEW OF EXISTING APPLICATIONS OF AI AND BLOCKCHAIN

The applications of both AI and Blockchain have been extensive and transformative across various sectors. AI has seen a surge of applications in numerous fields. In healthcare, AI has been used to predict patient outcomes, assist in diagnosis, and even generate treatment plans [13]. In finance, AI algorithms are utilized for credit scoring, algorithmic trading, and fraud detection [45]. In transportation,AI technologies, including deep learning, reinforcement learning, machine learning and neural networks, drive advancements in autonomous vehicles [46]. AI has even been used in climate modeling, helping scientists understand and predict climate patterns [47].

On the other hand, Blockchain has been primarily associated with financial applications due to the advent of cryptocurrencies. However, its applications extend beyond that sector. In supply chain management, Blockchain can enhance transparency and traceability, ensuring the authenticity of goods [48]. In the energy sector, Blockchain facilitates peer-to-peer energy trading platforms [49]. Blockchain's transparency, security, and decentralization features have also found use in voting systems, creating a more secure and reliable way of conducting elections [50].

The integration of AI and Blockchain is still an emerging field, but several promising applications have been proposed. One such application is using Blockchain technology to make AI models more transparent and explainable, addressing one of the major concerns in AI today [51]. The immutable nature of Blockchain can also be used to ensure the integrity and security of data used in AI models, particularly in sensitive fields like healthcare [52].

III. INTEGRATION OF BLOCKCHAIN TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE

Blockchain has emerged as one of the most highly acclaimed innovations today, garnering significant attention as a versatile technology with wide applicability across various fields. The exponential growth and generation of data from sensing systems, IoT devices, social media, and web applications have played a pivotal role in the advancement of AI. This data can be leveraged by employing diverse machine learning

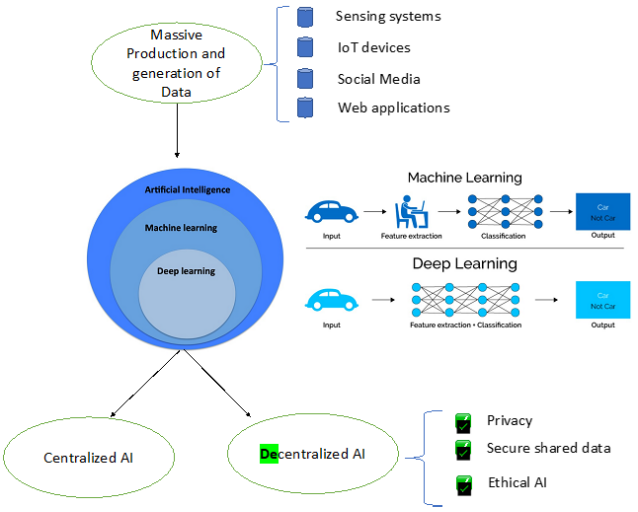

FIGURE 1. Blockchain and AI: centralized and decentralized AI.

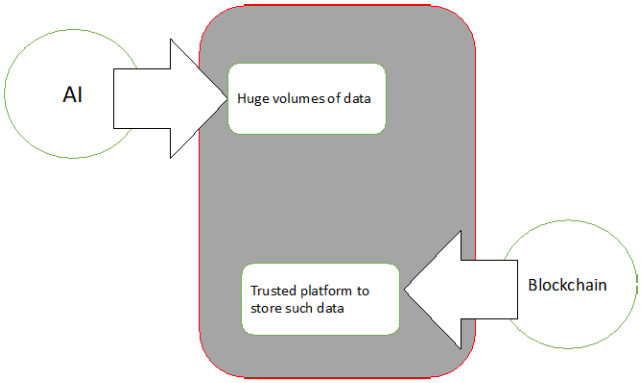

FIGURE 2. AI techniques that utilizes Blockchain: decentralized learning.

and deep learning methodologies. However, the majority of AI methods rely on a centralized model for training, where a set of servers execute specific models using training and validation datasets. Industry giants such as Google, Apple, Facebook, and Amazon handle enormous volumes of data to make informed decisions.

One notable challenge of centralized AI (see Figure 1) is the vulnerability of data to tampering, as it is managed and stored in a centralized manner, making it susceptible to hacking and manipulation. Furthermore, ensuring the data's provenance and authenticity from its sources is not guaranteed. These issues can lead to highly erroneous, risky, and even dangerous AI decision outcomes.

In light of these concerns, the concept of decentralized AI (see Figure 2) has emerged as a recent development, combining AI and Blockchain technologies. Decentralized AI enables processing, analytics, and decision-making based on trusted, digitally signed, and secure shared data that is transacted and stored on the Blockchain. This approach operates in a distributed and decentralized manner, eliminating the need for trusted third parties or intermediaries. Given AI's reliance on vast amounts of data, Blockchain has emerged as a trusted platform for storing such data securely. The feature

TABLE 1. Benefits of leveraging Blockchain for AI.

Blockchain	AI	Integration Benefits
Decentralized	Centralized	Enhanced Data Security
Deterministic	Changing	Improved Trust on Robotic Decisions
Immutable	Probabilistic	Collective Decision Making
Data Integrity	Volatile	Decentralized Intelligence
Attacks Resilient	Data	High Efficiency
	Knowledge	
	Decision-Centric	

of Blockchain smart contracts gives the ability to program the Blockchain to govern transactions among participants involved in decision making or generating and accessing the data.

AI techniques that utilize Blockchain can offer decentralized learning to facilitate a trust and secure sharing of knowledge and decision outcomes across a large number of autonomous agents, which can contribute, coordinate, and vote on further decisions. Smart contract-based autonomous systems and machines can learn and adapt to changes over time, and make trusted and accurate decision outcomes that are verified and validated by all mining nodes of the Blockchain. Such decisions cannot be refuted, and can be traced, tracked and verified by all participating entities.

Some of the significant features of leveraging Blockchain for AI are reported in Table 1. The benefits of Decentralized (Blockchain) AI can be summarized as follows:

- **Enhanced data security**: Blockchain's diskless environment securely stores sensitive and personal data. By digitally signing the data and ensuring secure private keys, AI algorithms can work on trusted and credible data, leading to more reliable decision outcomes.
- **Improved trust in robotic decisions**: Blockchain's decentralized ledger records transactions on a point-by-point basis, fostering acceptance and trust in the decisions made. Recording the decision-making process of AI systems on the Blockchain increases transparency and builds public trust in understanding robotic decisions.
- **Collective decision-making**: Decentralized and distributed decision-making algorithms eliminate the need for a central authority, allowing many robotic applications to benefit from collective decision-making.
- Decentralized intelligence: Combining individual cybersecurity AI agents into a coordinated network provides comprehensive security across underlying networks and resolves scheduling issues.
- **High efficiency**: Integrating AI and Blockchain technologies enables intelligent Decentralized Autonomous Agents (DAOs) for fast and automatic validation of data, value, and asset transfers among stakeholders.

The benefits of Decentralized (Blockchain) AI have significant impacts in different AI applications, including:

- **Autonomic Computing**: Blockchain architecture ensures operational decentralization and records permanent interactions between users, data, applications, devices, and systems, facilitating the development of fully decentralized autonomous systems.

- **Optimization**: Decentralized optimization processes highly relevant data, leading to increased system performance. It is especially useful when multiple strategies with different optimization objectives need to run simultaneously across applications and systems.
- **Planning**: Blockchain-based decentralized AI planning strategies provide more robust plans with permanent tracking and provenance history. Critical and immutable plans can be devised for strategic applications and mission-critical systems.
- **Perception**: Decentralized perception strategies eliminate the need for repeated data collection in AI applications, storing only the footprints of successful perceptions on the Blockchain.
- **Learning**: Decentralized learning models support distributed and autonomous learning systems, achieving fully coordinated local intelligence across all verticals in AI systems. Blockchain ensures secure versioning and maintenance of learning models.
- **Search**: Successful search traces and traversal paths can be permanently and securely stored on the Blockchain, providing optimal solutions for similar operations in the future.
- **Reasoning**: Blockchain-based distributed reasoning strategies facilitate the development of personalized reasoning strategies, particularly during perception, learning, and model deployment.
- **Decentralized Storage**: Blockchain-based decentralized storage infrastructure ensures cryptographically secure storage of personal and sensitive data while addressing scalability and capacity issues.
- **Data Management**: Decentralized data management schemes consider temporal and spatial attributes, deploying them at node levels in the network. Blockchain can store metadata for enhanced security and data provenance.
- **Learning Model Development**: Decentralizing the learning model development process enables the development of resource-efficient models for client applications.
- **Model Deployment**: Smart contract-based model deployment records changes, maintains immutable versioning of models, and enables secure and trustworthy sharing of models among different AI applications.

A. POTENTIAL AND ADVANTAGES OF INTEGRATING AI AND BLOCKCHAIN

The convergence of AI and Blockchain can generate significant synergies, leveraging the strengths of both technologies while mitigating some of their respective weaknesses. This integration could potentially result in systems that are not only more intelligent but also more transparent, secure, and efficient.

- **Transparency and Trust**. Blockchain technology's ability to provide transparency and data immutability could be harnessed to make AI systems more explainable and trustworthy. AI, particularly deep learning, is often criticized for its "black box" nature, meaning that the decision-making process is often opaque and difficult to interpret. By storing data and AI decisions on the Blockchain, it is possible to create a secure and transparent record of the AI's decision-making process, which can be audited and scrutinized.
- **Data Security and Privacy**. Combining AI and Blockchain can also enhance data security and privacy. The decentralized nature of Blockchain ensures that there is no single point of failure, which significantly increases the robustness of the system. Meanwhile, AI can enhance Blockchain security by identifying and mitigating potential threats or malicious activities through pattern recognition and anomaly detection.
- **Efficiency and Scalability**. AI can potentially address one of the main challenges facing Blockchain: the issue of scalability. AI algorithms can be used to optimize the performance of Blockchain networks, improve consensus mechanisms, and expedite the validation process.
- **Monetization of Data**. Integrating AI and Blockchain can facilitate secure data sharing and the creation of decentralized data marketplaces. In this way, individuals and organizations could control and monetize their data, providing data for AI algorithms in a privacy-preserving and secure manner.

In sum, the integration of AI and Blockchain holds great potential for enhancing trust, privacy, efficiency, and monetization of data, as depicted in the Table 2.

By integrating AI and Blockchain, we can benefit from the strengths of both technologies, achieving greater transparency, data security, and operational efficiency, while also opening up new opportunities for data monetization. However, the realization of these benefits is dependent on overcoming several technical and regulatory challenges that are currently associated with these technologies.

B. INTEGRATION OF BLOCKCHAIN WITH DISTINCT FIELD OF AI: OPPORTUNITIES AND CHALLENGES

The integration of Blockchain technology with various AI disciplines promises to revolutionize many aspects of technological applications. Given the increasing significance of both domains, this section delves into the prospects of integrating Blockchain with specific AI fields, including Neural Networks, Deep Learning, Machine Learning, and Natural Language Processing (NLP), and outlines potential challenges that may arise in these areas.

1) NEURAL NETWORKS AND BLOCKCHAIN [53], [54]

- **Opportunities**: By integrating Blockchain with neural networks, we can ensure the provenance and authenticity of data used to train these networks. This is especially useful in sectors where data integrity is paramount, such as healthcare and finance. Blockchain can also facilitate decentralized neural network models where multiple

TABLE 2. The potential of integrating AI and Blockchain to increase trust, privacy, efficiency and data monetization.

Potential Benefit	How it is Achieved	Elaboration
Transparency and Trust	Secure and transparent record of AI's decision-making process	Blockchain provides an immutable record of all transactions, which can make the AI decision-making process auditable. This can increase the trust in AI systems as all stakeholders can verify the decisions made by AI.
Data Security and Privacy	Decentralized system with no single point of failure, AI-enhanced security	Blockchain's decentralized nature ensures data integrity, while AI can help identify and address potential threats. Moreover, Blockchain can ensure that data shared for AI processing is secure, traceable, and unmodifiable, preserving privacy and preventing unauthorized access.
Efficiency and Scalability	AI optimization of Blockchain network performance	AI can potentially improve Blockchain's performance by optimizing data processing, network partitioning, and load balancing. AI could also be used to create more efficient consensus algorithms, thus solving some of the scalability issues currently facing Blockchain technology.
Monetization of Data	Decentralized data marketplaces facilitating secure data sharing	Blockchain technology allows the creation of decentralized data marketplaces, where users can safely store, share, and monetize their data. AI can benefit from these marketplaces as they could provide a large amount of secure and diverse data for AI models.

entities collaborate without centralized control, fostering trust and transparency in the model's predictions.
- **Challenges**: One of the challenges is the computational complexity and latency introduced by Blockchain. Real-time applications of neural networks may be hampered due to the time taken for Blockchain confirmations.

2) DEEP LEARNING AND BLOCKCHAIN [53], [55]
- **Opportunities**: Deep learning models, especially in areas like image recognition, could benefit from Blockchain's tamper-proof nature by verifying the authenticity of input data. Additionally, Blockchain can facilitate the monetization of deep learning models by recording transactions in a transparent and non-repudiable manner.
- **Challenges**: Deep learning models, characterized by their depth, require massive amounts of computational resources. Blockchain, with its consensus mechanisms, could add overheads, making real-time operations a challenge. Moreover, storing intricate deep learning models on-chain might be impractical due to storage constraints.

3) MACHINE LEARNING AND BLOCKCHAIN [54], [55]
- **Opportunities**: Blockchain can promote a secure and transparent environment for machine learning models, where data and algorithms can be shared without the fear of data manipulation. Blockchain can also foster decentralized machine learning, allowing multiple parties to contribute to and train a model, leading to potentially more robust solutions.
- **Challenges**: Scalability is a concern. As machine learning models continue to evolve with more data, the Blockchain must accommodate this iterative process efficiently. Another challenge is ensuring the privacy of data, especially when sensitive data is involved.

4) NATURAL LANGUAGE PROCESSING (NLP) AND BLOCKCHAIN [56], [57]
- **Opportunities**: NLP systems, especially chatbots, could utilize Blockchain to validate the authenticity of information sources, ensuring users receive accurate and untampered information. Furthermore, Blockchain can also play a role in content monetization, where authors can be directly compensated for their contributions.
- **Challenges**: The dynamic nature of languages, characterized by evolving semantics and dialects, may pose synchronization challenges in a Blockchain environment. Moreover, processing language data in real-time, such as in voice assistants, might face latency due to Blockchain's inherent delay in transaction validations.

The potential synergies between Blockchain and various AI fields are abundant, but the integration is not without challenges. It is essential to balance the need for security and trust, afforded by Blockchain, with the requirements for computational efficiency and scalability in AI applications. As technological advancements continue in both domains, we can anticipate more streamlined solutions that seamlessly merge the strengths of both Blockchain and AI, pushing the frontiers of what is achievable in the digital realm.

C. EXAMPLES OF SUCCESSFUL INTEGRATION AND USAGE OF AI AND BLOCKCHAIN
Integrating AI and Blockchain has seen success in various domains, showing potential in enhancing trust, security, and efficiency (see Table 3).

- **Health Care - Electronic Medical Records**. The use of Blockchain to provide proof-of-concept for a patient-controlled electronic medical records system. AI comes into play by processing these medical records to generate insights into patient health, predict diseases, and suggest personalized health recommendations [13]. Benefits: By leveraging Blockchain, system ensures the integrity and security of health data. Through AI,

it provides predictive insights, enhancing patient care. The integration empowers patients with control over their health data while facilitating efficient data sharing among healthcare providers.

- **Supply Chain Management - Food Trust Project (IBM)**. IBM's Food Trust Project is another prominent example where AI and Blockchain are integrated. This solution uses Blockchain to create a transparent, immutable record of food items' journey from farm to store. AI is utilized for pattern detection, predicting food demand, and detecting anomalies that could indicate fraud or contamination.[2] Benefits: Blockchain provides traceability, helping to enhance food safety and reduce waste. AI optimizes the supply chain by predicting demand and detecting anomalies. This results in increased efficiency, reduced costs, and improved consumer trust.
- **Financial Services – Numerai**. Numerai is a hedge fund using Blockchain and AI in a unique way. It uses a Blockchain-based marketplace to crowdsource AI models, which are then used to make investments in financial markets. The data used to build these models is encrypted, ensuring privacy while still allowing model builders to benefit from it.[3] Benefits: Blockchain ensures secure and transparent transactions, while AI is used to make investment decisions. The integration democratizes access to financial markets, leveraging the wisdom of the crowd' for improved decision-making.
- **Education - Sony Global Education**. Sony has developed a system that centralizes management of educational data, including learning history and performance, through Blockchain. This data can be processed by AI for individualized learning plans, predicting learning outcomes, and course optimization.[4] Benefits: Blockchain ensures the integrity and security of educational data, while AI helps in personalizing education, adapting to student needs and improving learning outcomes.
- **IoT - Xage Security**. Xage uses Blockchain to secure IoT devices, creating an immutable security fabric that's tamperproof. The AI component comes into play by autonomously identifying and mitigating potential security threats, managing access control, and enabling predictive maintenance of IoT devices.[5] Benefits: With Blockchain, Xage ensures secure and tamperproof IoT security. The use of AI enables real-time threat detection and prevention, thus improving overall system security and uptime.
- **Energy - Grid+**. Grid+ leverages the Ethereum Blockchain to give consumers direct access to wholesale energy markets, developing a secure Ethereum-enabled gateway and connecting it with a smart energy agent that uses AI algorithms to automate the buying/selling of electricity.[6] Benefits: Blockchain enables peer-to-peer energy transactions, reducing costs and improving efficiency. AI is used to optimize these transactions based on usage data, market conditions, and other factors, potentially saving money for the consumer and stabilizing the grid.
- **Health Care – MedRec**. MedRec, a project from MIT, uses Blockchain for the decentralized management of medical records. When integrated with AI, the system can provide insights to facilitate patient care, including predictive analytics for medical outcomes [58]. Benefits: Blockchain provides a secure, decentralized database for medical records, offering patients ownership and full control of their medical data. AI can generate valuable predictions and insights from these data, enhancing the care provided by health professionals.
- **Agriculture – AgriDigital**. AgriDigital uses Blockchain to provide transparency and traceability in grain supply chains, ensuring farmers get paid accurately and on time. Coupled with AI, it can optimize logistics and distribution, predict market demand, and help detect fraudulent activities.[7] Benefits: Blockchain ensures transparency and traceability, reducing fraud and improving efficiency. AI can enhance these benefits by predicting market trends, optimizing distribution, and further detecting anomalies and fraud.

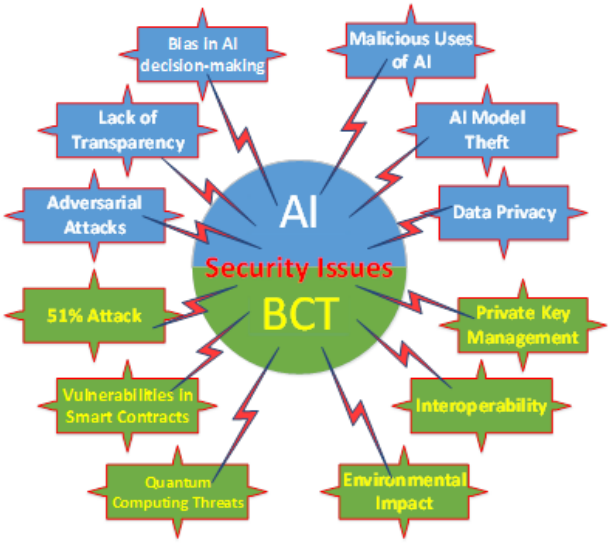

FIGURE 3. Existing security issues associated with Blockchain and AI.

IV. OVERVIEW OF EXISTING SECURITY ISSUES ASSOCIATED WITH BLOCKCHAIN AND AI

While the integration of Blockchain and AI has shown considerable promise, there are still several critical security issues that need to be addressed (see Figure 3).

[2]https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust

[3]https://numer.ai/

[4]https://www.sony.com/en/SonyInfo/sony_ai/Blockchain.html

[5]https://xage.com/

[6]https://whitepaper.io/document/269/grid-whitepaper

[7]https://www.agridigital.io/

TABLE 3. Benefits of using Blockchain and AI for various use cases.

Use Case	Blockchain Use	AI Use	Benefits
Health Care (Electronic Medical Records)	Secure record of patient health data	Process health data for insights and predictions	Enhanced data security, patient empowerment, improved health predictions
Supply Chain Management (Food Trust Project)	Traceability of food items from farm to store	Demand prediction, anomaly detection	Increased transparency, reduced waste, optimized supply chain
Financial Services (Numerai)	Secure and transparent marketplace for AI models	AI models for investment decisions	Democratized access to financial markets, improved investment decisions
Education (Sony Global Education)	Centralized management of educational data	Personalized learning plans, predicting learning outcomes	Integrity and security of educational data, personalized education
IoT (Xage Security)	Secure and tamperproof IoT security	Real-time threat detection and prevention	Secure and tamperproof IoT security, improved overall system security
Energy (Grid+)	Peer-to-peer energy transactions	Optimizing transactions based on usage data, market conditions	Reduced costs, improved efficiency, potential savings for consumer
Health Care (MedRec)	Decentralized management of medical records	Generate insights, predictive analytics for medical outcomes	Secure management of medical records, improved patient care
Agriculture (AgriDigital)	Transparency and traceability in grain supply chains	Predict market demand, detect fraudulent activities	Transparency and traceability, reduced fraud, optimized distribution

Concerning AI, the security issues are:

- AI algorithms are only as good as the data they are trained on, which can lead to security risks. Adversarial attacks are one such risk, where malicious actors manipulate input data to deceive AI models and produce incorrect outputs.
- There is also the issue of privacy. As AI systems often require vast amounts of data, it raises concerns about data protection, particularly when dealing with sensitive information like financial or health data.
- Furthermore, AI systems can be opaque, often referred to as "black boxes". If these systems are used in critical decision-making processes, this lack of transparency can lead to trust issues and potential misuse.
- Bias in AI decision-making: AI systems learn from the data they are fed. If this data is biased, the AI can inherit and even amplify these biases, leading to skewed or unfair decisions.
- AI Model Theft: As AI models become more valuable, there are growing concerns about the theft of AI models, particularly in cloud-based machine learning solutions.
- Malicious Uses of AI: AI technology can also be used maliciously. For instance, deepfakes can manipulate audio and video to make it appear as if someone said or did something they did not.

On the other hand, concerning Blockchain, the security issues are:

- Blockchain technology, while considered secure, is not immune to threats. One of the major concerns is the 51% attack, where if a single entity gains control of the majority of the network's mining hashrate, they can disrupt the functioning of the Blockchain, including double-spending and blocking transactions.
- Private key management is another security concern. If a user's private key is lost or stolen, the user can lose access to their Blockchain assets, and if the key is stolen, the assets can be misused.
- Smart contracts, despite their benefits, introduce additional security issues. They can contain vulnerabilities and bugs, which if exploited, can lead to significant financial losses, as evidenced by several high-profile incidents.
- Interoperability: Ensuring different Blockchain systems can work together securely is a significant challenge, as it could potentially open up new attack vectors.
- Quantum Computing Threats: Quantum computers could potentially break the cryptographic algorithms that keep Blockchain secure, thus posing a long-term security risk.
- Environmental Impact: While not a security concern in the traditional sense, the environmental impact of Blockchain, particularly proof-of-work Blockchains, is a significant issue due to their high energy consumption.

TABLE 4. Overview of existing security issues associated with AI.

Security Issue	Elaboration
Adversarial Attacks	Input data can be manipulated to deceive AI models
Data Privacy	AI often requires large amounts of data, raising concerns about data protection
Lack of Transparency	The decision-making process of AI systems can be opaque and difficult to interpret
Bias in AI decision-making	Biased data can lead to skewed or unfair AI decisions
AI Model Theft	Theft of valuable AI models, particularly in cloud-based machine learning solutions
Malicious Uses of AI	Misuse of AI technology for malicious purposes, such as deepfakes

This information is summarized and conceptualized in the Tables 4 and 5.

A. PROPOSED STRATEGIES FOR MITIGATION OR MINIMIZATION OF SECURITY ISSUES

Given the significance of the security issues associated with AI and Blockchain, developing effective strategies for mitigation or minimization is crucial (see Figure 4).

TABLE 5. Overview of existing security issues associated with Blockchain.

Security Issue	Elaboration
51% Attack	If a single entity gains control of the majority of the network's mining hashrate, they can disrupt the functioning of the Blockchain
Private Key Management	Loss or theft of a private key can lead to loss or misuse of Blockchain assets
Vulnerabilities in Smart Contracts	Smart contracts can contain bugs or vulnerabilities, which if exploited can lead to significant losses
Interoperability	Ensuring secure interaction between different Blockchain systems is a significant challenge
Quantum Computing Threats	Quantum computers could potentially break the cryptographic algorithms that secure Blockchain
Environmental Impact	High energy consumption of some Blockchains, particularly proof-of-work Blockchains

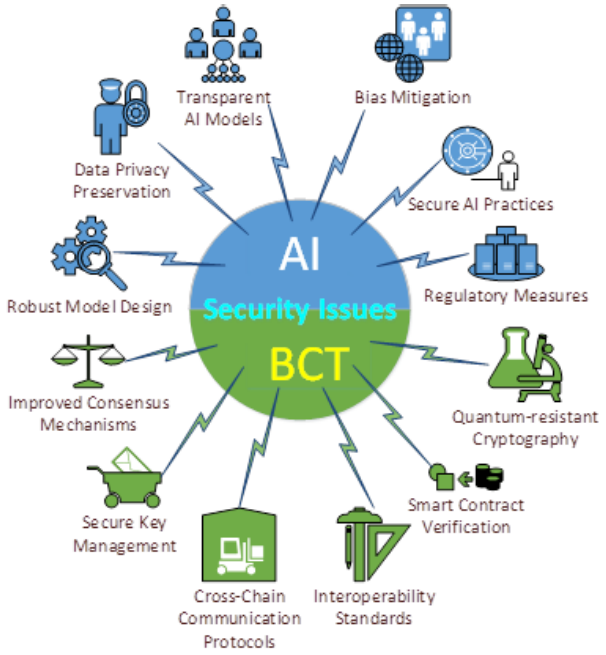

FIGURE 4. The mitigation needed to address the risks associated with Blockchain and AI.

Concerning AI, the following mitigation strategies can be applied:

- **Robust Model Design**: Building AI models that can recognize and resist adversarial attacks can help increase system robustness. Incorporating adversarial training, where the model is trained with adversarial examples, can improve its ability to resist such attacks [59], [60].
- **Data Privacy Preservation**: Using techniques such as differential privacy, which adds noise to the data, or federated learning, which leaves the data on the original device while the model learns from it, can help preserve privacy while still benefiting from AI [60], [61].
- **Transparent AI Models**: Efforts should be made to design more interpretable and explainable AI models, which can help increase trust and reveal biases [62], [63].
- **Bias Mitigation**: To prevent biased decision-making, efforts should be taken to ensure the data used to train AI models is representative and free from bias. Bias detection and mitigation techniques can be applied to both the data and the AI model [64], [65].
- **Secure AI Practices**: To prevent AI model theft, secure multi-party computation and homomorphic encryption techniques can be used to train models on encrypted data, providing the benefits of AI without exposing raw data [60], [66].
- **Regulatory Measures**: Implementing strict regulations can discourage malicious uses of AI and hold perpetrators accountable [67].

Concerning Blockchain, the following mitigation strategies can be applied:

- **Improved Consensus Mechanisms**: Alternatives to the traditional proof-of-work mechanism, such as proof-of-stake or proof-of-authority, can provide similar security while being less susceptible to 51% attacks and reducing environmental impact [68].
- **Secure Key Management**: Hardware wallets, multi-signature wallets, or key recovery services can help users secure and recover their private keys [68].
- **Smart Contract Verification**: Automated verification tools can be used to check smart contracts for known vulnerabilities before deployment [69], [70].
- **Interoperability Standards**: Standardization of protocols and interfaces can ensure secure and seamless interaction between different Blockchain systems [69], [70].
- **Quantum-resistant Cryptography**: The adoption of quantum-resistant cryptographic algorithms can prepare Blockchain technology for the advent of quantum computers.
- **Cross-Chain Communication Protocols**: Cross-chain communication protocols such as Polkadot or Cosmos can allow different Blockchains to interoperate, enabling secure cross-chain transactions [69], [70].

In addressing the issues of AI and Blockchain, the strategies mentioned involve a combination of technical solutions, such as the design of robust models or the adoption of quantum-resistant cryptography [71], and structural solutions [69], [70], such as the creation of interoperability standards or the implementation of regulations. For instance, the issue of adversarial attacks in AI can be addressed technically by designing more robust models [60]. On a structural level, regulations could be implemented to discourage such attacks. Similarly, for Blockchain, the technical problem of 51% attacks could be mitigated by using different consensus mechanisms, while the structural issue of interoperability could be addressed by standardizing protocols and interfaces [69], [70].

It is also worth noting that many of these strategies are not standalone but interrelated. For instance, improving data privacy preservation in AI could also help reduce

bias by allowing for more diverse datasets to be used in a privacy-preserving manner.

It is essential to acknowledge that while the strategies outlined are based on current research and best practices, the rapidly evolving nature of both AI and Blockchain technologies means that new challenges and solutions can emerge. It is always crucial for researchers, practitioners, and policymakers to stay updated with the latest developments and ensure that any strategies or recommendations are grounded in empirical evidence and real-world applicability. Furthermore, collaboration between academia, industry, and regulatory bodies can foster a more comprehensive understanding and robust solutions to the security challenges posed by these technologies.

B. ANALYZING THE IMPACT OF INTEGRATION ON SECURITY IN VARIOUS USE CASE SCENARIOS

The integration of Blockchain and AI can have profound implications for security across a variety of use case scenarios:

- **Healthcare Data Management** [51], [72], [73]: In healthcare, the integration can enhance data privacy and security. Blockchain can provide an immutable, transparent record of patient data, while AI can analyze this data to provide insights. By integrating the two, we could assure the integrity of the data being analyzed and the privacy of patients' sensitive information.
- **Supply Chain Transparency** [74], [75], [76]: The combination of Blockchain and AI could enhance the transparency and efficiency of supply chains. Blockchain can provide an immutable record of goods as they move through the supply chain, while AI can analyze these data to optimize logistics and detect anomalies.
- **Financial Fraud Detection** [77], [78]: Blockchain can provide a secure, tamper-proof system for financial transactions, while AI can be used to detect anomalous transactions that might indicate fraudulent activity. The integration of both could significantly enhance the ability to detect and prevent fraud.
- **Smart Contract Management** [78], [79]: AI can be utilized to automatically manage and execute smart contracts based on predefined conditions. The integration with Blockchain ensures the secure and transparent execution of these contracts, reducing the risk of disputes.
- **Personalized Education** [80], [81]: AI can provide personalized education solutions based on individual student learning patterns. With Blockchain ensuring the integrity and ownership of educational records, the combined use could revolutionize the educational system by providing secure, personalized learning.
- **Energy Grid Management** [76], [82]: AI can optimize energy grid management by predicting demand and optimizing distribution. By integrating with Blockchain for secure, transparent energy usage recording, this could significantly enhance the efficiency of energy grids.
- **Internet of Things (IoT)** [75], [83]: The vast number of devices in IoT networks poses significant security challenges. AI, integrated with Blockchain, could enhance security by identifying and responding to threats in real-time, while also handling device-to-device transactions securely.
- **Decentralized Autonomous Organizations (DAOs)** [84]: DAOs operate with smart contracts on a Blockchain. The addition of AI could lead to more efficient decision-making processes within DAOs, while maintaining the security and transparency of operations.
- **Content Creation and Ownership** [85], [86]: AI can create content, such as articles or artworks, and Blockchain can be used to establish original ownership and creation, providing a secure way for AI to not only generate but also protect content.
- **Digital Identity Verification** [87]: AI, with its capability to analyze patterns and behaviors, can be utilized for digital identity verification. Integration with Blockchain would provide a secure, immutable record of digital identities, reducing the risk of identity theft.

In these scenarios, the integration of AI and Blockchain has the potential to address major security concerns. By leveraging the immutability and transparency of Blockchain and the analytic capabilities of AI, a more secure, efficient, and reliable digital ecosystem could be created. However, the implementation of these technologies must be carefully managed to avoid introducing new vulnerabilities and to ensure that the benefits are realized across all sectors of society.

In conclusion, while the presented scenarios are based on current knowledge and understanding of AI and Blockchain, it is essential to approach the integration of these technologies with caution, ensuring that their combined use is both beneficial and ethical. While we acknowledge the need for empirical validation in many proposed scenarios, our conclusions are drawn from a synthesis of current knowledge, expert insights, and the anticipated trajectory of technological advancements. The extensive body of literature consulted for this work not only reinforces our claims but also underscores the potential and challenges of integrating AI and Blockchain. As the field matures, we anticipate that many of our projections will find empirical grounding, further solidifying the importance of this interdisciplinary exploration.

C. ADDITIONAL CONSIDERATIONS IN AI AND BLOCKCHAIN INTEGRATION

This subsection delves deeper into other significant aspects of integrating AI and Blockchain beyond the realm of security. Three vital areas warranting exploration include the adaptability of costs in Blockchain-based solutions, data standardization, and bias concerns.

1) COST ADAPTABILITY FOR BLOCKCHAIN-BASED SOLUTIONS

Blockchain, being a distributed ledger technology, brings forth undeniable advantages such as enhanced transparency

and reduced transactional fraud. However, the adaptability of costs in Blockchain implementations, especially in AI contexts, remains a prominent concern [88], [89].

- **Energy Consumption**: Blockchain, especially proof-of-work-based systems like Bitcoin, is notoriously energy-intensive. Integrating such systems with AI models, which themselves might be resource-hungry, could escalate operational costs.
- **Scalability Trade-offs**: Increasing the capacity of Blockchain systems often comes at the cost of decreased security or decentralization. This trade-off, known as the scalability trilemma, presents challenges in maintaining cost-effectiveness while ensuring system efficiency.
- **Solutions**: Layer 2 solutions, like the Lightning Network or Plasma, offer promise in mitigating scalability and cost concerns. Moreover, transitioning to proof-of-stake or hybrid models can curtail energy expenditures.

2) DATA STANDARDIZATION IN AI-BLOCKCHAIN PARADIGMS

The harmonization of data structures and formats becomes indispensable when blending AI and Blockchain [90].

- **Heterogeneous Data Sources**: AI often demands data from varied sources, each with its unique format. Integrating such diverse data into a standardized Blockchain system can be challenging.
- **Smart Contract Constraints**: The rigid nature of smart contracts can pose limitations in handling dynamic AI data inputs.
- **Solutions**: Developing middleware that acts as an interface between AI data sources and Blockchain can help in seamless integration. Additionally, flexible smart contract templates tailored for AI can be designed to overcome rigidity.

3) BIAS CONCERNS IN AI AND BLOCKCHAIN CONTEXTS

While Blockchain offers a transparent data ledger, AI models can inadvertently introduce or perpetuate biases, leading to skewed or unfair outcomes [91], [92].

- **Data Imbalances**: AI models are as good as the data they are trained on. If historical data on a Blockchain is biased, AI will produce biased predictions.
- **Model Transparency**: The integration of AI and Blockchain requires an emphasis on model transparency to ensure that biases, once identified, can be addressed.
- **Solutions**: Techniques like Differential Privacy can ensure data privacy while mitigating biases. Further, incorporating fairness algorithms in AI models can ensure equitable outcomes. Using Blockchain's immutable nature, stakeholders can also trace and correct biased data sources.

In conclusion, while integrating AI and Blockchain opens a plethora of opportunities, careful consideration of cost adaptability, data standardization, and biases is crucial to reap the full benefits of this synergy. The highlighted challenges, coupled with the solutions, offer a roadmap for researchers and practitioners venturing into this multidisciplinary domain.

V. COMPREHENSIVE ANALYSIS OF DATA, MODEL, AND NETWORK SECURITY IN AI AND BLOCKCHAIN INTEGRATION

Given the transformative potentials of both AI and Blockchain technologies, ensuring their secure integration is paramount. This encompasses challenges related to data encryption, ensuring strict access controls, and preserving anonymity, alongside model-centric issues of encryption, watermarking, and versioning [60]. Furthermore, the holistic security canvas extends to network considerations, such as robust firewall mechanisms, sophisticated intrusion detection systems, and the adoption of secure communication protocols. This section delves deeply into these facets, offering both descriptive insights and prescriptive measures.

A. DATA SECURITY IN AI-BLOCKCHAIN ECOSYSTEMS

In the intricate weave of AI and Blockchain technologies, the prominence of data cannot be understated. Data serves as the lifeblood, driving AI models to achieve unprecedented accuracies and facilitating the decentralized, trustless operations of Blockchain. As such, its security emerges as a focal point of concern and exploration [55], [72]. This subsection aims to shed light on the primary considerations surrounding data security, examining encryption, access controls, and data anonymization techniques that reinforce the fortifications of the AI-Blockchain amalgamation.

- **Data Encryption**: Encryption, the act of converting information into an unreadable format except to those possessing a secret key, remains a cornerstone of data security. Within the AI-Blockchain ecosystem, the stakes are raised due to the sensitive nature of data and the high-value transactions often taking place. While Blockchains like Bitcoin and Ethereum employ cryptographic algorithms to secure transactions, when integrated with AI, there's a necessity for layered encryption methodologies to safeguard both input data and output results. Advanced encryption techniques, such as Homomorphic encryption, allow computations on encrypted data without decrypting it first, making it an enticing prospect for preserving data privacy in AI operations on Blockchains.
- **Access Controls**: The principle of access control revolves around ensuring only authenticated and authorized entities can access specific data. With AI models requiring vast amounts of data for training and Blockchain often housing transactional data, establishing stringent access control mechanisms is pivotal. Role-based access control (RBAC) and attribute-based access control (ABAC) emerge as prevalent strategies. While RBAC restricts access based on a user's role within an organization, ABAC does so based on attributes such as location, time, or type of transaction.

When coupled, these techniques can fortify data repositories against unauthorized access, leaks, or breaches.

- **Data Anonymization**: In an era underscored by privacy concerns, ensuring data anonymity is not just a technical challenge but a moral imperative. Data anonymization techniques aim to modify data sets in a manner that individual data points cannot be linked back to the originating source. Techniques like differential privacy inject calculated amounts of noise into data, ensuring utility remains while shielding individual identities. Within the Blockchain context, this aligns with the principle of pseudonymity where transactions can be seen, but linking them to an individual's identity is obfuscated. Pairing AI's need for vast datasets with Blockchain's transparent nature necessitates the rigorous implementation of such anonymization methodologies.

In summation, while the union of AI and Blockchain heralds vast potentials, it is contingent upon a robust security framework centered around data. As technology evolves, ensuring the sanctity of data through encryption, regulated access, and stringent anonymization protocols will remain at the forefront of research and implementation.

B. MODEL SECURITY CONSIDERATIONS

In the intricate synergy of artificial intelligence and Blockchain technologies, while data stands as a foundational pillar, the AI models themselves become integral assets. These models, often the product of significant investment and research, encapsulate patterns and insights extracted from the data. Consequently, they become targets for malicious actors, emphasizing the need for rigorous model security measures [55], [60], [66]. This subsection delves into paramount areas of concern: model encryption, watermarking, and version control, aiming to present a holistic perspective on ensuring the integrity and confidentiality of AI models in a Blockchain environment.

- **Model Encryption**: AI models, especially deep learning ones, have grown in complexity, sometimes encapsulating millions of parameters. Protecting these models from unauthorized access or theft requires encryption mechanisms tailored to their unique structure. Homomorphic encryption, previously discussed in the context of data security, also has relevance here. By permitting computations on encrypted models without necessitating decryption, it offers a path to deploy AI models on public Blockchains securely. Further, encrypted model parameters ensure that even if a malicious actor gains access, the underlying model remains indecipherable without the appropriate decryption key.
- **Model Watermarking**: Beyond outright theft, there is a risk of unauthorized replication or misuse of AI models. Watermarking emerges as a solution, embedding a unique identifier or pattern into the model, much like watermarks in physical currency or documents. This embedded signature allows for the assertion of ownership and can act as a deterrent against unauthorized propagation. In the context of Blockchain, this watermark can be stored as an immutable record, providing undeniable evidence of original ownership.
- **Model Version Control**: AI models, by their nature, are continually evolving. As more data becomes available, or as the environment they operate in changes, models undergo iterations. In such a dynamic landscape, version control is not a luxury but a necessity. It ensures that at any given point, stakeholders can identify which version of a model is in operation, understand its provenance, and roll back to previous versions if needed. When integrated with Blockchain, every iteration of a model can be immutably recorded, providing a transparent history of model evolution and modifications.

To encapsulate, the security of AI models transcends mere protection from theft. It envelops considerations of integrity, traceability, and accountability. As AI and Blockchain continue to converge, creating mechanisms that instill confidence in the robustness of model security will be of paramount importance, underpinning the broader acceptance and adoption of these intertwined technologies.

C. NETWORK SECURITY PROTOCOLS

The confluence of artificial intelligence and Blockchain, while presenting vast opportunities, also exposes the integrated systems to potential vulnerabilities at the network layer. This stems from the extensive connectivity, decentralized nature, and the data-intensive tasks the combined AI-Blockchain networks typically handle. A fortified network ensures that both data in transit and control commands traverse in a manner that is not just efficient but also secure against adversarial attacks. This subsection delves into core aspects of network security, including firewalls, intrusion detection systems, and secure communication protocols, providing insights into their pivotal role in safeguarding the AI-Blockchain ecosystems [54], [72].

- **Firewalls**: Firewalls serve as the first line of defense in any network, regulating inbound and outbound traffic based on predetermined security rules. In an AI-Blockchain environment, they become even more critical given the decentralized nodes which can be geographically dispersed. Dynamic and stateful packet inspection, coupled with rule-based access controls, ensures that only legitimate packets are allowed, while potentially harmful or unauthorized data packets are blocked.
- **Intrusion Detection Systems (IDS)**: With the intricate nature of AI-Blockchain networks, merely blocking suspicious traffic might not suffice. It is crucial to actively monitor and detect unusual patterns or behaviors within the network. Intrusion Detection Systems provide real-time surveillance of the network activities, leveraging AI algorithms to discern anomalies from regular patterns. When a potential threat is identified, IDS can trigger alerts or integrate with other systems to take protective actions. Blockchain's

immutable ledger can further augment IDS by providing a tamper-evident record of all network transactions, enhancing traceability and post-incident analysis.

- **Secure Communication Protocols**: The essence of any AI-Blockchain system rests on the seamless and secure exchange of information between nodes. As such, adopting secure communication protocols becomes indispensable. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are foundational in this regard. They provide encrypted channels for data exchange, ensuring confidentiality and integrity. Furthermore, in a decentralized AI-Blockchain scenario, protocols such as the Whisper protocol in Ethereum can be used to enable secure peer-to-peer communication, ensuring that data and control commands are shared without eavesdropping.

In summation, as AI and Blockchain technologies continue their march towards deeper integration, the fabric of their interconnectivity - the network - demands steadfast security measures. Implementing rigorous network security protocols ensures not only the resilience of the system against adversarial attacks but also underpins the trust and reliability users place in this integrated technological paradigm.

VI. REGULATORY ASPECTS OF BLOCKCHAIN AND AI INTEGRATION

The current regulatory environment for AI and Blockchain is complex and varied across jurisdictions. The dynamic and disruptive nature of these technologies, combined with their global reach, makes their regulation a challenging task.

For AI, regulations typically focus on data protection and privacy, as well as the ethical use of AI. The European Union's General Data Protection Regulation (GDPR) is a key example, setting strict requirements for data protection and providing citizens with significant control over their personal data [93]. In terms of AI ethics, the European Commission's Ethics Guidelines for Trustworthy AI set out key principles for the development and use of AI [94]. The European Commission is also working on the proposal for an EU regulatory framework on AI, the so called AI act [95].

As for Blockchain, regulatory focus often lies in areas like cryptocurrency regulation, smart contracts, and initial coin offerings (ICOs) [96]. Given Blockchain's association with cryptocurrencies, many jurisdictions have established regulations to combat issues like money laundering and fraud [97]. At the same time, regulations also seek to address the legal status of smart contractss [98] and the governance of ICO [99].

Other regions of the World tackle the regulations differently. For example, the United States tends to apply a more decentralized and sector-specific regulatory framework for AI, with an industry-specific rationale [100]. In Blockchain regulation, the EU's comprehensive stance is distinct from the U.S.'s focus on financial aspects, as Money Services Business [101]. Differently, on AI China tries to integrate regulations at the national, provincial, and local levels, focusing on maintaining state authority and cultural values [102]. Concerning Blockchain, China acted differently from the US and EU, banning cryptocurrencies [103]. Therefore, this divergence highlights the challenges in establishing a cohesive global regulatory framework for emerging technologies.

The integration of AI and Blockchain presents a new array of legal challenges. Firstly, while Blockchain provides a secure and immutable ledger, it also raises significant data protection concerns, particularly in relation to the ''right to be forgotten'' enshrined in regulations like the GDPR. Another potential issue is the legal status of decisions made by AI or automated processes via smart contracts on a Blockchain. This could raise questions about liability, particularly in scenarios where decisions have significant consequences. Additionally, as AI algorithms can process large amounts of data, including personal data, integrating AI with Blockchain could potentially conflict with data minimization principles in data protection laws.

Developing an effective regulatory environment requires a delicate balance. On one hand, it is important to foster innovation and exploit the benefits of AI and Blockchain integration. On the other, there is a clear need to address the aforementioned legal challenges and ensure the secure and ethical use of these technologies. A multi-faceted approach could be beneficial:

- **Regulatory Flexibility**: Given the rapid pace of technological change, regulations need to be flexible to adapt to new developments. This could involve implementing principle-based regulations, rather than prescriptive ones, allowing for adaptation to different technologies and use cases.
- **Technological Neutrality**: Regulations should aim to be technology-neutral, focusing on the activity or outcome rather than the specific technology used. This would ensure that all technologies are subject to the same rules, promoting fairness and competition.
- **Global Cooperation**: Given the global nature of these technologies, international cooperation is essential. Regulators should work together to develop harmonized standards and avoid regulatory fragmentation.
- **Stakeholder Engagement**: Regulators should engage with a broad range of stakeholders, including industry, academia, and civil society, to ensure regulations are informed by a wide range of perspectives and expertise.
- **Promoting Transparency and Accountability**: It is crucial to ensure that both AI and BCT are deployed in a manner that is transparent and accountable. This might involve creating standards or certifications for transparency in AI, or ensuring clear governance structures for Blockchain networks.

In summary, the development of an effective regulatory environment for the integration of AI and Blockchain requires a careful and considered approach. With the right regulations in place, these technologies can be harnessed in a manner that maximizes their benefits while minimizing their risks.

VII. IMPACT ON PUBLIC TRUST AND RESEARCH

The integration of AI and Blockchain carries significant implications for public trust. On one hand, the enhanced security and transparency offered by Blockchain, combined with the efficiency of AI, can contribute to increased trust [104]. However, issues related to privacy, accountability, and the potential misuse of these technologies can conversely erode public trust [105]. Moreover, public understanding and perceptions of these technologies play a significant role. Misunderstandings or misconceptions about AI [106] and Blockchain [107] can fuel fear and skepticism, while greater understanding and transparency can foster trust.

The integration of AI and Blockchain in public sectors has the potential to impact service delivery and transparency. For instance, in healthcare, Blockchain-enabled AI systems are being deployed for secure patient data management and personalized treatment plans, enhancing both privacy and efficacy [108]. In finance, these technologies facilitate fraud detection and risk assessment, leveraging AI's predictive capabilities with Blockchain's immutable record-keeping [109]. Additionally, governments are exploring their use in voting systems, where AI assists in voter registration and fraud detection, while Blockchain ensures secure and transparent election processes [110].

Thus, the integration of AI and Blockchain can fundamentally transform interactions among people, businesses, and authorities by creating new forms of relational reliance. In peer-to-peer interactions, Blockchain's transparency and immutability can foster trust by ensuring accountability, while AI can facilitate these interactions more efficiently [111]. For businesses, this can enhance customer trust and enable more secure and efficient operations [112]. Authorities can leverage these technologies to offer more secure, transparent, and responsive public services, thereby enhancing public trust.

However, it is crucial to ensure this new form of relational reliance does not lead to over-reliance or misuse. It is important to foster an environment where these technologies are used to supplement, rather than supplant, traditional forms of trust-building.

Building public trust in AI and Blockchain requires a multi-faceted approach:

- **Transparency**: Ensuring transparency in the use of AI and Blockchain can foster trust. This could involve being clear about how these technologies are used, the data they process, and the implications for individuals.
- **Education and Awareness**: Public education initiatives can demystify these technologies, correct misconceptions, and promote informed public discourse.
- **Regulation**: Effective and fair regulation can foster trust by ensuring that these technologies are used responsibly and that any misuse is appropriately addressed.
- **Accountability**: Establishing clear accountability structures can help ensure that any negative impacts or misuse of AI and Blockchain are swiftly and effectively addressed.
- **Engagement**: Engaging with stakeholders, including the public, in decision-making processes regarding the use of AI and Blockchain can help ensure that diverse perspectives and concerns are taken into account.

In summary, fostering trust in AI and Blockchain requires a proactive and inclusive approach. Through transparency, education, regulation, accountability, and engagement, we can ensure that the integration of these technologies is seen not as a cause for concern, but as an opportunity for greater security, efficiency, and innovation.

VIII. CONCLUSION

This research aimed to investigate the integration of AI and BCT, with a particular focus on security aspects. We found that while these technologies have the potential to significantly enhance security, efficiency, and transparency across a range of sectors, they also present new challenges and risks. In the field of AI, issues such as adversarial attacks, data privacy, transparency, and bias were identified, while in the realm of Blockchain, concerns around consensus mechanisms, key management, smart contract vulnerabilities, and quantum resistance were highlighted. The integration of these technologies amplifies both their advantages and their challenges, creating a complex landscape that needs to be navigated carefully.

In response to these challenges, we propose a range of strategies for mitigation, including robust model design, improved consensus mechanisms, and regulatory measures. Moreover, we suggest that fostering a regulatory environment that is flexible, technology-neutral, globally cooperative, and engaging with stakeholders is essential to facilitating secure and ethical integration of AI and Blockchain.

ACKNOWLEDGMENT

This article reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 101007820-TRUST. This publication reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] F. J. Kurfess, "Artificial intelligence," in *Encyclopedia of Physical Science and Technology*, 3rd ed., R. A. Meyers, Ed. New York, NY, USA: Academic, 2003, pp. 609–629.
[2] Y. K. Dwivedi et al., "Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *Int. J. Inf. Manag.*, vol. 57, Apr. 2021, Art. no. 101994.
[3] J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, and S. Green, "Blockchain as a disruptive technology for business: A systematic review," *Int. J. Inf. Manage.*, vol. 51, Apr. 2020, Art. no. 102029.
[4] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.

[5] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jul. 24, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] J. A. Jaoude and R. George Saade, "Blockchain applications—Usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.

[7] A. A. Khan, A. A. Laghari, M. Rashid, H. Li, A. R. Javed, and T. R. Gadekallu, "Artificial intelligence and blockchain technology for secure smart grid and power distribution automation: A state-of-the-art review," *Sustain. Energy Technol. Assessments*, vol. 57, Jun. 2023, Art. no. 103282.

[8] S. Kumar, W. M. Lim, U. Sivarajah, and J. Kaur, "Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis," *Inf. Syst. Frontiers*, vol. 25, no. 2, pp. 871–896, 2023.

[9] N. Tsolakis, R. Schumacher, M. Dora, and M. Kumar, "Artificial intelligence and blockchain implementation in supply chains: A pathway to sustainability and data monetisation?" *Ann. Oper. Res.*, vol. 327, no. 1, pp. 157–210, Aug. 2023.

[10] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.-W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," *J. Cloud Comput.*, vol. 12, no. 1, p. 38, Mar. 2023.

[11] E. Bertino, A. Kundu, and Z. Sura, "Data transparency with blockchain and AI ethics," *J. Data Inf. Qual.*, vol. 11, no. 4, pp. 1–8, Dec. 2019.

[12] S. Vyas, M. Shabaz, P. Pandit, L. R. Parvathy, and I. Ofori, "Integration of artificial intelligence and blockchain technology in healthcare and agriculture," *J. Food Qual.*, vol. 2022, pp. 1–11, May 2022.

[13] R. Kumar, D. Singh, K. Srinivasan, and Y.-C. Hu, "AI-powered blockchain technology for public health: A contemporary review, open challenges, and future research directions," *Healthcare*, vol. 11, no. 1, p. 81, Dec. 2022.

[14] T. N. Dinh and M. T. Thai, "AI and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, Sep. 2018.

[15] A. Ekramifard, H. Amintoosi, A. H. Seno, A. Dehghantanha, and R. M. Parizi, *A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence*. Cham, Switzerland: Springer, 2020, pp. 147–160.

[16] B. Kitchenham, *Procedures for Performing Systematic Reviews*, vol. 33. Keele, U.K.: Keele Univ., 2004, pp. 1–26.

[17] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[18] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: From theory to IoT applications and beyond," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[19] B. Gan, Q. Wu, X. Li, and Y. Zhou, "Classification of blockchain consensus mechanisms based on PBFT algorithm," in *Proc. Int. Conf. Comput. Eng. Appl. (ICCEA)*, Jun. 2021, pp. 26–29.

[20] M. Di Pierro, "What is the blockchain?" *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 92–95, 2017.

[21] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," *Information*, vol. 14, no. 2, p. 117, Feb. 2023.

[22] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on private blockchain consensus algorithms," in *Proc. 1st Int. Conf. Innov. Inf. Commun. Technol. (ICIICT)*, Apr. 2019, pp. 1–6.

[23] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. Hamida, "Consortium blockchains: Overview, Applications and challenges," *Int. J. Adv. Telecommun.*, vol. 11, pp. 51–64, Sep. 2018.

[24] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436.

[25] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[26] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti, "A review on blockchain applications in the agri-food sector," *J. Sci. Food Agricult.*, vol. 99, no. 14, pp. 6129–6138, Nov. 2019.

[27] D. Dujak and D. Sajter, *Blockchain Applications in Supply Chain*. Cham, Switzerland: Springer, 2019, pp. 21–46.

[28] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Netw.*, vol. 2, pp. 130–139, Jan. 2021.

[29] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of blockchain technology applications for financial services," *BenchCouncil Trans. Benchmarks, Standards Eval.*, vol. 2, no. 3, Jul. 2022, Art. no. 100073.

[30] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017.

[31] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. London, U.K.: Pearson, 2020.

[32] N. Muthukrishnan, F. Maleki, K. Ovens, C. Reinhold, B. Forghani, and R. Forghani, "Brief history of artificial intelligence," *Neuroimaging Clinics*, vol. 30, no. 4, pp. 393–399, 2020.

[33] J. McCarthy, M. L. Minsky, N. Rochester, and C. E. Shannon, "A proposal for the Dartmouth summer research project on artificial intelligence, August 31, 1955," *AI Mag.*, vol. 27, no. 4, pp. 1–13, 2006.

[34] D. Steinkraus, I. Buck, and P. Y. Simard, "Using GPUs for machine learning algorithms," in *Proc. 8th Int. Conf. Document Anal. Recognit. (ICDAR)*, Aug. 2005, pp. 1115–1120.

[35] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, May 2017, doi: 10.1145/3065386.

[36] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*. London, U.K.: Oxford Univ. Pres, 2014.

[37] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[38] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[39] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1918–1929, Mar. 2022.

[40] D. Alahakoon, R. Nawaratne, Y. Xu, D. De Silva, U. Sivarajah, and B. Gupta, "Self-building artificial intelligence and machine learning to empower big data analytics in smart cities," *Inf. Syst. Frontiers*, vol. 25, no. 1, pp. 221–240, Feb. 2023.

[41] K.-H. Yu, A. L. Beam, and I. S. Kohane, "Artificial intelligence in healthcare," *Nature Biomed. Eng.*, vol. 2, no. 10, pp. 719–731, Oct. 2018.

[42] R. Abduljabbar, H. Dia, S. Liyanage, and S. A. Bagloee, "Applications of artificial intelligence in transport: An overview," *Sustainability*, vol. 11, no. 1, p. 189, Jan. 2019.

[43] S. Ahmed, M. M. Alshater, A. E. Ammari, and H. Hammami, "Artificial intelligence and machine learning in finance: A bibliometric review," *Res. Int. Bus. Finance*, vol. 61, Oct. 2022, Art. no. 101646.

[44] M. Coeckelbergh, "Artificial intelligence: Some ethical issues and regulatory challenges," *Technol. Regulation*, vol. 2019, pp. 31–34, May 2019.

[45] L. Cao, "AI in finance: Challenges, techniques, and opportunities," *ACM Comput. Surv.*, vol. 55, no. 3, pp. 1–38, Mar. 2023.

[46] R. Jabbar, E. Dhib, A. B. Said, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain technology for intelligent transportation systems: A systematic literature review," *IEEE Access*, vol. 10, pp. 20995–21031, 2022.

[47] M. Reichstein, G. Camps-Valls, B. Stevens, M. Jung, J. Denzler, N. Carvalhais, and Prabhat, "Deep learning and process understanding for data-driven Earth system science," *Nature*, vol. 566, no. 7743, pp. 195–204, Feb. 2019.

[48] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intell. Syst. Accounting, Finance Manag.*, vol. 25, no. 1, pp. 18–27, 2018.

[49] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, Feb. 2018.

[50] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Sliema, Malta, Apr. 2017, pp. 357–375.

[51] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.

[52] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017.

[53] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: Review and open challenges," *Cluster Comput.*, vol. 26, no. 1, pp. 197–221, Feb. 2023.

[54] R. Graf and R. King, "Neural network and blockchain based technique for cyber threat intelligence and situational awareness," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, May 2018, pp. 409–426.
[55] H. Taherdoost, "Blockchain and machine learning: A critical review on security," *Information*, vol. 14, no. 5, p. 295, May 2023.
[56] D. M. Katz, J. J. Nay, and N. M. Rosario, *Artificial Intelligence, Machine Learning, Natural Language Processing, and Blockchain*. Cambridge, U.K.: Cambridge Univ. Press, 2021, pp. 85–120.
[57] U. Prasad, S. Chakravarty, Y. S. Bisht, A. Prusty, G. Nijhawan, and D. M. Lourens, "Using natural language processing and blockchain for employee performance evaluation," in *Proc. 3rd Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, May 2023, pp. 311–315.
[58] A. Ekblaw. (2017). *Medrec: Blockchain for Medical Data Access, Permission Management and Trend Analysis*. Accessed: Jul. 16, 2023. [Online]. Available: https://www.media.mit.edu/publications/medrec-blockchain-for-medical-data-access-permission-management-and-trend-analysis/
[59] X. Tan, J. Gao, and R. Li, "A simple structure for building a robust model," in *Intelligence Science IV*, Z. Shi, Y. Jin, and X. Zhang, Eds. Cham, Switzerland: Springer, 2022, pp. 417–424.
[60] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: Threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021.
[61] IBM Research Blog. (2023). *What is Federated Learning*. Accessed: Oct. 1, 2023. [Online]. Available: https://research.ibm.com/blog/what-is-federated-learning
[62] R. Blackman and B. Ammanath. (2022). *Building Transparency Into AI Projects, Harvard Business Review*. Accessed: Oct. 1, 2023. [Online]. Available: https://hbr.org/2022/06/building-transparency-into-ai-projects
[63] G. Lawton. (2022). *AI Transparency: What is it and Why do We Need It? | Techtarget*. Accessed: Oct. 1, 2023. [Online]. Available: https://www.techtarget.com/searchcio/tip/AI-transparency-What-is-it-and-why-do-we-need-it
[64] P. Chen, L. Wu, and L. Wang, "AI fairness in data management and analytics: A review on challenges, methodologies and applications," *Appl. Sci.*, vol. 13, no. 18, p. 10258, Sep. 2023.
[65] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "Re-thinking data strategy and integration for artificial intelligence: Concepts, opportunities, and challenges," *Appl. Sci.*, vol. 13, no. 12, p. 7082, Jun. 2023.
[66] S. Dahmen-Lhuissier. (2023). *Securing Artificial Intelligence (SAI), ETSI*. Accessed: Oct. 1, 2023. [Online]. Available: https://www.etsi.org/technologies/securing-artificial-intelligence
[67] N. A. Yaacob, M. I. Yusof, S. M. Nuruddin, Z. M. Zain, and N. A. Mustapa, "Non-traditional security issues in Southeast Asia during COVID-19: Implications and mitigation strategies by ASEAN," *Proceedings*, vol. 82, no. 1, p. 90, 2022.
[68] N. Kolokotronis, M. Dareioti, S. Shiaeles, and E. Bellini, "An intelligent platform for threat assessment and cyber-attack mitigation in IoMT ecosystems," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2022, pp. 541–546.
[69] C. Killer, B. Rodrigues. (2019). *Threat Management Dashboard for a Blockchain Collaborative Defense*. UZH Blockchain Center. Accessed: Oct. 1, 2023. [Online]. Available: https://www.blockchain.uzh.ch/publication/threat-management-dashboard-for-a-blockchain-collaborative-defense/
[70] S. Coretti, A. Kiayias, C. Moore, and A. Russell, "The Generals' scuttlebutt: Byzantine-resilient gossip protocols," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.* New York, NY, USA: Association for Computing Machinery, Nov. 2022, pp. 595–608.
[71] M. Allende, D. L. León, S. Cerón, A. Pareja, E. Pacheco, A. Leal, M. Da Silva, A. Pardo, D. Jones, D. J. Worrall, B. Merriman, J. Gilmore, N. Kitchener, and S. E. Venegas-Andraca, "Quantum-resistance in blockchain networks," *Sci. Rep.*, vol. 13, no. 1, p. 5664, Apr. 2023.
[72] A. Agarwal, R. Joshi, H. Arora, and R. Kaushik, "Privacy and security of healthcare data in cloud based on the blockchain technology," in *Proc. 7th Int. Conf. Comput. Methodolog. Commun. (ICCMC)*, Feb. 2023, pp. 87–92.
[73] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 260–264.
[74] M. Hader, A. Elmhamedi, and A. Abouabdellah, "Blockchain technology in supply chain management and loyalty programs: Toward blockchain implementation in retail market," in *Proc. IEEE 13th Int. Colloq. Logistics Supply Chain Manage. (LOGISTIQUA)*, Dec. 2020, pp. 1–6.
[75] R. Kushwaha and D. Singh, *Hyperledger Architecture for Internet of Things and Supply Chain Management Services* (Blockchain Technologies). Singapore: Springer, 2021, pp. 39–63.
[76] A. S. Sani, D. Yuan, K. Meng, and Z. Y. Dong, "Idenx: A blockchain-based identity management system for supply chain attacks mitigation in smart grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.
[77] T. Ashfaq, R. Khalid, A. S. Yahaya, S. Aslam, A. T. Azar, S. Alsafari, and I. A. Hameed, "A machine learning and blockchain based efficient fraud detection mechanism," *Sensors*, vol. 22, no. 19, p. 7162, Sep. 2022.
[78] G. Khan. (2021). *The Synergy of AI and Blockchain: Smart Contracts, Fraud Detection, and Beyond*. Accessed: Oct. 1, 2023. [Online]. Available: https://medium.com/blockchain-biz/the-synergy-of-ai-and-blockchain-smart-contracts-fraud-detection-and-beyond-b46b8ef91d5c
[79] K. Gilani, F. Ghaffari, E. Bertin, and N. Crespi, "Self-sovereign identity management framework using smart contracts," in *Proc. NOMS - IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2022, pp. 1–7.
[80] EDU3LABS. (2023). *Personalized Learning: The Next Frontier in Education With AI and Blockchain*. Medium. Accessed: Oct. 1, 2023. [Online]. Available: https://edu3labs.medium.com/personalized-learning-the-next-frontier-in-education-with-ai-and-blockchain-146b45e77080
[81] A. Bhutoria, "Personalized education and artificial intelligence in the United States, China, and India: A systematic review using a human-in-the-loop model," *Comput. Educ., Artif. Intell.*, vol. 3, Jan. 2022, Art. no. 100068.
[82] W. Hua, Y. Chen, M. Qadrdan, J. Jiang, H. Sun, and J. Wu, "Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review," *Renew. Sustain. Energy Rev.*, vol. 161, Jun. 2022, Art. no. 112308.
[83] S. Aroua, R. Champagnat, M. Coustaty, G. Falquet, S. Ghadfi, Y. Ghamri-Doudane, P. Gomez-Kramer, G. Howells, K. D. McDonald-Maier, J. Murphy, M. Rabah, K. Rouis, N. Sidère, and N. Tamani, "Security and PrIvacy foR the Internet of Things: An overview of the project," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 3993–3998.
[84] V. Buterin, G. Wood, and J. Wilcke. (2015). *Decentralized Autonomous Organizations (DAOS)*. ethereum.org. Accessed: Oct. 1, 2023. [Online]. Available: https://ethereum.org
[85] Numbers. (2023). *Ensuring Trust and Accountability: The Role of Provenance in Generative AI for Content Creation*. Medium. Accessed: Oct. 1, 2023. [Online]. Available: https://numbersprotocol.medium.com/ensuring-trust-and-accountability-the-role-of-provenance-in-generative-ai-for-content-creation-3f9dd7b4b3b0
[86] S. Morgan. (2023). *The Rise of AI in Content Creation*. Burlingtons Legal. Accessed: Oct. 1, 2023. https://burlingtonslegal.com/insight/the-rise-of-ai-in-content-creation/
[87] M. Eltuhami, M. Abdullah, and B. A. Talip, "Identity verification and document traceability in digital identity systems using non-transferable non-fungible tokens," in *Proc. Int. Visualizat., Informat. Technol. Conf. (IVIT)*, Nov. 2022, pp. 136–142.
[88] M. Iranmanesh, P. Maroufkhani, S. Asadi, M. Ghobakhloo, Y. K. Dwivedi, and M.-L. Tseng, "Effects of supply chain transparency, alignment, adaptability, and agility on blockchain adoption in supply chain among SMEs," *Comput. Ind. Eng.*, vol. 176, Feb. 2023, Art. no. 108931.
[89] Y. Wang and Y. Tang, "Enabling cost-effective blockchain applications via workload-adaptive transaction execution," 2022, *arXiv:2210.04644*.
[90] H. Taherdoost, "Blockchain technology and artificial intelligence together: A critical review on applications," *Appl. Sci.*, vol. 12, no. 24, p. 12948, Dec. 2022.
[91] K. Escherich. (2023). *Why Do We Need to Talk About Ethics and Bias in AI? IBM Nordic Blog*. Accessed: Oct. 1, 2023. [Online]. Available: https://www.ibm.com/blogs/nordic-msp/ethics-and-bias-in-ai/
[92] P. S. Varsha, "How can we manage biases in artificial intelligence systems—A systematic literature review," *Int. J. Inf. Manage. Data Insights*, vol. 3, no. 1, Apr. 2023, Art. no. 100165.
[93] M. van Bekkum and F. Z. Borgesius, "Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?" *Comput. Law Secur. Rev.*, vol. 48, Apr. 2023, Art. no. 105770.
[94] L. Floridi, "Establishing the rules for building trustworthy AI," *Nature Mach. Intell.*, vol. 1, no. 6, pp. 261–262, May 2019.

[95] T. Madiega, "Artificial intelligence act," *Eur. Parliament, Eur. Parliamentary Res. Service*, p. 12, Jun. 2023. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792
[96] S. Shanaev, S. Sharma, B. Ghimire, and A. Shuraeva, "Taming the blockchain beast? Regulatory implications for the cryptocurrency market," *Res. Int. Bus. Finance*, vol. 51, Jan. 2020, Art. no. 101080.
[97] D. Dupuis and K. Gleason, "Money laundering with cryptocurrency: Open doors and the regulatory dialectic," *J. Financial Crime*, vol. 28, no. 1, pp. 60–74, Aug. 2020.
[98] J. Gilcrest and A. Carvalho, "Smart contracts: Legal considerations," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 3277–3281.
[99] A. Collomb, P. De Filippi, and K. Sok, "Blockchain technology and financial regulation: A risk-based approach to the regulation of ICOs," *Eur. J. Risk Regulation*, vol. 10, no. 2, pp. 263–314, Jun. 2019.
[100] W. Wu and S. Liu, "A comprehensive review and systematic analysis of artificial intelligence regulation policies," 2023, *arXiv:2307.12218*.
[101] R. Xie, "Why China had to ban cryptocurrency but the US did not: A comparative analysis of regulations on crypto-markets between the US and China," *Wash. U. Global Stud. L. Rev.*, vol. 18, pp. 457–492, Jan. 2019.
[102] J. Zeng, *Artificial Intelligence With Chinese Characteristics: National Strategy, Security and Authoritarian Governance*. Cham, Switzerland: Springer, 2022.
[103] C. Chen and L. Liu, "How effective is China's cryptocurrency trading ban?" *Finance Res. Lett.*, vol. 46, May 2022, Art. no. 102429.
[104] M. Khan, S. Imtiaz, G. S. Parvaiz, A. Hussain, and J. Bae, "Integration of Internet-of-Things with blockchain technology to enhance humanitarian logistics performance," *IEEE Access*, vol. 9, pp. 25422–25436, 2021.
[105] S. Guergov and N. Radwan, "Blockchain convergence: Analysis of issues affecting IoT, AI and blockchain," *Int. J. Computations, Inf. Manuf. (IJCIM)*, vol. 1, no. 1, pp. 1–17, Dec. 2021.
[106] A. Bewersdorff, X. Zhai, J. Roberts, and C. Nerdel, "Myths, mis- and preconceptions of artificial intelligence: A review of the literature," *Comput. Educ., Artif. Intell.*, vol. 4, Jan. 2023, Art. no. 100143.
[107] H. Zhu, "Blockchain and artificial intelligence are also hot topics in the IEEE Systems, Man, and Cybernetics Society [Editorial]," *IEEE Syst. Man, Cybern. Mag.*, vol. 8, no. 4, pp. 4–5, Oct. 2022.
[108] A. Haddad, M. H. Habaebi, Md. R. Islam, N. F. Hasbullah, and S. A. Zabidi, "Systematic review on AI-blockchain based E-healthcare records management systems," *IEEE Access*, vol. 10, pp. 94583–94615, 2022.
[109] N. Dhieb, H. Ghazzai, H. Besbes, and Y. Massoud, "A secure AI-driven architecture for automated insurance systems: Fraud detection and risk measurement," *IEEE Access*, vol. 8, pp. 58546–58558, 2020.
[110] H. Li, Y. Li, Y. Yu, B. Wang, and K. Chen, "A blockchain-based traceable self-tallying E-voting protocol in AI era," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1019–1032, Apr. 2021.
[111] T. Wang, J. Guo, S. Ai, and J. Cao, "RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration," *Appl. Energy*, vol. 295, Aug. 2021, Art. no. 117056.
[112] D. M. Gligor, K. G. Pillai, and I. Golgeci, "Theorizing the dark side of business-to-business relationships in the era of AI, big data, and blockchain," *J. Bus. Res.*, vol. 133, pp. 79–88, Sep. 2021.

OLEKSANDR KUZNETSOV (Member, IEEE) received the D.Sc. degree in engineering. He is currently a Visiting Professor with the Department of Political Science, Communication and International Relations, University of Macerata, Italy. He is also a Professor with the Department of Security Information Systems and Technologies, V. N. Karazin Kharkiv National University, Ukraine. He is a Full Professor and an Academician with the Academy of Applied Radioelectronics Sciences. His research interests include applied cryptology and coding theory, blockchain technologies, the Internet of Things (IoT), and the application of AI in cybersecurity. He was a recipient of the Boris Paton National Prize of Ukraine, in 2021.

PAOLO SERNANI received the Ph.D. degree in information engineering from Marche Polytechnic University, in March 2016. His Ph.D. thesis was on "design and virtualization of intelligent systems for the management of assistive environments." He is an Assistant Professor with the Department of Law, University of Macerata, Italy, where he is currently in charge of the courses "Digital Processes and Technologies" and "Information Systems for Transportation." His main research interests include deep learning for image and video analysis, multi-agent systems, expert systems, and decision support systems.

LUCA ROMEO received the Ph.D. degree in computer science in 2018. His Ph.D. thesis was on "applied machine learning for human motion analysis and affective computing." He is currently a tenure track Assistant Professor of computer science with the Department of Economics and Law, University of Macerata. He is also an Adjunct Professor of customer intelligence and big data at Luiss, Roma. He is affiliated with the Unit of Computational Statistics and Machine Learning, Fondazione Istituto Italiano di Tecnologia, Genova. His research interests include the design of novel machine-learning algorithms for solving relevant challenges in different real-world domains.

EMANUELE FRONTONI (Member, IEEE) is currently a Full Professor of computer science with the University of Macerata and the Co-Director of the VRAI Vision Robotics and Artificial Intelligence Laboratory. He is the author of more than 230 international articles and collaborates with numerous national and international companies in technology transfer and innovation activities. His research interests include computer vision and artificial intelligence with applications in robotics, video analysis, human behavior analysis, extended reality, and digital humanities. He has been the Program Chair or the General Chair of various international conferences and summer schools, such as the IEEE/ASME MESA Mechatronic Embedded System and Applications, in 2016 and 2017, the IEEE ECMR European Conference on Mobile Robotics, in 2017, BigDat 2020, and DeepLearn 2021, and a Co-Organizer of many international workshops, such as DeepRetail@ICPR 2020, D2CH@CVPR 2021, and AI4DH@ICIAP 2022.

ADRIANO MANCINI received the Ph.D. degree in artificial intelligence systems from Marche Polytechnic University, under the supervision of Prof. Primo Zingaretti. His Ph.D. thesis was on "A new methodological framework for land use/land cover mapping and change detection." He is currently an Associate Professor with Marche Polytechnic University. He is involved in several national and international projects, such as EU and Industry-funded projects in the fields of precision/smart agriculture, remote sensing, robotics, cloud-based technologies, and big data. His research interests include computer vision and artificial intelligence with applications in robotics, video analysis, human behavior analysis, and the automatic classification of images.