information

MDPI

Article

The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead

Dhanasak Bhumichai [1], Christos Smiliotopoulos [2,*], Ryan Benton [1], Georgios Kambourakis [2] and Dimitrios Damopoulos [1,3]

[1] School of Computing, University of South Alabama, Mobile, AL 36688, USA; db1924@jagmail.southalabama.edu (D.B.); rbenton@southalabama.edu (R.B.); damopoulos@centinels.org (D.D.)
[2] Department of Information & Communication Systems Engineering, University of the Aegean, 83200 Karlovasi, Greece; gkamb@aegean.gr
[3] Centinels Labs, 52056 Kastoria, Greece
[*] Correspondence: csmiliotopoulos@aegean.gr

Abstract: Artificial intelligence (AI) and blockchain technology have emerged as increasingly prevalent and influential elements shaping global trends in Information and Communications Technology (ICT). Namely, the synergistic combination of blockchain and AI introduces beneficial, unique features with the potential to enhance the performance and efficiency of existing ICT systems. However, presently, the confluence of these two disruptive technologies remains in a rather nascent stage, undergoing continuous exploration and study. In this context, the work at hand offers insight regarding the most significant features of the AI and blockchain intersection. Sixteen outstanding, recent articles exploring the combination of AI and blockchain technology have been systematically selected and thoroughly investigated. From them, fourteen key features have been extracted, including data security and privacy, data encryption, data sharing, decentralized intelligent systems, efficiency, automated decision systems, collective decision making, scalability, system security, transparency, sustainability, device cooperation, and mining hardware design. Moreover, drawing upon the related literature stemming from major digital databases, we constructed a timeline of this technological convergence comprising three eras: emerging, convergence, and application. For the convergence era, we categorized the pertinent features into three primary groups: data manipulation, potential applicability to legacy systems, and hardware issues. For the application era, we elaborate on the impact of this technology fusion from the perspective of five distinct focus areas, from Internet of Things applications and cybersecurity, to finance, energy, and smart cities. This multifaceted, but succinct analysis is instrumental in delineating the timeline of AI and blockchain convergence and pinpointing the unique characteristics inherent in their integration. The paper culminates by highlighting the prevailing challenges and unresolved questions in blockchain and AI-based systems, thereby charting potential avenues for future scholarly inquiry.

Keywords: blockchain; artificial intelligence; smart contract; survey

check for updates

Citation: Bhumichai, D.; Smiliotopoulos, C.; Benton, R.; Kambourakis, G.; Damopoulos, D. The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead. *Information* **2024**, *15*, 268. https://doi.org/10.3390/info15050268

Academic Editors: Nelly Leligou and Kun She

Received: 7 February 2024
Revised: 23 April 2024
Accepted: 3 May 2024
Published: 9 May 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Blockchain and artificial intelligence (AI) are widely recognized as technologies with the potential to fundamentally transform and innovate across multiple industries and sectors. While the term blockchain truly began to captivate the global tech community in 2008 through the launch of the Bitcoin cryptocurrency by Satoshi Nakamoto [1], the fundamental principles and concepts it is based on have been in practice since the 1980s [2]. Specifically, the first attempt to create a decentralized and cryptographic digital money came out as early as 1983 in the seminal paper titled "Blind signatures for untraceable payments" [3]. At the other end of the spectrum, modern conceptions of AI began when mathematician and computer scientist Dr. Turing (1950) introduced the foundational concept of machine intelligence through his examination of whether machines could think [4]. Currently, the ongoing integration of blockchain and AI into a unified methodology is transforming business paradigms by incorporating the principles of decentralization, data immutability, and procedural democracy [5–7].

On the one hand, blockchain operates as a distributed ledger, employing a range of protocols, consensus algorithms, and governance models [1,8–10]. It allows network entities like nodes, smart contracts, and end-users to achieve consensus autonomously, eliminating the necessity for intermediary third parties, such as banks, legal services, payment processors, or any entity that acts as a centralized authority to validate, authorize, or oversee operation. Its design ensures that, once data are recorded, they become immutable, safeguarding the integrity of sequential event records. Its non-reliance on intermediaries such as banks or lawyers to ensure trust and security can additionally decrease costs and increase processing speed. Actually, as blockchain technology evolves to include smart contracts and AI agents, it could offer greater transparency and efficiency. For instance, the Ethereum network executes approximately 429K simple instructions per sec, highlighting its substantial computational capacity. However, this figure is a rough estimate, and the actual number can vary significantly based on the complexity and types of operations processed. For instance, other blockchains such as Avalanche offer private (permissioned) or public (permissionless or trustless) blockchain subnetworks to resolve the challenges of scalability and interoperability. Experts urge caution, highlighting the complex challenges and mixed opinions regarding the integration of AI with blockchain technology [11].

Furthermore, the authors in [12] conducted an exhaustive investigation into the balance between energy efficiency, decentralization, and security attained through decentralized consensus algorithms. This scrutiny reveals their profound influence on both the scalability and widespread adoption of blockchain infrastructures, underscoring the pivotal role these algorithms occupy in the progression of blockchain technology. Financial experts project the global blockchain market to surge from USD 564.01M in 2024 to USD 2475.35M by 2030, growing at a Compound Annual Growth Rate (CAGR) of 27.9% [13].

On the other hand, AI encompasses a broad spectrum of computing, empowering machines to perform complex tasks and solve problems through knowledge databases [14,15]. AI's capabilities extend to learning, decision making, prediction, and classification, using both pre-collected and real-time data. The McKinsey Global Institute forecasts that AI applications could generate an additional USD 13T in economic output by 2030, boosting global Gross Domestic Product (GDP) by about 1.2% annually [16].

The merging of blockchain and AI is shaping up to be a dynamic and rapidly evolving area of scientific inquiry. This combination has the potential to enhance performance, quality, and security across various sectors, including logistics for food supply chains and healthcare marketplaces [8,17–20]. AI's ability to process vast datasets, innovate, and identify patterns can substantially complement the security mechanisms of blockchain technology [19]. Furthermore, decentralized blockchain networks can validate new classifiers and patterns identified by AI [21]. Together, these technologies can revolutionize traditional methods, offering groundbreaking advancements to individuals, organizations, and businesses. Altogether, blockchain can improve transaction processes, addressing longstanding challenges related to security, transparency, traceability, authenticity, and in some cases, performance [22–25], while AI reshapes global economic activities by relieving humans from repetitive, resource-heavy, and time-consuming tasks.

Furthermore, AI agents in combination with smart contracts play a crucial role in automating routine tasks, allowing for the reallocation of human resources to more complex and creative tasks. The collaborative synergy between AI and blockchain technologies promises to optimize numerous sectors, enhancing efficiency, performance, and security and fostering innovation across the board [26].

This paper presents a systematic meta-survey of contemporary literature on blockchain and AI convergence, aiming to develop a new model for anyone interested in this area.

After identifying related literature trends, this work offers insights into integrating these technologies for organizational and business benefits, efficiency, and accountability. Altogether, our work serves as a critical tool for students, researchers, scholars, and industry experts, by analyzing the recent literature. It streamlines current knowledge, identifies critical gaps, and sets directions for future research, thereby systematizing and possibly enhancing both theory and practice in the AI and blockchain field. Specifically, the paper seeks to answer the following key questions about consolidating these technologies, as well as developing a fully fledged meta-survey for anyone interested in this dynamic field:

- How do these two technologies support each other when they are combined?
- What are the distinctive eras in the convergence of blockchain/AI technologies?
- What are the characteristics of these two technologies, before and after they are merged?
- After their convergence, how will these two technologies be applied to the real world?
- What are the challenges and future trends?

The remainder of this paper is organized as follows. The next section delves into the specifics of blockchain and AI, briefly examining how these technologies complement and enhance each other. Section 3 details our methodology, also offering a brief review of the relevant literature. Section 4 introduces a taxonomy that delineates the characteristics and applications of blockchain and AI in their combined form. The same section also details the combined application of blockchain and AI technologies in five focus areas. Section 5 discusses the impact of the synergistic combination of blockchain and AI, while Section 6 identifies the challenges and open issues that arise from the integration of blockchain and AI. The concluding section summarizes our findings and suggests directions for future work.

2. Background

This section provides a brief, but concise overview of the fundamentals of blockchain and AI, emphasizing how the integration of these two technologies enhances their performance and effectiveness.

2.1. Blockchain Technology

Bitcoin, as introduced by Nakamoto [1], has catalyzed the prominence of blockchain technology within the research community. This milestone, however, marked the beginning of a broader technological evolution, extending blockchain into an umbrella term for various forms of distributed ledger technologies (DLTs). These advancements have paved the way for the adoption of blockchain technology across multiple industries, including finance, healthcare, cybersecurity, and business, supporting practical applications [27–30].

Notably, the broader blockchain ecosystem, featuring over 2.4M cryptocurrencies across various layers, has achieved a staggering market cap of USD 2.66T [31]. The enterprise sector is witnessing a similar trend, with nearly 90% of businesses in the U.S., U.K., India, and China starting to use blockchain in some capacity. Governments around the world are leveraging blockchain to enhance public services, streamline administrative processes, and boost trust among citizens [32–34]. The World Economic Forum has highlighted that many countries worldwide, representing 98% of global GDP, are currently exploring the adoption of Central Bank Digital Currencies (CBDCs) [35]. These figures suggest that blockchain technology's adoption continues to expand, offering transformative possibilities for both government and enterprise sectors globally.

Beyond the transition from Bitcoin's Proof of Work (PoW) to incorporating earlier consensus algorithms like Practical Byzantine Fault Tolerance (PBFT), the field has seen the emergence of a multitude of consensus mechanisms [36]. These mechanisms address various challenges such as scalability, energy efficiency, and transaction speed, reflecting the dynamic adaptability of DLTs [37]. Moreover, the exploration into scalability and interoperability issues highlights the ongoing efforts to enhance DLT functionalities, ensuring their seamless integration across different platforms and industries [27–30,38]. The impact of these technologies extends beyond technical improvements, influencing societal structures and governance models, and redefining trust in digital transactions [39–43]. This comprehensive evolution underscores the multifaceted potential of blockchain and DLTs, heralding a new era of technological innovation and societal transformation.

Blockchain technology enables the secure tracking and updating of information on distributed systems, such as cryptocurrency transactions [44]; the reader should keep in mind that "secure" in a ledger means that entries have not been altered, but not that they were factually correct when entered. Namely, blockchain enables participants to connect and transfer state-updated information across the network based on a distributed network of participants, each of whom maintains a copy of the ledger. (Note that, depending on the case, the term participants is used to refer to the various actors involved, not just in the context of Bitcoin or any specific layer, but across the entire spectrum including the network, protocol, governance, and application layers). These participants must contain a trusted quorum of intermediaries, with the specific quorum size and trust model depending on the consensus mechanism employed by the blockchain solution. The decentralization of trust ensures that transactions are validated and recorded through a consensus process involving multiple participants. It should be mentioned that, while blockchain technology enhances transaction security and transparency through cryptographic algorithms, decentralization, and consensus mechanisms, it inherently relies on trust assumptions regarding the network's participants. For instance, in Bitcoin's PoW consensus, there is a fundamental trust assumption that the majority of computing power is controlled by honest nodes to prevent 51% attacks, which could compromise ledger integrity. Therefore, rather than eliminating the need for trust, blockchain shifts where and how trust is required within the system, especially in scenarios susceptible to the 51% attack, software vulnerabilities, or other forms of collusion.

Overall, in terms of trust, while blockchain technology enables secure, intermediary-free transactions, the degree of trustlessness varies by architecture. Public blockchains like Bitcoin and Ethereum are highly decentralized, promoting a trustless environment if protocol rules are followed and there is a lack of system vulnerability, whereas private blockchains involve some trust among a limited group of participants. Additionally, it is important to acknowledge that blockchain operators and majority stakeholders can significantly influence a blockchain's operations, as evidenced by historical adjustments in various networks. Such adjustments, like Ethereum's DAO fork [45] and Bitcoin's SegWit [46], illustrate how blockchains adapt to issues like security and centralization, highlighting the technology's dynamic nature and its susceptibility to influence from key players.

Altogether, the inherent key characteristics of blockchain are depicted in Figure 1 and succinctly detailed below; note that the same characteristics are also critical minimum requirements for the successful operation of any distributed project:

(a) Decentralization: Blockchain is inherently a decentralized and distributed system, designed to facilitate Peer-to-Peer (P2P) communication among participating nodes. This decentralization eliminates single points of failure [47], thereby contributing to the overall resilience of the system. Note that decentralized refers to the absence of a central authority in controlling the system, while distributed implies the spread of data and processing across multiple nodes. Simply put, decentralization ensures that no single entity has control over the network, while distribution ensures that copies of the ledger are stored across multiple nodes for redundancy and security [48]. This decentralization is particularly effective in permissionless blockchains like Bitcoin, where anyone can join as a full node, making the system more robust against censorship and control by any single entity. However, the resilience to attacks depends on the specific protocol and network configuration, the threat model, and the attack surface.

(b) Censorship resistant: In permissionless blockchains, where participation is open to anyone, censorship resistance is a core feature. Transactions are recorded on the blockchain through a consensus mechanism that involves a decentralized network of nodes, making it extremely difficult for any single entity to control or censor transactions. In contrast, permissioned blockchains, which are controlled by a membership service deciding who may join, do not inherently offer the same level of resistance to censorship [49–51]; nevertheless, they still typically offer more resilience against censorship compared to centralized databases. The permissioned nature of the blockchain and the distributed control among authorized participants contribute to this resistance.

(c) Immutability: Immutability, a fundamental characteristic often attributed to blockchain technology, arises from the combination of consensus mechanisms and the decentralized architecture inherent in blockchain systems. These consensus mechanisms, including, but not limited to, PoW or Proof of Stake (PoS), contribute to the security and unalterability of the ledger [49,52,53]. This decentralized consensus ensures that once data are recorded on the blockchain, they cannot be altered without the consensus of the network, making the blockchain, viewed as a data structure, resistant to modification and tampering.

(d) Transparency: Blockchain promotes transparency by allowing all nodes in the network access to transaction details [54]. Compared with centralized systems, where the central server has exclusive control and access to all data, blockchain technology is designed to support all nodes actively involved in the network. These nodes have the ability to view comprehensive information related to transactions. Moreover, every single node possesses its own copy of the ledger and shares a record of all transactions, which maintains individual nodes staying synchronized and up-to-date with the latest transactions and modifications to the blockchain.

(e) Anonymity: In blockchain networks, participants can create multiple addresses for access, enhancing privacy as their personal information is not stored on third-party platforms. While this approach offers a strong degree of anonymity, perfect privacy preservation is not guaranteed due to the inherent limitations of the technology [55,56].

(f) Security: Blockchain technology provides robust security features such as tamper-proof record keeping and traceable transactions. Merkle trees enhance this security by allowing the efficient and verifiable linkage of transaction blocks, ensuring the integrity and immutability of data [57]. These traits offer an efficient means to safeguard data integrity, particularly in sensitive domains like medical records [17,58] and financial transactions [59]. By tailoring blockchain solutions to specific applications or integrating AI algorithms for enhanced data analysis, organizations can further enhance security and protect against unauthorized access and tampering.

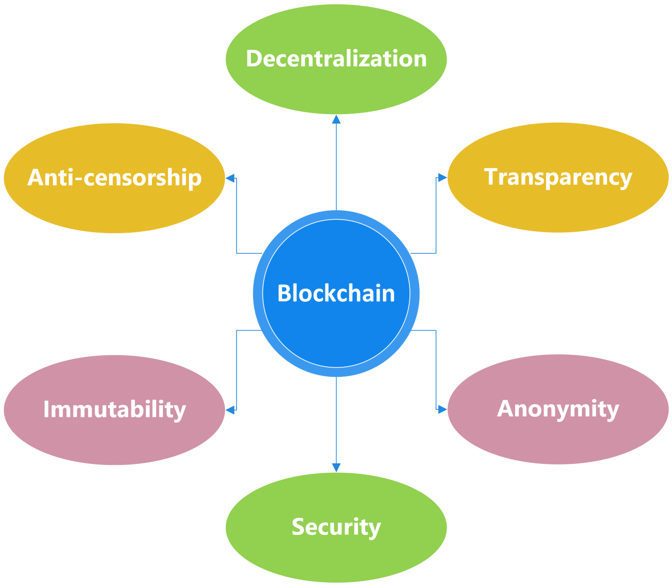

Figure 1. Key characteristics of blockchain.

2.2. Artificial Intelligence

Artificial intelligence enables machines to simulate human intelligence and problem-solving capabilities. Specifically, autonomy in AI systems refers to the ability of AI to operate independently, without human intervention, input, or direct supervision.

AI has been defined in a number of different ways, which can be loosely grouped into four categories: (a) thinking humanly, (b) thinking rationally, (c) acting humanly, and (d) acting rationally [60]. More specifically, AI can be defined as "the study of computations that make it possible to perceive, reason and act" [61] or "the study of how to make computers do things at which, at the moment, people are better" [62]. As such, while AI methods do utilize well-defined algorithms, they distinguish themselves from traditional programs by incorporating elements of adaptability and learning. This departure from strict determinism allows AI algorithms to handle more complex and dynamic situations, marking a notable contrast with the more rigid nature of traditional programming approaches.

The recent progress in AI, specifically in the development of Large Language Models (LLMs), like GPT, Massive Multitask Language Understanding techniques (MMLU) in Gemini, and other AI-powered autonomous agents, has shown remarkable ability in analyzing and understanding vast amounts of data. These advanced AI models, developed through extensive training on large datasets, demonstrate exceptional abilities in tasks involving the comprehension and production of natural language. Despite not storing information conventionally, these models have complex architectures that enable quick access and modification of large models. This is accomplished by utilizing modern techniques such as fine-tuning [63], prompt engineering [64], and reinforcement learning [65]. These methods improve the ability and effectiveness of the systems in changing conditions.

AI, an interdisciplinary domain, integrates insights from various fields including nature, neuroscience, psychology, philosophy, linguistics, electrical engineering, and computer science [66]. The key features of AI, illustrated in Figure 2, are detailed below.

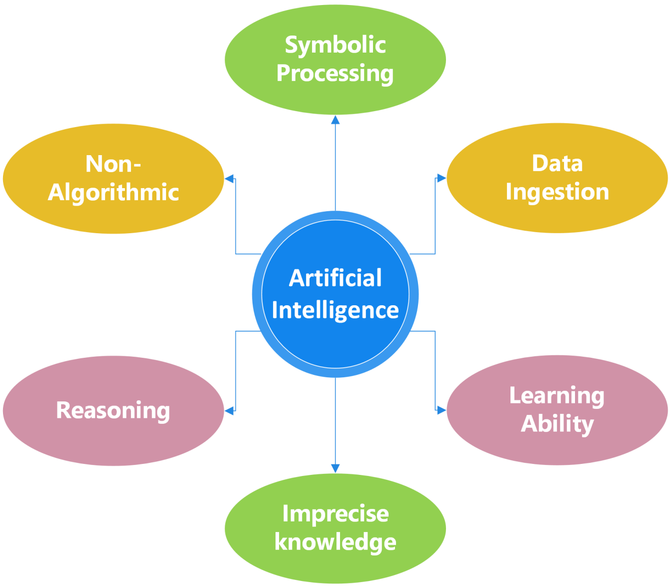

Figure 2. Key characteristics of AI.

(a) Symbolic Processing: As already pointed out, AI algorithms concentrate on symbols more than numbers or letters. In other words, real-world objects, events, and environments are transformed and represented by strings. Then, the strings are transformed into symbols before being organized into structures like lists or hierarchies [67], which can illustrate the relationship among those symbols. Altogether, AI algorithms can support machines to understand and recognize objects, events, and environments in the real world.

(b) Non-Algorithmic: Traditional computer programs adhere to predefined algorithms, necessitating explicit human instructions for each step. In contrast, AI algorithms autonomously navigate problem-solving processes. This autonomy not only streamlines solutions, but also allows for adaptability, as AI can dynamically respond to varying conditions without rigid human programming [66].

(c) Reasoning: AI's distinction lies in its capacity to handle knowledge rather than mere data, enabling the application of deductive or inductive reasoning approaches. This is pivotal for refining machine reasoning's effectiveness. Therefore, several algorithms such as case-based reasoning, case-based decisions, and analogical reasoning [68] were proposed to enhance the effectiveness of machine reasoning. By leveraging such reasoning methods, AI algorithms excel in finding solutions, mirroring the cognitive processes employed by humans.

(d) Data ingestion: AI, leveraging statistical algorithms and Machine Learning (ML) [69], autonomously manages vast datasets from diverse sources. This autonomous data ingestion eliminates human errors, accelerates processes, and minimizes inaccuracies in data handling. The practical advantages manifest in heightened efficiency and enhanced accuracy throughout the data-processing stages.

(e) Learning ability: The primary goal of AI is to emulate human cognition by learning from experience, adapting to new circumstances, and performing tasks that typically require human intelligence [70]. Examples include chess games, stock market predictions [71], and self-driving vehicles [72]. The importance here is not only in the emulation of human intelligence, but also in the requirement for data ingestion to support AI models in manipulating specific tasks and enhancing learning ability.

(f) Imprecise knowledge: While traditional applications thrive on precise knowledge, AI algorithms excel in navigating unstructured and imprecise information. Innovations like fuzzy set theory, formal logic, and mathematical morphology [73] enhance AI's prowess in managing imperfect information. This adaptability positions AI as a powerful tool for real-world applications, where achieving precision may pose challenges.

3. Methodology

Previous work on the subject reveals that combining AI with blockchain technology is a novel, disruptive issue with several ongoing open research challenges such as privacy policy, smart contract security, the reliable manner of oracles, expandability, consensus protocols, standardization, interoperability, the resilience of quantum computing, and data governance [6,18,74–76], which have not been yet extensively investigated and initiated. In this context, as already pointed out, the objective of this study is to offer a comprehensive and holistic, but succinct viewpoint on the integration of blockchain and AI. This endeavor starts with the examination of the pertinent, recent literature. Namely, the concentration is on key survey works that at least touch upon the subject of blockchain and AI convergence, only considering contributions published between 2018 and 2023.

To ensure the robustness and reproducibility of our study, we adopted a methodology grounded in the principles of Systematic Literature Reviews (SLRs) [77] complemented by bibliometric analysis [78]. This approach allowed us to systematically identify, evaluate, and synthesize the existing body of knowledge on the convergence of blockchain and AI, ensuring comprehensive coverage and objectivity:

- Following the guidelines proposed by Kitchenham et al. [77] for conducting SLRs in software engineering, we meticulously defined our research questions, identified relevant search terms, and selected appropriate databases for our search.
- Our selection criteria were explicitly defined to ensure the inclusion of seminal works that contribute significantly to the topic.
- Furthermore, as described by Ellegaard et al. [78], to analyze trends and patterns in the literature, we applied bibliometric analysis techniques, which enabled us to construct

a timeline of the convergence of blockchain and AI and to identify key thematic areas of focus.

- This dual approach of SLR and bibliometric analysis ensures our methodology is not only transparent and replicable, but also provides a comprehensive overview of the field's current state and future directions.

Towards this end, we strategically identified closely relevant terms or abbreviations for investigation, including "blockchain", "artificial intelligence", "intelligence", "intelligent", "AI", and "Machine Learning". Next, for enhancing the precision of our search and ensuring its alignment with the fundamental goals of the current meta-survey, we focused our attention on seminal literature for extracting pertinent keywords. The utilization of Karger's approach [79] played a key role in systematically gathering relevant studies and academic papers. In particular, the search strategy employed a comprehensive range of specific terms and phrases, such as "distributed ledger", "smart contract", "deep learning", and "neural network". The search was conducted with attention to detail and thoroughness, encompassing major scientific databases, namely Scopus, ACM, IEEE Xplore, Science Direct, and Springer Nature. Specifically, each database was queried based on the combination of the following keywords dedicated to the studied subject: "blockchain" AND "artificial intelligence" (OR "intelligence" OR "intelligent" OR "AI" OR "Machine Learning" OR "distributed ledger" OR "smart contract" OR "deep learning" OR "neural network").

An in-depth examination of the chosen papers was conducted, focusing on studies that delve into the convergence, integration, incorporation, combination, collaboration, merging, or amalgamation of blockchain and AI. Eight previously reviewed survey papers were identified as pivotal, due to their precise alignment with the aims of the current meta-survey. As detailed in Section 4, a timeline reflecting the convergence drawn from the accumulated data was then constructed. This was followed by a separate extraction of features pertinent to the fusion of blockchain and AI. That is, 14 notable cross-sectoral features emerged: data security (DS), data privacy (DPri), data encryption (DE), data sharing (DShr), decentralized intelligent systems (DISs), efficiency (EF), automated decision systems (ADSs), collective decision making (CDM), scalability (SC), system security (SS), transparency (TR), sustainability (SUS), device cooperation (DCop), and mining hardware design (MHD). To ease the reader in navigating through the pertinent key literature, a brief summary of each included work along with a map of the fulfilled features per work is given in Table 1.

Table 1. Extracted features based on key survey works.

Work	Extracted Features														Year	Summary
	DS	**DPri**	**DShr**	**DE**	**DIS**	**EF**	**ADS**	**CDM**	**SC**	**SS**	**SUS**	**TR**	**DCop**	**MHD**		
AI and blockchain: A disruptive integration [19]	✓	✓	✓		✓		✓		✓	✓			✓		2018	Presentation of contemporary efforts in the field of blockchain and AI convergence and their impact on everyday life, the working environment, and human interactions.
The synergy of blockchain and artificial intelligence [80]		✓		✓		✓	✓		✓	✓	✓			✓	2018	Examination of how the merging of contemporary AI decentralized techniques with blockchain's smart contracts philosophy may create new possibilities and opportunities towards the upcoming blockchain 2.0 era of bug-free smart contracts.
Blockchain for AI: Review and open research challenge [18]	✓				✓	✓	✓	✓							2019	A detailed taxonomy of blockchain's key characteristics, specifically focused on how those can be integrated and leveraged into AI decentralized applications.
Data transparency with blockchain and AI ethics [81]		✓							✓			✓			2019	Examination of data ethics and transparency as two integral and fundamental parts of AI, under the concept of convergence with blockchain transparency practices.
Decentralized and collaborative AI on blockchain [82]					✓	✓						✓			2019	Presentation of a decentralized AI framework that permits multiple participants to collaboratively collect massive amounts of no-spam data, towards the creation of robust datasets ideal for ML problems. Blockchain smart contracts are imported for guaranteeing immutability during the data-collection process.
Combining Blockchain and Artificial Intelligence-Literature Review and State of the Art [79]	✓	✓	✓	✓	✓		✓			✓		✓		✓	2020	Systematic literature review on the subject of blockchain and AI integration. Presentation of the most prominent real-life projects of applicability, their advantages, arisen concerns, and possible drawbacks that should concern the scientific community.
Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city [83]	✓	✓	✓	✓	✓		✓				✓	✓			2020	Detailed discussion on the convergence of blockchain and AI applications under the dedicated concept of a blockchain–AI designed smart city. Systematic presentation of the most important concerns regarding the security vulnerabilities and sustainability of smart infrastructures towards an ever-expanding hostile environment, along with the proposal of ongoing projects and future directions.

Table 1. *Cont.*

Work	**Extracted Features**														**Year**	**Summary**
	DS	**DPri**	**DShr**	**DE**	**DIS**	**EF**	**ADS**	**CDM**	**SC**	**SS**	**SUS**	**TR**	**DCop**	**MHD**		
Convergence of Blockchain and Artificial Intelligence to Decentralize Healthcare Systems [84]	✓	✓	✓	✓	✓		✓				✓	✓			2020	Inspection of the applicability of blockchain and AI dynamic features towards the creation of a decentralized storage network of private bio-data in favor of the amelioration of precautionary healthcare and dedicated prescription of drugs.
The Applications of Blockchain in Artificial Intelligence [85]	✓	✓	✓		✓		✓	✓							2021	Systematic survey on the subject of how blockchain smart contracts may benefit AI decentralized concepts upon secure data sharing, data privacy, and trusted decision making.
Convergence of Blockchain and Artificial Intelligence [86]		✓	✓	✓	✓	✓			✓	✓			✓		2022	Presentation of blockchain's and AI's major concepts of applicability, how the former benefits the latter, and vice versa, when it comes to the implementation of collaborative integration projects.
A Bibliometric Analysis of Research on the Convergence of Artificial Intelligence and Blockchain in Smart Cities [87]	✓	✓	✓	✓	✓		✓				✓	✓			2023	Systematic literature review focused on the subject of blockchain and AI convergence in favor of smart transportation techniques under the concept of the smart city.
Analysis of Issues Affecting IoT, AI, and Blockchain Convergence [88]		✓					✓		✓			✓			2023	Hybrid technique focused on overriding potential constraints caused by blockchain and AI integration under the general concept of IoT applicability.
Artificial intelligence and blockchain integration in business: trends from a bibliometric-content analysis [89]	✓		✓				✓			✓		✓			2023	Systematic content analysis on the subject of blockchain and AI convergence, oriented toward business applicability around 10 prominent areas, including supply chains, healthcare, secure transactions, finance, etc.
Bibliometric Analysis on the Convergence of Artificial Intelligence and Blockchain [90]	✓				✓	✓			✓			✓			2023	Presentation of the motivation and philosophy behind the architecture of a hybrid Internet Computer Protocol (ICT) digital twin (DT) model that is developed on top of the concept of converging blockchain's and AI's versatile decentralized features.
Convergence of Distributed Ledger Technologies with Digital Twins, IoT, and AI for fresh food logistics: Challenges and opportunities [91]		✓		✓	✓		✓					✓			2023	Systematic review on existing areas of applicability and integration of blockchain and AI decentralized concepts, including the IoT, DTs, and distributed ledgers under the general theme of food supply logistics.
Integration of Blockchain and AI: Exploring Application in the Digital Business [7]	✓				✓	✓			✓			✓			2023	Presentation of the potentials of the applicability of blockchain and AI convergence as those are implemented in productive business concepts.

4. Blockchain and AI Convergence

The initial concept of integrating AI and blockchain can be traced back to 2014 and 2015 [79]. However, at that juncture, the integration of blockchain and AI was germinal and unclear, as evidenced by the solitary work found from that time [92]. Also with reference to Table 1, a more thorough and concerted exploration into the amalgamation of these technologies emerged in subsequent years (2018–2023), as indicated by a series of publications [7,17–19,47,58,74–76,79–91,93,94].

Omohundro et al. [95] suggested that both cryptocurrencies and smart contracts can potentially contribute to ensuring that AI systems have positive and beneficial impacts on human society. Traditional smart contracts are generally satisfactory when it comes to handling transactions that are purely digital in nature. However, challenges may arise when dealing with interactions that involve the real and physical world. In such cases, additional intelligence and a deeper understanding of decision-making processes might become necessary. Moreover, AI systems play a crucial role in translating data collected from various sensors into a format that can be precisely understood by smart contracts. This translation is essential for making sense of real-world information in a way that smart contracts can process and respond to. For smart contracts that go beyond digital transactions and interact with the physical world, e.g., triggering the delivery of objects, a more sophisticated approach is needed. This involves linking these smart contracts to either human agents or robotic agents capable of carrying out physical actions [95].

The experiment of Zyskind et al. [96] revealed that blockchain technology can be utilized as a framework or infrastructure for databases to promote increased sharing of personal data by individuals. Personal data that individuals share within the blockchain systems implemented as database resources play a crucial role in training AI algorithms to make predictions, recommendations, or decisions. This wealth of data can be utilized as a source of information for training and improving AI systems [79].

To provide a comprehensive, but easier understanding of the evolution and integration of blockchain and AI and their distinct features both individually and in combination, we have segmented the timeline into three distinct phases detailed in Sections 4.1–4.3: the emerging era, the convergence time, and the application and combination stage. In view of the above, Figure 3 offers a detailed taxonomy and outlines the timeline of blockchain and AI integration, including an in-depth look at feature categorization.

With reference to Sections 2 and 3, and Table 1, it becomes apparent that the literature works on blockchain's and AI's integration towards the applicability of their inherent distributed nature in favor of real-life concepts follows an increasing trend from at least 2018 onwards. Naturally, this reflects the augmenting rise in the complexity and frequency of concerns, including security vulnerabilities, exploitation and cyberattacks from malevolent actors, robustness, and sustainability as part of an ever-evolving environment and, above all, their functionality in favor of the well-being of human societies.

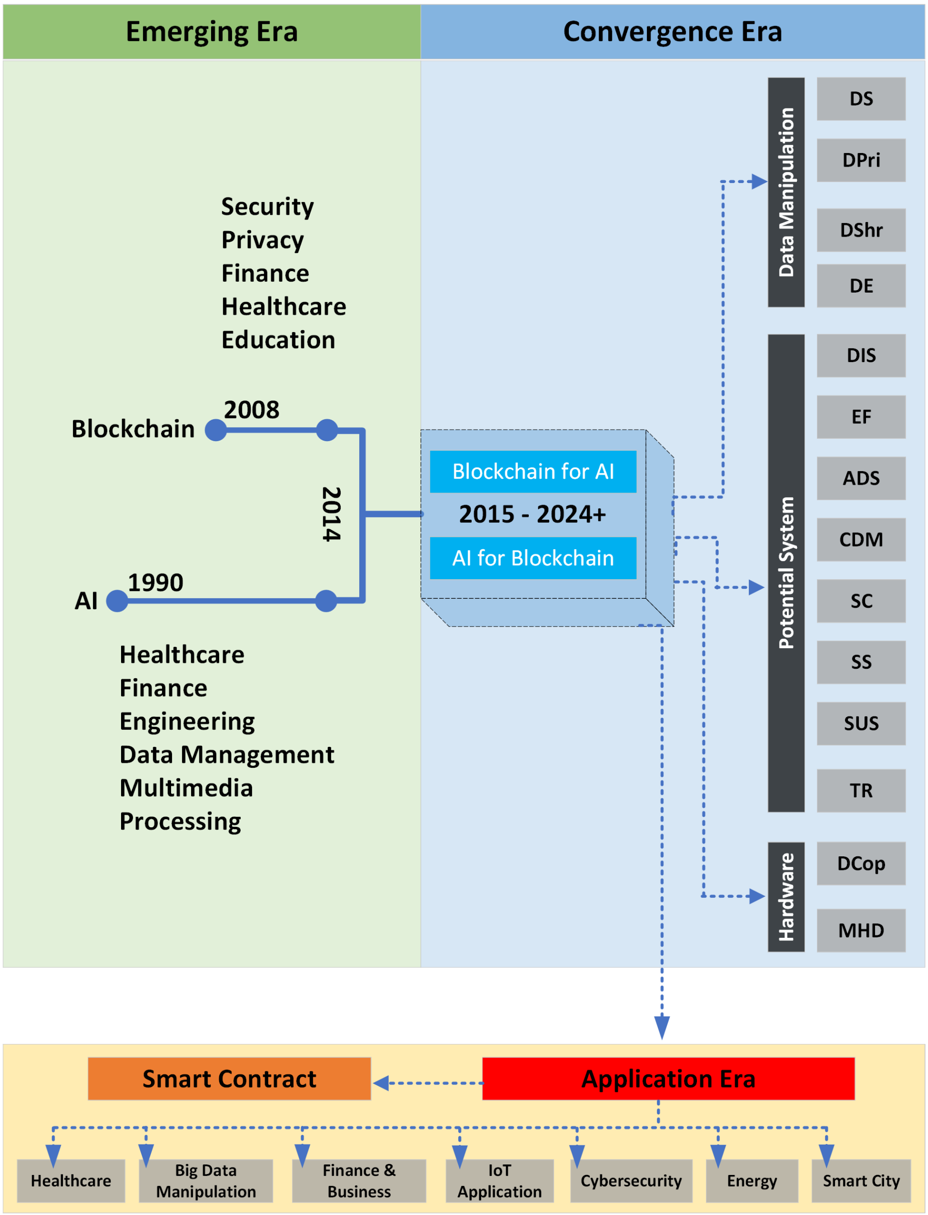

Figure 3. Taxonomy of the timeline of blockchain and AI integration.

4.1. Emerging Era

Prior research in this field has consistently affirmed the potential of both blockchain and AI as instrumental tools in augmenting the efficacy of various business, organizational, and industrial operations. Consequently, AI and blockchain technologies have been extensively adopted across numerous, diverse objectives and fields, underscoring their versatility and wide-ranging applicability. For instance, in transportation systems, implementing blockchain for smart vehicles can improve the security and privacy of this intelligent vehicle ecosystem [97,98]. Furthermore, the combination of these two technologies is prevalent in healthcare sections. For instance, integrating blockchain and AI for enhanced data analysis and streamlined information flow in cardiovascular medicine [58] and the application of AI and blockchain technology for safeguarding and securing personal data involve empowering users with control over the transmission of their personally identifiable information [97]. This also showcases the tangible adoption of these technologies in practical settings. The combination of AI and blockchain also benefits business units. This integration enhances market processes and ensures secure communication among diverse customers [73].

Recent advancements in Internet of Things (IoT) and blockchain predictions have led to the incorporation of numerous classification schemes to formulate a hybrid model. Although challenges in placing blockchain, AI, and the IoT under the same umbrella, possibly forming a cohesive system, include issues related to security, scalability, accountability, and the trustworthiness of communications, few, however, will argue that a successful and effective integration of these domains will propel the development of new business models, as well as the digital transformation of market corporations [88]. By examining real-world instances of deployment and success stories, it becomes evident that adoption in this context implies active utilization and integration into operational frameworks.

The convergence of these technologies represents a significant advancement in the field of ICT. As already mentioned, blockchain technology, initially developed to support Bitcoin algorithms, has rapidly expanded its applications beyond cryptocurrency. It is renowned for its data privacy, security, and decentralized nature. Blockchain's influence extends across various sectors, including banking, healthcare, and other sectors, revolutionizing the way data are managed and transactions are conducted. Its ability to offer decentralized solutions has made it a valuable and handy tool for industries aiming to enhance efficiency, security, and transparency in their operations. On the other hand, AI, evolving significantly since its early days, has become pivotal in creating intelligent network systems, especially with the introduction of deep learning (DL) methods. These methods, leveraging advanced computing technology, have far enhanced the capabilities of traditional neural networks by effectively handling complex, non-linear data. AI's application spans diverse fields, including smart energy systems, healthcare, finance, gaming, and cybersecurity.

More specifically, blockchain has been wildly adopted in several aspects of information technology, thanks to its several advantages. First, blockchain technology was developed with the purpose of contributing to the Bitcoin algorithms introduced by Nakamoto [1] in 2008. In the same year blockchain was introduced, the anonymous blockchain was examined, and data privacy on the Bitcoin platforms was investigated by [99]. They explored how participants are tracked on Bitcoin systems using the transaction graph and data available to the public. A few years later, blockchain technology, which has become a popular topic among ICT researchers, has also been applied to several types of scientific areas. For example, blockchain 1.0 was initially introduced with the purpose of decentralizing currency transactions and digital payment systems [100]. Blockchain is also employed to improve the performance outcomes of different types of industries in various domains. Many industrial sections adopt blockchain technology to improve workflows, run a smooth operation, provide data privacy, data security, and data sharing, raise efficiency, and control organizational costs [101]. Especially for the health sector, the decentralization feature of blockchain can aid stakeholders in accessing the same patient records without associating with a third party over global health records [102].

Furthermore, AI has been remarkable, transitioning from the initial stages of limited success to its current status as a rapidly growing field, particularly after the advent of DL methods [103]. These advanced algorithms, emerging alongside the rapid evolution of computer technology [104], have addressed some limitations of traditional neural networks, notably in handling complex and non-linear data more effectively [105]. AI's scope has expanded significantly, finding applications in various sectors such as smart energy systems [106,107], hospital inpatient care and clinical decision support systems [108,109], finance [96], computer games [110], and more notably, in cybersecurity [111–114].

4.2. Convergence Era

With reference to Table 1, similarities among certain extracted features were identified, leading to their organization into three groups: data manipulation, potential system, and hardware issues. Each group comprises a number of sub-features, as given in the "Extracted Features" column of Table 1. Namely, the first group includes data security, data privacy, data sharing, and data encryption. The second group comprises eight sub-features, i.e., decentralized decision systems, efficiency, automated decision systems, collective decision systems, scalability, system security, sustainability, and transparency. The last group encompasses device cooperation and mining hardware design as its sub-features. Detailed discussions of each group and their associated features are presented in Sections 4.2.1, 4.2.2 and 4.2.3, respectively.

4.2.1. Data Manipulation

Data hold critical importance for both individuals and organizations. As mentioned earlier, this work outlines four key features destined to ensure comprehensive data protection, accurate transfer, and secure storage within systems where blockchain and AI are integrated:

(a) Data security: Blockchain technology offers exceptional security for data storage. It creates a diskless environment, where sensitive and confidential information is securely held. This secure environment enables AI algorithms to operate on protected data, significantly enhancing the accuracy of decision-making processes [18]. Furthermore, the application of blockchain in ML, and generally in AI, tasks can elevate the quality of learning data. It also encourages data creators or owners to share their resources [79,87]. For instance, in the medical field, physicians and researchers could access anonymized patient records, which are invaluable for discovering cures and developing advanced treatment methods and medical procedures [19]. This approach is particularly beneficial for doctors dealing with rare diseases, as it facilitates the search for similar cases worldwide.

(b) Data privacy: Blockchain systems, which house extensive personal information, necessitate stringent privacy measures [80,88]. In a blockchain environment, privacy becomes a crucial concern, as each participant has access to an identical copy of the entire shared database [79,81]. This raises several privacy-related considerations, such as determining who has the authority to access, read, and write data, view transactions, and create smart contracts [86]. The protection of sensitive personal information during digital network sharing is complex. Rigorous privacy-preserving protocols may hinder participants from sharing their information, yet it is essential that participants maintain control over their data [85]. In addressing these privacy challenges, AI emerges as a viable solution. For instance, the introduction of a decentralized content provider represents a novel content-selection model that augments AI's capability to offer more personalized content to users. In this model, sensitive personal data are processed locally rather than on central servers, ensuring that personal information remains private. Additionally, this approach safeguards users from invasive profiling processes typically employed by content providers. Thus, privacy and personalization are maintained through a modern, pulling-based method [19], offering a balanced approach to data protection and user experience in blockchain systems. Emerging ML paradigms like federated learning are also concrete approaches towards the same goal.

(c) Data encryption: In the domain of data security, the advantages of encrypted data over plaintext are pronounced, especially when AI and encryption algorithms are integrated [86]. As the amount of confidential personal data in blockchain systems increases, the importance of data encryption in safeguarding data privacy grows. Currently, elliptic-curve cryptography, a public key cryptographic algorithm, is prevalently used for encrypting data. This encryption method notably boosts the efficiency of intelligent systems, including swarm robotic systems. In such systems, each intelligent node utilizes public keys for secure communication across the network. This method enables nodes to target information transmission to specific recipients, with decryption possible only by nodes possessing the matching private keys [79,115].

(d) Data sharing: Data are a pivotal asset for AI, as the accuracy of AI algorithm predictions is inherently dependent on the quality and volume of the input data. However, challenges arise in the data-sharing process for AI algorithms. First, data authorization and verification become complex when multiple collaborators are involved, often leading to trust issues. Secondly, there is a risk of malicious data being distributed over the network by attackers with ulterior motives [85,89]. Blockchain technology offers a solution to these issues by providing large, trustworthy datasets for training, programming libraries, and pre-trained models for AI and ML applications. In addition, thanks to the use of cryptographic hash functions in blockchain, the integrity of data sourced from external providers can be verified [79,86]. Furthermore, blockchain enhances data sharing by introducing transparency and accountability. It controls access to confidential data, specifying who can access them and when. This mechanism assures participants of the appropriate use of their information [19]. Additionally, emerging blockchain-based data-collection methods guarantee complete maintenance and updating of data, with a verifiable record of origin [116]. This approach not only safeguards data against misuse, but also bolsters the overall integrity and reliability of the data used in AI systems.

4.2.2. Potential System

When blockchain and AI are combined, the effectiveness of the traditional systems operating based on these two technologies is also expected to be improved. This work presents nine aspects of the system ameliorated by this integration:

(a) Decentralized intelligent systems: Blockchain enhances decentralized systems and coordination platforms for AI, including methods, data, and computing power [81]. The integration of AI and blockchain aids in developing a new ecosystem of decentralized economies by utilizing the field of blockchain to enhance the dependability, security, transparency, trustworthiness, and administration of data and algorithms within AI applications [18]. Blockchain can fuel decentralized marketplaces and coordination platforms for multiple aspects of AI, as well as enhance the transparency, explainability, and trustworthiness of AI decisions. On the other hand, the functioning of a blockchain entails numerous parameters and trade-offs, encompassing considerations like security, performance, and decentralization. AI can simplify these decisions, automating and optimizing the blockchain for improved performance and enhanced governance [19]. The integration of blockchain technology with other distributed systems, such as robotic swarm systems, offers the potential to enhance the security, autonomy, flexibility, and profitability of robotic swarm operations. This combination aims to leverage the decentralized and cryptographic features of blockchain to secure data, improve decision-making autonomy within the swarm, increase operational flexibility, and potentially lead to more profitable outcomes [47]. The decentralization of swarm intelligence algorithms, where computing systems operate with autonomous components connected by a network [117,118], resonates with the principles of blockchain technology. Similarly, blockchain's decentralized nature facilitates the convenient sharing of AI training data, processes, and pre-trained models [92]. This synergy underscores a broader trend in leveraging decentralized architectures to enhance collaboration and trust within intelligent systems. AI algorithms protect data confidentiality and privacy on the blockchain. The blockchain serves as an innovative filing system for digital information, employing an encrypted, distributed ledger format to store data. The encryption and distribution of data across numerous computers create tamper-proof, exceptionally resilient databases. Access to read and update information on the blockchain is restricted to those with proper permissions, enhancing security and control [119]. Collaboration and data sharing among healthcare organizations form the bedrock of interoperability, enhanced health outcomes, and a more streamlined system. The use of blockchain to facilitate secure sharing of patient, outcome, and administrative data allows organizations to train AI models on expansive and diverse datasets without compromising privacy and security. This collaborative effort is poised to produce better trained models, yielding deeper insights, improved outcomes, and an overall more efficient healthcare industry [120]. The integration of blockchain technology into AI offers multiple benefits. Firstly, it enables data sharing with transparency and immutability, ensures the confidentiality, integrity, and authenticity of sensitive data, and encourages collaboration among participants in AI training tasks [92,107].

(b) Scalability: Traditional blockchain scalability concentrates on participant numbers. However, it also involves transaction confirmation time, validation duration, and transaction costs. These factors can restrict blockchain expansion as each chain stores limited transaction data. While data mining enhances IT system scalability, traditional mining techniques are inefficient for blockchain [121]. Modern AI along with its subdomains, like DL and federated learning, is implemented to operate on distributed data and support blockchain [80] via their integration in favor of making it more scalable and robust [19]. Conversely, blockchain technology can be costly due to additional consensus requirements and storage needs for transaction record integrity. Scalability challenges in blockchain–AI convergence require consideration [86]. Nevertheless, AI, driven by big data and advanced computing, could step up the scalability of these technologies [81].

(c) High efficiency: Organizations handle transactions involving customers, partners, and government agencies. Traditional ICT systems may struggle with high-volume, multi-business transactions and data [18,80,82], while blockchain with smart contracts, such as Decentralized Autonomous Agents (DAOs), and AI integration can automatically validate stakeholder information exchanges, enhancing system efficiency [86,121]. Multi-user business processes, which engage various stakeholders such as individual users, businesses, and government entities, inherently face inefficiencies attributed to the need for multiple parties to authorize business transactions [18]. In a blockchain network, several factors like network congestion, network routing, and network scheduling can impact a transaction validation process, especially in real-world situations where several available resources are unknown in advance. AI can be implemented to actively learn about the available resources, speed up the estimation process, and ultimately improve how well the entire system performs [80]. The integration of blockchain and AI provides efficiency advantages for storing and managing the source code of a software project on a remote server. The approach ensures public accessibility, fostering collaboration and knowledge sharing. Additionally, the persistence and decentralization inherent in blockchain contribute to a robust and resilient system, minimizing downtime and potential disruptions. The transparency provided by the blockchain ensures a clear and traceable history of modifications, enhancing accountability and reducing the likelihood of errors. Moreover, the establishment of trust within the system is significantly streamlined. That is, the decentralized nature of blockchain, coupled with AI capabilities, ensures a secure and trustworthy environment for hosting and deploying code [81].

(d) Automated decision system: AI-generated decisions can be challenging if users lack understanding or trust. Blockchain's distributed ledgers record transactions, enhancing auditing and decision transparency [122]. On the other hand, advanced ML algorithms improve AI's handling of complex situations, offering unbiased and tamper-resistant real-world considerations. In this respect, AI's data-driven decision making becomes more consistent and trustworthy [18,19,79]. Blockchain and AI integration also enables automatic transaction data handling, while AI-assisted online learning enhances blockchain algorithms [80].

(e) Collective decision making: Centralized systems require coordinated node processing for collective goals, often involving a third party. Blockchain eliminates this need, allowing nodes to autonomously decide. Voting techniques in blockchain improve decentralized decision-making in AI, especially ML as a subdomain of

AI. AI activities like model construction and training are recorded on blockchain, providing a highly trustable, unalterable data-sharing system [85].

(f) System security: Blockchain security focuses on application layer vulnerabilities and encryption methods [19,80]. ML-driven intrusion detection and prevention systems may also address application layer vulnerabilities, among others [80]. Namely, swarm intelligence, a computational intelligence technique, can be used to improve intrusion detection effectiveness [80,123], while computational intelligence models can ameliorate encryption robustness, bolstering blockchain resilience [79,80,91]. ML in blockchain detects attacks and either protects systems or blocks attacks from spreading [19]. However, security stability is a concern, as integrating secure and insecure systems might compromise one or more qualities of the confidentiality, integrity, availability (CIA) triad [86].

(g) Sustainability: AI algorithms manage resources in sustainable, large-scale distributed systems like electric power. These systems share characteristics with blockchain and microeconomics, both featuring decentralized computation platforms [7,80]. Nevertheless, microeconomics face challenges in managing limited resources for unlimited needs. Blockchain–AI integration can support sustainability in microeconomic systems, considering large-scale system aspects.

(h) Transparency system: Data collection in ML requires trustworthy user interfaces. Blockchain ensures source code execution on local nodes without third-party servers [86], managing user contributions and activities for transparency [79]. AI decision systems require traceability, auditability, and explainability for transparency [124]. Recording AI decision processes on blockchain enhances transparency and user trust [122]. Audit trails and decision-making processes in blockchain improve traceability [80]. Nevertheless, auditability in blockchain, focusing on data storage and transactions, requires further research for enhanced transparency [125].

4.2.3. Hardware Issues

(a) Device cooperation: Blockchain–AI integrated systems involve untrusting devices like IoT devices and swarm robotics. These devices collaboratively make decisions [116]. Blockchain can act as a coordination system backbone, although vulnerable to attacks [19]. Traditional security systems respond to attacks by shutting down compromised nodes centrally. On the other hand, blockchain technology offers an automatic, decentralized solution, shutting down compromised nodes individually [19].

(b) Mining hardware design: Specialized hardware is crucial for smooth blockchain functioning. Traditional computer hardware separates components like the CPU, memory, storage, and buses. Neuromorphic computing technology, inspired by the human brain, aims to develop machines capable of learning and logical processing [117]. Neural-inspired hardware [117,118] and spike-timing-dependent plasticity models [80] are such examples. Current data mining is energy-intensive [126]. This can be alleviated through the use of ML in data centers for managing energy usage. If so, according to the work by [119], energy consumption can be reduced by 40% or more. Similar approaches could optimize mining hardware energy efficiency [126].

4.3. Application Era

As already pointed out, the convergence of blockchain and AI has heralded a new era of technological innovation, with the amalgamation of these disruptive technologies poised to make a substantial impact across various sectors. From finance and healthcare to communication and network security, the integration of blockchain and AI is transformative. With reference to Section 3 and Figure 3, while reviewing this topic, we identified seven key areas that reap significant advantages from this integration. These areas encompass IoT applications, cybersecurity, energy, smart cities, finance, healthcare, and big data manipulation, highlighting the broad and diverse benefits of merging blockchain and AI technologies. For brevity reasons, the following subsections elaborate on the first five of the aforementioned focus areas, also referring to key publications per focus area.

4.3.1. IoT Applications

The Internet of Things has revolutionized the way data are connected and transformed between physical and virtual entities. Traditional IoT systems, operating on centralized architectures, face challenges like single points of failure and concerns regarding the security, transparency, privacy, integrity, and confidentiality of data [47,127,128]. These challenges have the potential to hinder the future development and application of IoT technology. For instance, as also detailed in the following, transitioning the IoT to an intelligent distributed ledger system offers a multitude of benefits.

The fusion of blockchain, AI, and the IoT is a focal point of contemporary research. Rouwer and Borda [129] introduced NeuRoNt, a system based on Ethereum blockchain technology, utilizing smart contracts at the edge layer to enable complex problem-solving by multiple agents. Rahman et al. [130] proposed a mobile edge-sharing system on Ethereum platforms and smart contract technology for service sharing among IoT devices, applicable to smart city systems. Rathore et al. [131] developed the BlockDeepNet framework, integrating DL algorithms, blockchain, and smart contracts to manage IoT network data, ensuring the security of local and global learning updates in DL algorithms through blockchain.

Moreover, Alrubei et al. [132] designed a Distributed Artificial Intelligence (DAI) platform to enhance IoT architectures, tested using low-cost IoT devices and demonstrating high accuracy. Singh et al. [133] combined the IoT architecture with blockchain and AI to improve big data analysis, with their architecture centering on the performance improvement over previous models, considering accuracy, latency, security, privacy, computational complexity, and energy cost. Alrubei et al. [134] introduced a framework combining edge computing, AI algorithms, IoT end-devices, and blockchain for monitoring IoT ecosystems and predicting outcomes (such as COVID-19 spread) before disseminating the results on a public blockchain.

The diversity of IoT devices, the massive data generated, the unstructured data processing, and data security are key challenges in the industrial cyber–physical cybersecurity realm [135,136]. Latif et al. [137] developed a new architecture for IoT ecosystems, enhancing security and energy efficiency by integrating Software-Defined Networking and blockchain. This model aims to reduce energy consumption, improve data transfer efficiency, and decrease latency. However, deep research into energy management and system security remains a primary challenge for the next generation of industrial cyber–physical cybersecurity.

4.3.2. Cybersecurity

Cybersecurity is becoming increasingly critical for various sectors, including government organizations and private enterprises. The rapid escalation of cyberattacks and emerging legislation demand enhanced data-protection measures [138,139]. Blockchain and distributed ledger technology offer novel solutions for safeguarding information in both decentralized and centralized network systems [140]. Concurrently, AI enhances system security and personal data protection, also aiding in improving dataset quality and analytical model processing [19]. Nonetheless, the integration of AI and blockchain in cybersecurity necessitates well-defined operational guidelines and control mechanisms.

Wang et al. [17] introduced a robust tool for network system protection, combining blockchain technology with AI algorithms. This system ensures the safety and protection of data transmitted across network systems by various users. Deebak and AL-Turjman [141] developed privacy-preserving smart contracts based on blockchain and an AI framework called PPSC-BCAI. This model streamlines human–computer interaction, system activity monitoring, cybersecurity risk assessment, and fraudulent claim detection. Kim and Park [142] designed a data-preserving AI system to verify learning data integrity using blockchain technology, centering on data confidentiality and integrity in AI learning data monitoring and verification. Last but not least, Liang et al. [143] proposed a mechanism to detect cyberattacks in blockchain systems, employing data fusion techniques to match user behaviors with data characteristics. This model enhances traditional anomaly intrusion detection by classifying clustering characteristics in abnormal blockchain networks.

In the advent of Industry 5.0, the industrial sector has evolved significantly, adopting advanced devices and technologies to meet growing demands and enhance product quality. However, this diversity in both information technology (IT) and Operational Technology (OT) systems increases the attack surface, augmenting susceptibility to cyberattacks, including data leaks, Distributed Denial of Service (DDoS), and Advanced Persistent Threats (APTs). In addressing these challenges, the integration of blockchain and AI emerges as a promising solution. For instance, Rahman et al. [144] developed a system capable of detecting APTs at the edge of IoT nodes and recording attack information in an immutable blockchain ledger, fostering trust in industrial network systems. Such approaches represent a significant step forward in reinforcing cybersecurity in the industrial environment.

4.3.3. Energy

Intelligent energy systems are evolving towards decentralization and efficiency, yet the financial mechanisms supporting these systems often remain centralized and reliant on third-party services [145]. Blockchain technology is revolutionizing this paradigm by digitizing physical currencies, enabling direct energy transactions between consumers and suppliers. This advancement allows energy suppliers to efficiently monitor transactions within a distributed environment at lower costs. Additionally, the integration of AI in energy sectors enhances the processing of complex tasks and uncertain parameters, such as predicting energy demand or assessing reliable business partners [145].

Kumar et al. [146] explored the application of AI, the IoT, and blockchain in the energy sector, addressing distributed environments, power electronics, electric vehicles, and cybersecurity. Their study examined AI analytics, the IoT in energy Internet systems, and blockchain for smart grid services' enhancement, concluding that this integration transforms traditional grids into automated, reliable, sustainable, and secure distributed services. Moreover, Xiao et al. [147] introduced a natural gas output prediction model using the Temporal Pattern Attention Long Short-Term Memory (TPA LSTM) algorithm, integrating blockchain for transaction security and real-time accuracy in matching dynamic pricing. Moreover, Mylrea [148] proposed the Distributed Autonomous Energy Organizations (DAEOs) model to link energy suppliers and consumers, enhancing the efficiency of energy generation, consumption, and transfer processes.

4.3.4. Smart Cities

The concept of a smart city in the modern information age involves harnessing cutting-edge technologies to improve efficiency and sustainability. On the other hand, as already pointed out, blockchain technology plays a key role in transitioning traditional systems into digitally intelligent urban environments, finding applications in diverse sectors like supply chains, finance, the IoT, and cybersecurity. The synergy of blockchain and AI significantly enhances smart city networks, making them more effective and sustainable [83].

Rahman et al. [130] introduced a blockchain-based infrastructure to bolster security and privacy in smart contract services for IoT devices in smart cities. This framework, combining AI and blockchain, ensures secure data transfer for IoT devices using cyber–physical sharing economy services, defining a new generation of smart city systems. It facilitates complex service provision on a global blockchain level without needing a certificate authority for user authentication. Moreover, Ren et al. [149] implemented blockchain as a decentralized technology in intelligent traffic models, allowing vehicle-to-vehicle information sharing without a central authority. This P2P approach ensures direct node connectivity for right-of-way acquisition, with lane property rights and consensus achieved through smart contracts.

Instead of focusing on applying blockchain and AI to improve traditional technology systems, Pandey et al. [150] investigated the application of blockchain and AI to solve environmental pollution. The rapid growth of the world population directly pushes the environment into damage, especially waste pollution. To deal with this challenge, ML techniques and blockchain technology were combined to classify the waste objects or products, providing recommendations to the user on how to reuse or recycle those waste objects or products. The developed approach was broadcast on a website, providing easy access to the end-user.

4.3.5. Finance

The present subsection sheds light on how converging blockchain and AI technologies may act in favor of the improvement of smart contracts in real-life scenarios. The concept of smart contracts was initially introduced by Nick Szabo in 1994 [19], gaining prominence with the advent of blockchain technology [149]. Smart contracts are computer programs capable of self-enforcing and self-verifying the terms set within them. They enable complex solutions and behaviors to be executed accurately and automatically, controlling blockchain system functions via software without the need for trusted third-party authorities [151]. Blockchain and smart contract technology have developed into sophisticated digital infrastructures for distributed storage, trustless economies, and disintermediation networks, characterized by trustlessness, traceability, self-governance, and tamper resistance [152–154]. However, technical vulnerabilities in blockchain that could be exploited have been identified [155,156]. That is, smart contracts facilitate automatic P2P transactions when predefined conditions are met, requiring blockchain consensus mechanisms for execution. The public accessibility of smart contract codes allows system participants to scrutinize every line of code, but this openness can create security vulnerabilities that AI could help mitigate.

In AI research, machine cooperation and agent collaboration are key focuses [151]. Various AI algorithms support nodes in collaborative operations by sharing information, mechanisms, and resources within network systems. Ensemble learning, for example, enables collaboration between nodes for extracting high-quality data features [157], and distributed DL accelerates AI model training using multiple Graphics Processing Units (GPUs) [158]. However, the proliferation of IoT and edge computing has led to data creation by decentralized devices, challenging centralized AI architectures with data privacy and network resource issues. Therefore, distributed AI collaboration and smart contract technology have become vital for scalability and collaboration in decentralized AI networks.

Ouyang et al. [151] introduced the Learning Markets model for decentralized AI collaboration. This model utilizes blockchain technology for trustless collaboration and transaction security, with smart contracts controlling software-defined agents for marketing operations and scalability management. LM encourages participation in collaborative mining and creates an auditable, traceable AI market for trading trusted models, addressing challenges in data, resources, and models. Moreover, Wang et al. [152] proposed a six-layer architecture for smart contracts, covering infrastructure, contracts, operations, intelligence, manifestations, and applications. In more detail, their framework addresses the smart contract lifecycle stages, including negotiation, development, deployment, maintenance, learning, and self-destruction, offering a research and development guideline.

In addition, the collaboration of AI with other cutting-edge technologies might not be as strong or frequent because it is still in the process of development. However, even if the occurrence of AI and the mentioned technologies together may not be highly frequent, the practical outcomes and advantages gained from integrating AI with these technologies are substantial. Technologies like blockchain and immersive environments (augmented reality, digital twin, virtual reality) have the potential to be effectively integrated with AI. This integration could lead to innovative and efficient solutions by combining the strengths of these technologies in various applications and industries. For instance, digital twins have the capability to conduct analyses and simulations in virtual environments, creating new data associated with physical production processes. Subsequently, AI can use this information to construct predictive models aimed at optimizing production efficiency. Moreover, blockchain, with its distributed ledger technology, can serve as a reliable source of data for ML activities. The immutability, transparency, and visibility of data on the blockchain render it suitable for training ML models and supporting decision-making processes. Additionally, the trustworthy nature of blockchain data allows for the automation of certain operations, contributing to efficiency and reliability in various processes [159].

In the context of Industry 4.0 and beyond, AI and blockchain technology are integral components among several cutting-edge technologies such as the IoT, autonomous vehicles, and virtual reality. Together, these technologies are driving advancements in efficiency, flexibility, and innovation within industrial processes. The integration and collaboration of these technologies create smarter, interconnected, and automated systems, characterizing the Industry 4.0 paradigm [159]

Addressing the static nature of blockchain-generated smart contracts and the limitations of AI in prediction integrity, Badruddoja et al. [160] proposed a Naive Bayes prediction technique for enhanced predictive performance within blockchain smart contracts. This model aims to synergize AI and blockchain, leveraging their strengths to create a decentralized ML framework, enhancing security, automation, and system dynamism. This approach opens new possibilities for AI decentralized applications based on blockchain technology.

5. Discussion

As already pointed out in Section 4, the integration of AI and blockchain is reshaping numerous sectors, offering novel solutions and posing new challenges. In healthcare, AI's predictive analytics combined with blockchain's secure data management is revolutionizing patient care and record keeping. Finance sees the emergence of smart contracts, while cybersecurity benefits from enhanced security controls. This transformative impact signifies a shift in how technology addresses complex problems, yet it also brings forth new questions and considerations, particularly in terms of scalability, interoperability, and governance.

AI-powered blockchain solutions offer unprecedented transparency, security, and efficiency, revolutionizing sectors such as supply chain management, finance, and healthcare [161]. These technologies enable automated decision making, smart contracts, and DAOs, paving the way for new business models and collaborations. Governments are also exploring the integration of AI and blockchain to bolster data security, streamline administrative processes, and foster digital identity initiatives [162,163]. Moreover, the World Economic Forum has emphasized the transformative impact of AI and blockchain on the future of work, predicting the creation of 58M net new jobs by 2025 [164]. This synergy between AI and blockchain technologies signifies a profound shift towards decentralized, AI-driven economies, promising immense opportunities for innovation and growth.

Overall, the critical synthesis of recent survey and research papers performed in the context of the current article reveals significant advancements and challenges in the AI and blockchain domain. This overview not only highlights technological progress, but also identifies potential areas for future research. It is evident that, while strides have been made in understanding and applying these disruptive technologies, there remains a vast landscape of unexplored territory. In this respect, this synthesis serves as a roadmap for scholars and practitioners, outlining key areas where further exploration and innovation are both needed and promising.

In line with the objective of aiding researchers in this field, new theoretical models based on the insights from the systematic survey are proposed. These models are designed to encapsulate the complexities of AI and blockchain convergence, addressing both theoretical and practical aspects. They encourage innovative thinking and experimentation, potentially paving the way for breakthroughs in application and understanding.

As a prominent example, Table 2 serves as a pivotal conduit between theoretical constructs and practical applications, elucidating the intersections of AI and blockchain technology within the cryptocurrency ecosystem, illustrating the practical application of theoretical concepts examined through this overarching survey work. That is, each project in Table 2 is categorized based on different key attributes, including market cap, blockchain type, blockchain layer, service(s), and consensus. Notably, this variety of projects showcases the integration of AI with blockchain technology, offering innovative solutions across various sectors.

Table 2. Overview of real-life AI–blockchain projects.

Token	Market Cap	Blockchain Type	Layer	Service(s)	Consensus
AGI	USD 35.4M	Ethereum	Layer 3	Decentralized AI Services Marketplace	PoS on Ethereum, exploring dPoS on Cardano
ENJ	USD 5.12B	Ethereum	Layer 3	NFT Ecosystem, Gaming Integration	PoS
HBAR	$5.97B	Hedera Hashgraph	Layer 1	Decentralized Consensus and Smart Contracts	aBFT
RNDR	$4.15B	Solana	Layer 1	Decentralized GPU Rendering and AI Computation	PoH, Solana's unique consensus mechanism
FET	$175M	Cosmos	Layer 1	Decentralized Network of Autonomous Agents for AI	PoS
AGIX	$1.49B	Multi-chain	Layer 3	Decentralized AI Services Marketplace	PoS on Ethereum, exploring dPoS on Cardano
OCEAN	$631M	Ethereum	Layer 3	Decentralized Data Exchange	PoS
FIL	$5.26B	Filecoin	Layer 1	Decentralized Storage Network	PoRep
LINK	$12.26B	Ethereum	Layer 3	Decentralized Oracle Network	Not directly applicable; utilizes external data validation by decentralized oracles
CTXC	$102M	Cortex	Layer 1	AI on Blockchain	Not specified; focuses on on-chain AI execution
TAO	N/A	Bittensor	Layer 3	Decentralized ML	PoI
RLC	$149M	Ethereum	Layer 3	Decentralized Cloud Computing	PoS
GLM	$93.5M	Ethereum	Layer 3	Decentralized Data Marketplace	PoS
ICP	$3.99B	Internet Computer	Layer 1	Decentralized Internet	Threshold Relay (PoW-based)
CGPT	N/A	Ethereum	Layer 3	AI Language Model Utility	PoS
AKT	$97.6M	Cosmos	Layer 1	AI-Based Investment Management	PoS
THETA	$2.98B	Theta Network	Layer 1	Decentralized Video Streaming	Multi-level BFT consensus (PoS-based)
AIOZ	N/A	Ethereum	Layer 3	Decentralized Video Streaming	PoS
MANA	$2.91B	Ethereum	Layer 3	Virtual Reality Platform	PoS
GNT	N/A	Ethereum	Layer 3	Decentralized Computing Power Marketplace	PoS
NU	$379M	Ethereum	Layer 3	Decentralized Encryption and Privacy	PoS
DAGT	N/A	Ethereum	Layer 3	Decentralized Ecosystem	PoS

With reference to Table 2, there is a wide range of AI applications combined with blockchain, including decentralized marketplaces, data exchange platforms, and autonomous agents, demonstrating blockchain's capacity to support diverse AI applications. The variation in consensus algorithms and governance models reflects continuous innovation aimed at optimizing processes. The assortment of blockchain types and layers used by these projects signifies the evolving complexity of blockchain ecosystems and the development of platforms for specific applications. In summary, the above-mentioned table provides a concise view of the current innovations at the AI–blockchain nexus, indicating a dynamic and rapidly advancing field. Furthermore, the variety of different types and layers of blockchain used by these projects reflects the growing sophistication of blockchain ecosystems and the emergence of specialized platforms designed to meet specific needs.

Looking ahead, in Section 6, the article at hand outlines potential future research trajectories in the dynamic landscape of AI and blockchain. Emerging areas within this convergence, ripe with opportunities for innovative research and development, are highlighted. This forward-looking perspective aims to inspire, guide, and propel ongoing research efforts, illuminating new directions in this rapidly evolving technological realm. That is, the inclusion of this comprehensive exploration significantly contributes to the academic discourse surrounding AI and blockchain convergence. By providing a thorough analysis, proposing new theoretical models, and highlighting future research avenues, this article reaffirms its commitment to advancing understanding and exploration in this multifaceted field. Overall, as already mentioned, the present work stands as a guiding resource for researchers, enriching the collective knowledge and sparking further innovation in the convergence of AI and blockchain technologies.

6. Challenges and Open Research Issues

The integration of blockchain and AI, currently in a rather early phase, presents numerous benefits and challenges. This section discusses the significant challenges and open issues related to this integration, addressing how they impact various aspects of technology and society. We split this discussion into 10 axes, as detailed below:

(a) Data operation: Data operation in computing systems involves analysis, processing, storage, and representation, while in the real world, data are often grouped as objects or object lists. A key challenge is tracking each data piece through computational architectures, where boundaries among data elements may become blurred, leading to inaccurate data sharing [81]. Restructuring lower levels of computing architectures is essential to differentiate between variable-sized data elements. The semantic information method, an emerging solution, requires further investigation [165]. Additionally, blockchain–AI models risk being dominated by low-quality or fake data from affluent or rogue autonomous agents [82]. Financial and non-financial incentives have been suggested to encourage high-quality data submission [134], though high transaction fees remain a barrier. Ambiguous data also pose challenges, necessitating the integration of advanced technologies like natural language processing and DL for accurate interpretation [82].

(b) Privacy: While public ledgers in cryptocurrencies offer data security and authentication, they lack privacy due to their open-access nature. Conversely, private blockchain ledgers employ cryptographic methods and access control algorithms to secure data, but potentially limit the data available for AI processing [18]. Balancing transparency with privacy is crucial, but not straightforward. Future research should concentrate on designing privacy policies that support transparency, enforcing policies to address privacy issues, and developing effective user authentication techniques [81]. Moreover, considerations should extend to security, scalability, and availability. Technologies like tamper-evident logging and advanced database security could enhance blockchain–AI mechanisms [81].

(c) System scalability: Blockchain scalability, determined by data storage and transaction rates, often conflicts with the storage needs of AI algorithms for training data and transactions [85]. Current well-known blockchain systems, like Bitcoin and Ethereum, have limited transaction capacities, which are insufficient compared to the needs of platforms like Facebook or applications like smart grids [18,85]. Solutions like sharding and sidechain aim to improve blockchain efficiency by facilitating transactions outside the main chain and revamping consensus algorithms [166,167]. The emergence of new, more efficient consensus mechanisms like Graphchain and Algorand offers promise, but further research is needed to enhance system scalability [168,169]. As big data evolve and computing systems develop, blockchain must adapt to become more scalable, distributed, and heterogeneous, requiring sophisticated data management and transparency policies [81]. No less important, the integration of AI with blockchain holds potential for advanced data analytics and automated decision making within secure blockchain networks. However, this convergence presents challenges, including scalability and computational demand. AI can optimize blockchain operations and improve transparency in automated processes, but ethical and practical implications must be considered to ensure fairness and efficiency.

(d) Blockchain security: Despite blockchain's reliable security mechanisms, research [20,170] indicates that blockchain systems are susceptible to cyberattacks, with a significant vulnerability rate. Additionally, consensus mechanisms relying on miners' hash rates could centralize decentralized systems, particularly in public blockchains like Ethereum or Bitcoin [18]. To address this, technologies like Intel SGX [171] have been developed, integrating specific hardware to enhance Trusted Execution Environments (TEEs). Nevertheless, this area requires further research to bolster the efficacy of blockchain–AI technology. Some practitioners have investigated the combination of TEEs and blockchains to maintain confidentiality and privacy within smart contracts [172,173]. Note that the TEE is a secure section within the main processor, dedicated to safeguarding sensitive data. This isolated environment, known as an enclave, ensures that confidential information can be stored, processed, and safeguarded [174]. There have been various instances of TEEs; one specific example is Intel Software Guard Extensions (SGX) [175]. The implementation of Intel's new SGX trusted hardware enables an authenticated data feed system acting as a bridge between smart contracts and existing websites to deliver datagrams with a significant level of reliability and trustworthiness [174].

(e) Smart contract security: Smart contracts should be devoid of errors and vulnerabilities to prevent cyberattacks. For instance, the Ethereum-based Decentralized Autonomous Organizations (DAOs) were compromised in 2016 due to code vulnerabilities, resulting in significant Ether losses [18,81]. Addressing these issues requires better blockchain engineering and coding practices in programming languages like Solidity and Chaincode. Developing tools for vulnerability assessment in smart contracts is critical [156,160,176]. Additionally, deterministic outcomes in smart contracts could impact decentralized AI algorithms, necessitating new approaches for predictable outcome mechanisms and consensus protocol redesign [18].

(f) Decentralized oracle in smart contracts: Smart contracts rely on external functions for execution, often requiring third-party oracles. This reliance could centralize decentralized systems, contradicting blockchain's advantages [177]. Solutions like Chainlink aim to bridge this gap, but further development is needed to meet individual and business needs.

(g) Emergence of fog computing: Fog computing extends cloud computing capabilities to edge networks. In autonomous vehicles, for example, blockchain can secure high-integrity AI-processed data, with fog computing enhancing system speed [121]. Kumar et al. [178] proposed securing smart contracts in blockchain–IoT systems using AI algorithms and fog computing for DDoS attack detection. Nevertheless, the application of fog computing in blockchain still faces challenges like automated billing and charging in self-driving trucks, necessitating intelligent systems for user authentication and authorization [121].

(h) System governance: Managing blockchain systems with multiple users poses governance challenges: Who administers and maintains the systems, deploys nodes, creates smart contracts, resolves disputes, selects oracles, and operates off-chain activities? These questions open research opportunities for developing effective governance models [18,81].

(i) Cryptocurrency transaction fee: Blockchain services like Bitcoin and Ethereum require transaction fees [31,179,180]. Third parties may absorb these fees to encourage user participation, but the trustworthiness and efficacy of their validation algorithms remain a concern.

(j) Standards, interoperability, and regulation requirements: Formal standards for blockchain technology are yet to be established. Organizations like IEEE, ITU, and NIST are working on standards for blockchain interoperability and infrastructure [181,182]. Recommendations, regulations, and policies are needed to support blockchain applications and prevent misuse. Developing new models and mechanisms for AI algorithms, especially in public blockchain platforms dealing with financial transactions and digital money, is an emerging challenge that calls for further exploration.

7. Conclusions

The comprehensive meta-survey on the convergence of blockchain technology and AI, undertaken in this work, yields significant insights and findings that underscore the metamorphic potential of this integration across various domains. We analyzed a wide range of research papers, leading to a deeper understanding of how the fusion of these two technologies is reshaping traditional systems and introducing innovative features. Altogether, the most notable takeaways from our review of the pertinent literature can be summarized as follows.

- Identification of major trends: Our analysis revealed prominent trends in the application of blockchain and AI technologies operating in tandem, highlighting their impact on enhancing data security, privacy, and efficiency in systems ranging from IoT applications to financial services.
- Emergence of novel features: The integration of blockchain and AI has led to the emergence of novel features and functionalities. These have been categorized into three primary groups: data manipulation, potential system, and hardware issues, each consisting of various sub-characteristics that collectively contribute to the robustness and versatility of the resulting fused technology.
- Application across sectors: A detailed analysis of the diverse applications of blockchain/AI-based technology was offered. It indicatively underscored how the synergy of blockchain and AI is not only enhancing existing systems, but also paving the way for new applications, particularly in improving smart contract capabilities.
- Challenges and future research directions: A key aspect of this work was identifying the challenges and potential research areas. Specifically, it highlighted the need for further exploration in scalability, security, and the development of more efficient and interoperable systems within the fused blockchain/AI domain.

Altogether, the paper at hand has demonstrated that the convergence of blockchain and AI holds immense promise for revolutionizing various sectors. It provides a roadmap for future research and development efforts, guiding researchers and practitioners towards leveraging these technologies' full potential.

The exploration of AI-designed blockchains, the enhancement of smart contract security, and the development of AI-agent-based smart contracts, alongside the adoption of modern governing models such as DAOs, underscores the urgent need for empirical research studies. These studies are crucial for rigorously testing the integration of AI with blockchain technology, underscoring the indispensable role of interdisciplinary collaboration. Additionally, they spotlight the necessity of weaving in legal frameworks and recognizing the interconnectedness of the cyber–physical ecosystem to adeptly address complex challenges. This holistic approach emphasizes the importance of not only advancing technological synergies, but also ensuring that these advancements are underpinned by robust legal structures and are seamlessly integrated into the fabric of our digital and physical environments, navigating the nuances of both realms effectively. We aspire that the insights gathered from this study will contribute to the ongoing discourse in the field, laying the groundwork for future innovations and advancements in blockchain and AI integration.

Author Contributions: Conceptualization, D.B., D.D. and R.B.; methodology, D.B., D.D., C.S. and G.K.; validation, G.K., C.S. and D.D.; formal analysis, G.K.; investigation, D.B. and C.S.; resources, D.B. and C.S.; writing—original draft preparation, D.B. and D.D.; writing—review and editing, C.S., G.K. and R.B.; visualization, D.B. and C.S.; supervision, G.K. and C.S.; project administration, G.K. and C.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are not contained within the article.

Acknowledgments: The authors would like to thank the anonymous reviewers for their constructive criticism and valuable comments towards improving the quality of this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Satoshi, N. A peer-to-peer electronic cash system. *Bitcoin* **2008**, *4*, 2. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 2 February 2022).
2. Tripathi, G.; Ahad, M.A.; Casalino, G. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decis. Anal. J.* **2023**, *9*, 100344. [CrossRef]
3. Chaum, D. Blind Signatures for Untraceable Payments. In Proceedings of the Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, CA, USA, 23–25 August 1982; Chaum, D., Rivest, R.L., Sherman, A.T., Eds.; Plenum Press: New York, NY, USA, 1983; pp. 199–203. [CrossRef]
4. Turing, A.M. Computing Machinery and Intelligence. In *The Philosophy of Artificial Intelligence*; Boden, M.A., Ed.; Oxford Readings in Philosophy; Oxford University Press: Oxford, UK, 1990; pp. 40–66.
5. Vijayakumar, H. Impact of AI-Blockchain Adoption on Annual Revenue Growth: An Empirical Analysis of Small and Medium-sized Enterprises in the United States. *Int. J. Bus. Intell. Big Data Anal.* **2021**, *4*, 12–21.
6. Wang, Z.; Li, M.; Lu, J.; Cheng, X. Business Innovation based on artificial intelligence and Blockchain technology. *Inf. Process. Manag.* **2022**, *59*, 102759. [CrossRef]
7. Xuan, T.R.; Ness, S. Integration of Blockchain and AI: Exploring Application in the Digital Business. *J. Eng. Res. Rep.* **2023**, *25*, 20–39. [CrossRef]
8. Wood, G. A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
9. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.Y.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2020**, *8*, 4157–4185. [CrossRef]
10. Feng, J.; Yu, F.R.; Pei, Q.; Du, J.; Zhu, L. Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4321–4334. [CrossRef]
11. Sam, K. Vitalik Buterin Says Developers Should Tread Carefully Mixing Crypto and AI. 2024. Available online: https://www.coindesk.com/tech/2024/01/30/vitalik-buterin-says-developers-should-tread-carefully-mixing-crypto-and-ai/ (accessed on 2 May 2024).
12. Hussein, Z.; Salama, M.A.; El-Rahman, S.A. Evolution of blockchain consensus algorithms: A review on the latest milestones of blockchain consensus algorithms. *Cybersecurity* **2023**, *6*, 30. [CrossRef]
13. Markets-Store, R. Global Blockchain in Telecom Market by Provider (Application Providers, Infrastructure Providers, Middleware Providers), Organization Size (Large Enterprises, SMEs), Application—Forecast 2024–2030. Available online: https://www.researchandmarkets.com/report/telecommunication-blockchain#rela3-5025113 (accessed on 1 March 2024).
14. Singh, R.; Gill, S.S. Edge AI: A survey. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 71–92. [CrossRef]
15. Brcic, M.; Yampolskiy, R.V. Impossibility Results in AI: A Survey. *ACM Comput. Surv.* **2023**, *56*, 1–24. [CrossRef]
16. Bughin, J.; Seong, J.; Manyika, J.; Chui, M.; Joshi, R. Notes from the AI frontier: Modeling the impact of AI on the world economy. *McKinsey Glob. Inst.* **2018**, *4*, 1–64
17. Wang, K.; Dong, J.; Wang, Y.; Yin, H. Securing data with blockchain and AI. *IEEE Access* **2019**, *7*, 77981–77989. [CrossRef]
18. Salah, K.; Rehman, M.H.U.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for AI: Review and open research challenges. *IEEE Access* **2019**, *7*, 10127–10149. [CrossRef]
19. Dinh, T.N.; Thai, M.T. AI and blockchain: A disruptive integration. *Computer* **2018**, *51*, 48–53. [CrossRef]
20. CryptoBlogs. AI Crypto Projects. 2023. Available online: https://www.cryptoblogs.io/ai-crypto-projects (accessed on 1 July 2023).
21. Shafay, M.; Ahmad, R.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Omar, M. Blockchain for deep learning: Review and open challenges. *Clust. Comput.* **2023**, *26*, 197–221. [CrossRef] [PubMed]
22. Breda. Blockchain and Banking Efficiency: Global Evidence from Ripple Network Adoption. 2023. Available online: http://essay.utwente.nl/94787/ (accessed on 1 July 2023).

23. Franchina, L.; Carlomagno, G. A Comparison Between SWIFT and Blockchain from a Cyber Resiliency Perspective. In *Proceedings of the Critical Information Infrastructures Security*; Nadjm-Tehrani, S., Ed.; Springer: Cham, Switzerland, 2020; pp. 149–160.
24. Schäffer, M.; di Angelo, M.; Salzer, G. Performance and Scalability of Private Ethereum Blockchains. In *Proceedings of the Business Process Management: Blockchain and Central and Eastern Europe Forum*; Di Ciccio, C., Gabryelczyk, R., García-Bañuelos, L., Hernaus, T., Hull, R., Indihar Štemberger, M., Kő, A., Staples, M., Eds.; Springer: Cham, Switzerland, 2019; pp. 103–118.
25. Choi, W.; Hong, J.W.K. Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper. In Proceedings of the 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), Virtual, 8–10 September 2021; pp. 325–329. [CrossRef]
26. Cao, L. Decentralized AI: Edge Intelligence and Smart Blockchain, Metaverse, Web3, and DeSci. *IEEE Intell. Syst.* **2022**, *37*, 6–19. [CrossRef]
27. Tyagi, A.K.; Dananjayan, S.; Agarwal, D.; Thariq Ahmed, H.F. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. *Sensors* **2023**, *23*, 947. [CrossRef]
28. Girdhar, K.; Singh, C.; Kumar, Y. AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda. In *Blockchain for Cybersecurity in Cyber-Physical Systems*; Maleh, Y., Alazab, M., Romdhani, I., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 185–213. [CrossRef]
29. Jiang, E.; Qin, B.; Wang, Q.; Wang, Z.; Wu, Q.; Weng, J.; Li, X.; Wang, C.; Ding, Y.; Zhang, Y. Decentralized Finance (DeFi): A Survey. *arXiv* **2023**, arXiv:2308.05282.
30. Ghosh, P.K.; Chakraborty, A.; Hasan, M.; Rashid, K.; Siddique, A.H. Blockchain Application in Healthcare Systems: A Review. *Systems* **2023**, *11*, 38. [CrossRef]
31. CoinMarketCap: Cryptocurrency Prices, Charts and Market Capitalizations. Available online: https://coinmarketcap.com (accessed on 14 March 2024).
32. Indian State Governments Spur Blockchain Adoption in Public Administration. Available online: https://cointelegraph.com/news/indian-state-governments-spur-blockchain-adoption-in-public-administration (accessed on 28 September 2023).
33. State of Enterprise Blockchain Adoption 2023. Available online: https://www.casperlabs.io/blog/the-state-of-enterprise-blockchain-adoption-in-2023 (accessed on 28 September 2023).
34. European Central Bank. Eurosystem Proceeds to Next Phase of Digital Euro Project, 2023. Available online: https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html#:~:text=The%20digital%20euro%20would%20fill,digital%20euro%20platform%20and%20infrastructure (accessed on 28 September 2023).
35. World Economic Forum. EU Unveils Plans for Digital Euro, Promising Complete Privacy, 2023. Available online: https://www.weforum.org/agenda/2023/08/digital-euro-is-coming-privacy/ (accessed on 28 September 2023).
36. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, LA, USA, 22–25 February 1999; pp. 173–186.
37. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In Proceedings of the International Workshop on Open Problems in Network Security, Zurich, Switzerland, 29 October 2015; pp. 112–125.
38. Belchior, R.; Vasconcelos, A.; Correia, M.; Hardjono, T. Enabling Cross-Jurisdiction Digital Asset Transfer. In Proceedings of the 2021 IEEE International Conference on Services Computing (SCC), Virtual, 5–11 September 2021; pp. 431–436. [CrossRef]
39. Maurer, B. The social life of money in the digital age. *Annu. Rev. Anthropol.* **2013**, *42*, 497–516.
40. Rhodes, R. *Internet Governance: The New Frontier of Global Institutions*; Routledge: London, UK, 2017.
41. Walch, A. Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems. In *Crypto Assets: Legal and Monetary Perspectives*; Oxford University Press: Oxford, UK, 2020; pp. 23–43.
42. Catalini, C.; Gans, J.S. The Digital Economy: Implications for Financial Services and Payments. *J. Econ. Perspect.* **2020**, *34*, 22–48.
43. Hawlitschek, F.; Notheisen, B.; Teubner, T. The Limits of Trust-Free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy. In *Proceedings of the Electronic Commerce Research and Applications*; Elsevier: Amsterdam, The Netherlands, 2020; Volume 29, pp. 50–63.
44. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385. [CrossRef]
45. Community, E. The DAO Incident and Ethereum Hard Fork. 2016. Available online: https://ethereum.org/en/history/#dao-fork-summary (accessed on 10 April 2024).
46. Team, B.D. Segregated Witness and Its Impact on Bitcoin. 2017. Available online: https://bitcoin.org/en/segwit_wallets (accessed on 10 April 2024).
47. Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. *Big Data Cogn. Comput.* **2020**, *4*, 28. [CrossRef]
48. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.
49. Solat, S.; Calvez, P.; Naït-Abdesselam, F. Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice. *J. Softw.* **2021**, *16*, 95–106. [CrossRef]
50. Wang, Z.; Xiong, X.; Knottenbelt, W.J. Blockchain Transaction Censorship: (In)secure and (In)efficient? Cryptology ePrint Archive, Paper 2023/786, 2023. Available online: https://eprint.iacr.org/2023/786 (accessed on 20 July 2023).

51. Wahrstätter, A.; Ernstberger, J.; Yaish, A.; Zhou, L.; Qin, K.; Tsuchiya, T.; Steinhorst, S.; Svetinovic, D.; Christin, N.; Barczentewicz, M.; et al. Blockchain Censorship. *arXiv* **2023**, arXiv:2305.18545. [CrossRef]
52. Lashkari, B.; Musilek, P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
53. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; pp. 2567–2572. [CrossRef]
54. Zhu, Y. Research on Digital Finance Based on Blockchain Technology. In Proceedings of the 2021 International Conference on Computer, Blockchain and Financial Development (CBFD), Nanjing, China, 23–25 April 2021; pp. 410–414. [CrossRef]
55. Andola, N.; Yadav, V.K.; Venkatesan, S.; Verma, S.; Verma, S. Anonymity on blockchain based e-cash protocols—A survey. *Comput. Sci. Rev.* **2021**, *40*, 100394. [CrossRef]
56. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
57. Ismail, L.; Materwala, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. *Symmetry* **2019**, *11*, 1198. [CrossRef]
58. Krittanawong, C.; Rogers, A.J.; Aydar, M.; Choi, E.; Johnson, K.W.; Wang, Z.; Narayan, S.M. Integrating blockchain technology with artificial intelligence for cardiovascular medicine. *Nat. Rev. Cardiol.* **2020**, *17*, 1–3. [CrossRef]
59. Jamaludin, J.; Rohani, J.M. Cyber-physical system (cps): State of the art. In Proceedings of the 2018 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), Quetta, Pakistan, 12–13 November 2018; pp. 1–5. [CrossRef]
60. Russell, S.J.; Norvig, P. *Artificial Intelligence a Modern Approach*; Pearson: London, UK, 2010.
61. Winston, P.H. *Artificial intelligence*; Addison-Wesley Longman Publishing Co., Inc.: Reading, MA, USA, 1992.
62. Elaine Rich, K.K. *Artificial Intelligence*; McGraw-Hill: New York, NY, USA, 1991.
63. Devlin, J.; Chang, M.W.; Lee, K.; Toutanova, K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. *arXiv* **2018**, arXiv:1810.04805.
64. Liu, P.; Yuan, W.; Fu, J.; Jiang, Z.; Hayashi, H.; Neubig, G. Pre-train, Prompt, and Predict: A Systematic Survey of Prompting Methods in Natural Language Processing. *arXiv* **2021**, arXiv:2107.13586. [CrossRef]
65. Ziegler, D.M.; Stiennon, N.; Wu, J.; Brown, T.B.; Radford, A.; Amodei, D.; Christiano, P.; Irving, G. Fine-Tuning Language Models from Human Preferences. *arXiv* **2019**, arXiv:1909.08593.
66. Bootpoot. What is Artificial Intelligence? Characteristics, Applications and Importance of A.I. Available online: https://bootpoot.tech/what-is-artificial-intelligence-characteristics-applications-and-importance-of-a-i (accessed on 22 October 2021).
67. Greff, K.; van Steenkiste, S.; Schmidhuber, J. On the Binding Problem in Artificial Neural Networks. *arXiv* **2020**, arXiv:2012.05208. [CrossRef]
68. Prade, H. Reasoning with data-a new challenge for AI? In *Proceedings of the International Conference on Scalable Uncertainty Management*; Springer: New York, NY, USA, 2016; pp. 274–288. [CrossRef]
69. Walch, K. Walch, How Do Big Data and AI Work Together? Available online: https://www.techtarget.com/searchenterpriseai/tip/How-do-big-data-and-AI-work-together (accessed on 2 May 2024).
70. Sas. Artificial Intelligence: What it Is and Why It Matters. Available online: https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html (accessed on 2 October 2022).
71. Dutta, A. Reasoning with imprecise knowledge in expert systems. *Inf. Sci.* **1985**, *37*, 3–24. [CrossRef]
72. Basu, A.; Dutta, A. Reasoning with imprecise knowledge to enhance intelligent decision support. *IEEE Trans. Syst. Man Cybern.* **1989**, *19*, 756–770. [CrossRef]
73. Bloch, I. Spatial reasoning under imprecision using fuzzy set theory, formal logics and mathematical morphology. *Int. J. Approx. Reason.* **2006**, *41*, 77–95. [CrossRef]
74. Kumari, A.; Gupta, R.; Tanwar, S.; Kumar, N. Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *J. Parallel Distrib. Comput.* **2020**, *143*, 148–166. [CrossRef]
75. Moniruzzaman, M.; Khezr, S.; Yassine, A.; Benlamri, R. Blockchain for smart homes: Review of current trends and research challenges. *Comput. Electr. Eng.* **2020**, *83*, 106585. [CrossRef]
76. Shae, Z.; Tsai, J. AI blockchain platform for trusting news. In Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 7–9 July 2019; pp. 1610–1619. [CrossRef]
77. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE Technical Report EBSE-2007-01; 2007. Available online: https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf (accessed on 18 December 2022).
78. Ellegaard, O.; Wallin, J. The bibliometric analysis of scholarly production: How great is the impact? *Scientometrics* **2015**, *105*, 1809–1831. [CrossRef]
79. Karger, E. Combining Blockchain and Artificial Intelligence-Literature Review and State of the Art. In Proceedings of the Forty-First International Conference on Information Systems (ICIS), Virtual, 13–16 December 2020.
80. Xing, B.; Marwala, T. The Synergy of Blockchain and Artificial Intelligence. 2018. Available online: https://ssrn.com/abstract=3225357 (accessed on 2 May 2024).
81. Bertino, E.; Kundu, A.; Sura, Z. Data transparency with blockchain and AI ethics. *J. Data Inf. Qual. (JDIQ)* **2019**, *11*, 1–8. [CrossRef]

82. Harris, J.D.; Waggoner, B. Decentralized and collaborative AI on blockchain. In Proceedings of the 2019 IEEE international conference on blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 368–375. [CrossRef]
83. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
84. Lobo, V.B.; Analin, J.; Laban, R.M.; More, S.S. Convergence of Blockchain and Artificial Intelligence to Decentralize Healthcare Systems. In Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 11–13 March 2020; pp. 925–931. [CrossRef]
85. Wang, R.; Luo, M.; Wen, Y.; Wang, L.; Kim-Kwang, R.C.; He, D. The Applications of Blockchain in Artificial Intelligence. *Secur. Commun. Netw.* **2021**, *2021*, 6126247. [CrossRef]
86. Research, G. Convergence of Blockchain and Artificial Intelligence. Available online: https://m.guardtime.com/files/blockchain_and_ai.pdf (accessed on 15 February 2022).
87. Alaeddini, M.; Hajizadeh, M.; Reaidy, P. A Bibliometric Analysis of Research on the Convergence of Artificial Intelligence and Blockchain in Smart Cities. *Smart Cities* **2023**, *6*, 764–795. [CrossRef]
88. Taleb, N.; Al-Dmour, N.A.; Issa, G.F.; Abdellatif, T.M.; Alzoubi, H.M.; Alshurideh, M.; Salahat, M. Analysis of Issues Affecting IoT, AI, and Blockchain Convergence. In *The Effect of Information Technology on Business and Marketing Intelligence Systems*; Alshurideh, M., Al Kurdi, B.H., Masa'deh, R., Alzoubi, H.M., Salloum, S., Eds.; Springer International Publishing: Cham, Switzerland, 2023; pp. 2055–2066. [CrossRef]
89. Kumar, S.; Lim, W.M.; Sivarajah, U.; Kaur, J. Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis. *Inf. Syst. Front.* **2023**, *25*, 871–896. [CrossRef] [PubMed]
90. Hajizadeh, M.; Alaeddini, M.; Reaidy, P. Bibliometric Analysis on the Convergence of Artificial Intelligence and Blockchain. In *Blockchain and Applications, 4th International Congress*; Prieto, J., Benítez Martínez, F.L., Ferretti, S., Arroyo Guardeño, D., Tomás Nevado-Batalla, P., Eds.; Springer: Cham, Switzerland, 2023; pp. 334–344.
91. Vilas-Boas, J.L.; Rodrigues, J.J.; Alberti, A.M. Convergence of Distributed Ledger Technologies with Digital Twins, IoT, and AI for fresh food logistics: Challenges and opportunities. *J. Ind. Inf. Integr.* **2023**, *31*, 100393. [CrossRef]
92. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21 May 2015; pp. 180–184. [CrossRef]
93. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Trans. Ind. Inform.* **2018**, *15*, 4197–4205. [CrossRef]
94. He, S.; Tang, Q.; Wu, C.Q.; Shen, X. Decentralizing IoT management systems using blockchain for censorship resistance. *IEEE Trans. Ind. Inform.* **2019**, *16*, 715–727. [CrossRef]
95. Omohundro, S. Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters* **2014**, *1*, 19–21. [CrossRef]
96. Bahrammirzaee, A. A comparative survey of artificial intelligence applications in finance: Artificial neural networks, expert system and hybrid intelligent systems. *Neural Comput. Appl.* **2010**, *19*, 1165–1195. [CrossRef]
97. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. Blockchain: A distributed solution to automotive security and privacy. *IEEE Commun. Mag.* **2017**, *55*, 119–125. [CrossRef]
98. Singh, P.; Elmi, Z.; Lau, Y.-Y.; Borowska-Stefańska, M.; Wiśniewski, S.; Dulebenets, M.A. Blockchain and AI technology convergence: Applications in transportation systems. *Veh. Commun.* **2022**, *38*, 100521. [CrossRef]
99. Möser, M. Anonymity of Bitcoin Transactions An Analysis of Mixing Services. 2013. Available online: https://api.semanticscholar.org/CorpusID:7112283 (accessed on 18 December 2022).
100. Barwal, D.; Behera, R.; Saho, A. Blockchain: A Primer. *CIS Commun. Knowl. Dig. IT Community* **2017**, *41*, 15–19.
101. Al-Jaroodi, J.; Mohamed, N. Blockchain in industries: A survey. *IEEE Access* **2019**, *7*, 36500–36515. [CrossRef]
102. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56. [CrossRef]
103. Halal, W.E. Artificial intelligence is almost here. *On the Horizon* **2003**, 11, 37–38. [CrossRef]
104. Arel, I.; Rose, D.C.; Karnowski, T.P. Deep machine learning-a new frontier in artificial intelligence research [research frontier]. *IEEE Comput. Intell. Mag.* **2010**, *5*, 13–18. [CrossRef]
105. Jiang, F.; Jiang, Y.; Zhi, H.; Dong, Y.; Li, H.; Ma, S.; Wang, Y.; Dong, Q.; Shen, H.; Wang, Y. Artificial intelligence in healthcare: Past, present and future. *Stroke Vasc. Neurol.* **2017**, *2*. [CrossRef]
106. Pannu, A. Artificial intelligence and its application in different areas. *Artif. Intell.* **2015**, *4*, 79–84.
107. Krarti, M. An overview of artificial intelligence-based methods for building energy systems. *J. Sol. Energy Eng.* **2003**, *125*, 331–342. [CrossRef]
108. Deepa, S.; Devi, B.A. A survey on artificial intelligence approaches for medical image classification. *Indian J. Sci. Technol.* **2011**, *4*, 1583–1595. [CrossRef]
109. Kodogiannis, V.; Lygouras, J.N. Neuro-fuzzy classification system for wireless-capsule endoscopic images. *Int. J. Electr. Comput. Syst. Eng.* **2008**, *2*, 55–63.
110. Riedl, M.O.; Zook, A. AI for game production. In Proceedings of the 2013 IEEE Conference on Computational Inteligence in Games (CIG), Niagara Falls, ON, Canada, 11–13 August 2013; pp. 1–8. [CrossRef]
111. Anifowose, F.A.; Eludiora, S.I. Application of artificial intelligence in network intrusion detection. *World Appl. Program.* **2012**, *2*, 158–166.

112. Milton, R.; Hay, D.; Gray, S.; Buyuklieva, B.; Hudson-Smith, A. Smart iot and soft ai. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT-2018, IET, London, UK, 28–29 March 2018; pp. 1–6. [CrossRef]
113. Wu, P.; Guo, H. LuNET: A deep neural network for network intrusion detection. In Proceedings of the 2019 IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, 6–9 December 2019; pp. 617–624. [CrossRef]
114. Aslan, Ö.; Yilmaz, A.A. A new malware classification framework based on deep learning algorithms. *IEEE Access* **2021**, *9*, 87936–87951. [CrossRef]
115. Castelló Ferrer, E. The blockchain: A new framework for robotic swarm systems. In Proceedings of the *Future Technologies Conference*; Springer: New York, NY, USA, 2018; pp. 1037–1058. [CrossRef]
116. Shrestha, A.K.; Vassileva, J. Blockchain-based research data sharing framework for incentivizing the data owners. In *Proceedings of the International Conference on Blockchain*; Springer: New York, NY, USA, 2018; pp. 259–266. [CrossRef]
117. Idiveri, G.; Horiuchi, T.K. Frontiers in Neuromorphic Engineering, 2011. pp. 1–2. *Front. Neurosci.* **2011**, *5*, 13375. [CrossRef] [PubMed]
118. Suri, M. *Advances in Neuromorphic Hardware Exploiting Emerging Nanoscale Devices*; Springer: New York, NY, USA, 2017.
119. Evans, R.; Gao, J. DeepMind AI Reduces Energy Used for Cooling Google Data Centers by 40%, Google. Available online: https://blog.google/outreach-initiatives/environment/deepmind-ai-reduces-energy-used-for (accessed on 5 March 2022).
120. CapTec. Combining Blockchain and AI to Foster Trust in Healthcare. Available online: https://www.captechconsulting.com/blogs/combining-blockchain-and-ai-to-foster-trust-in-healthcare (accessed on 20 December 2023).
121. Rabah, K. Convergence of AI, IoT, Big Data and Blockchain: A Review. *Lake Inst. J.* **2018**, *1*, 1–18.
122. Marr, B. Artificial Intelligence and Blockchain: 3 Major Benefits of Combining These Two Mega-Trends. Available online: https://www.forbes.com/sites/bernardmarr/2018/03/02/artificial-intelligence-and-blockchain-3-major-benefits-of-combining-these-two-mega-trends/?sh=3c54ff5a4b44 (accessed on 20 February 2022).
123. Kolias, C.; Kolias, V.; Kambourakis, G. TermID: A distributed swarm intelligence-based approach for wireless intrusion detection. *Int. J. Inf. Sec.* **2017**, *16*, 401–416. [CrossRef]
124. Corea, F. *Applied Artificial Intelligence: Where AI Can Be Used in Business*; Springer: New York, NY, USA, 2019; Volume 1. [CrossRef]
125. Commission, E. High-Level Expert Group on Artificial Intelligence. Available online: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf (accessed on 25 February 2022).
126. Oleksiuk, A. Five Benefits of Combining AI and Blockchain, Intellian Global Technology Partner. Available online: https://intellias.com/five-benefits-of-combining-ai-and-blockchain (accessed on 25 February 2022).
127. Kambourakis, G.; Kolias, C.; Stavrou, A. The Mirai botnet and the IoT Zombie Armies. In Proceedings of the 2017 IEEE Military Communications Conference, MILCOM 2017, Baltimore, MD, USA, 23–25 October 2017; pp. 267–272. [CrossRef]
128. Chatzoglou, E.; Kambourakis, G.; Smiliotopoulos, C. Let the Cat out of the Bag: Popular Android IoT Apps under Security Scrutiny. *Sensors* **2022**, *22*, 513. [CrossRef]
129. De Brouwer, W.; Borda, M. NeuRoN: Decentralized Artificial Intelligence, Distributing Deep Learning to the Edge of the Network, 2017. Available online: https://coinpaprika.com/storage/cdn/whitepapers/448539.pdf (accessed on 10 January 2023).
130. Rahman, M.A.; Rashid, M.M.; Hossain, M.S.; Hassanain, E.; Alhamid, M.F.; Guizani, M. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access* **2019**, *7*, 18611–18621. [CrossRef]
131. Rathore, S.; Pan, Y.; Park, J.H. BlockDeepNet: A Blockchain-based secure deep learning for IoT network. *Sustainability* **2019**, *11*, 3974. [CrossRef]
132. Alrubei, S.M.; Ball, E.; Rigelsford, J.M. The use of blockchain to support distributed AI implementation in IoT systems. *IEEE Internet Things J.* **2021**, *9*, 14790–14802. [CrossRef]
133. Singh, S.K.; Rathore, S.; Park, J.H. Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
134. Alrubei, S.M.; Ball, E.; Rigelsford, J.M. A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer. *IEEE Access* **2022**, *10*, 18583–18595. [CrossRef]
135. Kampourakis, V.; Gkioulos, V.; Katsikas, S. A systematic literature review on wireless security testbeds in the cyber-physical realm. *Comput. Secur.* **2023**, *133*, 103383. [CrossRef]
136. Smiliotopoulos, C.; Kambourakis, G.; Kolias, C. Detecting Lateral Movement: A Systematic Survey. Available at SSRN 4606223. Available online: https://doi.org/https://dx.doi.org/10.2139/ssrn.4606223 (accessed on 10 January 2023).
137. Latif, S.A.; Wen, F.B.X.; Iwendi, C.; Li-li, F.W.; Mohsin, S.M.; Han, Z.; Band, S.S. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Comput. Commun.* **2022**, *181*, 274–283. [CrossRef]
138. Smiliotopoulos, C.; Barmpatsalou, K.; Kambourakis, G. Revisiting the Detection of Lateral Movement through Sysmon. *Appl. Sci.* **2022**, *12*, 7746. [CrossRef]
139. Smiliotopoulos, C.; Kambourakis, G.; Barbatsalou, K. On the detection of lateral movement through supervised machine learning and an open-source tool to create turnkey datasets from Sysmon logs. *Int. J. Inf. Secur.* **2023**, *22*, 1893–1919. [CrossRef]
140. Heister, S.; Yuthas, K. How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity. In Proceedings of the Advances in the Convergence of Blockchain and Artificial Intelligence, London, UK, 12 January 2022. [CrossRef]
141. Deebak, B.D.; Al-Turjman, F. Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. *J. Inf. Secur. Appl.* **2021**, *58*, 102749. [CrossRef]

142. Kim, J.; Park, N. Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments. *Appl. Sci.* **2020**, *10*, 4718. [CrossRef]
143. Liang, W.; Xiao, L.; Zhang, K.; Tang, M.; He, D.; Li, K.C. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. *IEEE Internet Things J.* **2021**, *9*, 1474–14751. [CrossRef]
144. Rahman, Z.; Yi, X.; Khalil, I. Blockchain-based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet Things J.* **2022**, *10*, 6769–6778. [CrossRef]
145. Otoum, S.; Mouftah, H.T. Enabling Trustworthiness in Sustainable Energy Infrastructure Through Blockchain and AI-Assisted Solutions. *IEEE Wirel. Commun.* **2021**, *28*, 19–25. [CrossRef]
146. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.; Chopra, S.S. Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies* **2020**, *13*, 5739. [CrossRef]
147. Xiao, W.; Liu, C.; Wang, H.; Zhou, M.; Hossain, M.S.; Alrashoud, M.; Muhammad, G. Blockchain for secure-GaS: Blockchain-powered secure natural gas IoT system with AI-enabled gas prediction and transaction in smart city. *IEEE Internet Things J.* **2020**, *8*, 6305–6312. [CrossRef]
148. Mylrea, M. Distributed autonomous energy organizations: Next-generation blockchain applications for energy infrastructure. In *Artificial Intelligence for the Internet of Everything*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 217–239. [CrossRef]
149. Ren, Q.; Man, K.; Li, M.; Gao, B. Using Blockchain to Enhance and Optimize IoT-based Intelligent Traffic System. In Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Republic of Korea, 28–30 January 2019; pp. 1–4. [CrossRef]
150. Pandey, S.; Chouhan, V.; Verma, D.; Rajrah, S.; Alenezi, F.; Saini, R.; Santosh, K. Do-It-Yourself Recommender System: Reusing and Recycling With Blockchain and Deep Learning. *IEEE Access* **2022**, *10*, 90056–90067. [CrossRef]
151. Ouyang, L.; Yuan, Y. Learning Markets: An AI Collaboration Framework Based on Blockchain and Smart Contracts. *IEEE Internet Things J.* **2022**, *9*, 14273–14286. [CrossRef]
152. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
153. Ouyang, L.; Yuan, Y.; Wang, F.Y. A Blockchain-based Framework for Collaborative Production in Distributed and Social Manufacturing. In Proceedings of the 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, 6–8 November 2019; pp. 76–81. [CrossRef]
154. Wang, F.Y.; Yuan, Y.; Zhang, J.; Qin, R.; Smith, M. Blockchainized Internet of Minds: A New Opportunity for Cyber–Physical–Social Systems. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 897–906. [CrossRef]
155. Qu, Y.; Gao, L.; Luan, T.H.; Xiang, Y.; Yu, S.; Li, B.; Zheng, G. Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing. *IEEE Internet Things J.* **2020**, *7*, 5171–5183. [CrossRef]
156. Zhou, H.; Milani Fard, A.; Makanju, A. The State of Ethereum Smart Contracts Security: Vulnerabilities, Countermeasures, and Tool Support. *J. Cybersecur. Priv.* **2022**, *2*, 358–378. [CrossRef]
157. Dietterich, T.G. Ensemble learning. *Handb. Brain Theory Neural Netw.* **2002**, *2*, 110–125.
158. Strubell, E.; Ganesh, A.; McCallum, A. Energy and policy considerations for deep learning in NLP. *arXiv* **2019**, arXiv:1906.02243. [CrossRef]
159. Varriale, V.; Cammarano, A.; Michelino, F.; Caputo, M. Critical analysis of the impact of artificial intelligence integration with cutting-edge technologies for production systems. *J. Intell. Manuf.* **2023**, *327*, 7–47. [CrossRef] [PubMed]
160. Badruddoja, S.; Dantu, R.; He, Y.; Upadhayay, K.; Thompson, M. Making smart contracts smarter. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021; pp. 1–3. [CrossRef]
161. Gartner. Gartner Says Worldwide Artificial Intelligence Spending Will Reach $110 Billion in 2024. 2023. Available online: https://www.gartner.com/en/newsroom/press-releases/2024-04-16-gartner-forecast-worldwide-it-spending-to-grow-8-percent-in-2024 (accessed on 25 March 2023).
162. MIT Technology Review. MIT Technology Review. 2023. Available online: https://www.technologyreview.com/ (accessed on 25 March 2023).
163. AI Now Institute. AI Now Institute. 2023. Available online: https://ainowinstitute.org/ (accessed on 25 March 2023).
164. World Economic Forum. The Future of Jobs Report 2022. 2023. Available online: https://www.weforum.org/publications/the-future-of-jobs-report-2023/digest/ (accessed on 25 March 2023).
165. El Hajj, I.; Merritt, A.; Zellweger, G.; Milojicic, D.; Achermann, R.; Faraboschi, P.; Hwu, W.m.; Roscoe, T.; Schwan, K. SpaceJMP: Programming with multiple virtual address spaces. *ACM SIGPLAN Not.* **2016**, *51*, 353–368. [CrossRef]
166. Dang, H.; Dinh, T.T.A.; Loghin, D.; Chang, E.C.; Lin, Q.; Ooi, B.C. Towards scaling blockchain systems via sharding. In Proceedings of the 2019 International Conference on Management of Data, Amsterdam, The Netherlands, 30 June–5 July 2019; pp. 123–140. [CrossRef]
167. Hwang, G.H.; Chen, P.H.; Lu, C.H.; Chiu, C.; Lin, H.C.; Jheng, A.J. InfiniteChain: A multi-chain architecture with distributed auditing of sidechains for public blockchains. In *Proceedings of the International Conference on Blockchain*; Springer: New York, NY, USA, 2018; pp. 47–60. [CrossRef]
168. Boyen, X.; Carr, C.; Haines, T. Graphchain: A blockchain-free scalable decentralised ledger. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Incheon, Republic of Korea, 4 June 2018; pp. 21–33. [CrossRef]

169. Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand: Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, 28–31 October 2017; pp. 51–68. [CrossRef]
170. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
171. Destefanis, G.; Marchesi, M.; Ortu, M.; Tonelli, R.; Bracciali, A.; Hierons, R. Smart contracts vulnerabilities: A call for blockchain software engineering? In Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 20 March 2018; pp. 19–25. [CrossRef]
172. Nicholas; Johnson, N.; Juels, A.; Miller, A.; Song, D. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 185–200.
173. Galal, H.S.; Youssef, A.M. Trustee: Full privacy preserving vickrey auction on top of ethereum. In Proceedings of the Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, 18–22 February 2019; Revised Selected Papers 23; Springer: New York, NY, USA, 2020; pp. 190–207.
174. Zhang, F.; Cecchetti, E.; Croman, K.; Juels, A.; Shi, E. Town crier: An authenticated data feed for smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 270–282. [CrossRef]
175. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart contract development: Challenges and opportunities. *IEEE Trans. Softw. Eng.* **2019**, *47*, 2084–2106. [CrossRef]
176. Tsankov, P.; Dan, A.; Drachsler-Cohen, D.; Gervais, A.; Buenzli, F.; Vechev, M. Securify: Practical security analysis of smart contracts. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 67–82. [CrossRef]
177. Patni, S. Centralized and Decentralized Systems Finally Get 'Chained'. Available online: https://blog.shubhpatni.com/centralized-and-decentralized-systems-finally-get-chained-ba702dea972 (accessed on 1 April 2022).
178. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R. A Distributed framework for detecting DDoS attacks in smart contract-based Blockchain-IoT Systems by leveraging Fog computing. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4112. [CrossRef]
179. Deepankar, S.; Chowdhury, S.R. Blockchain-based smart contract for international business–a framework. *J. Glob. Oper. Strateg. Sourc.* **2021**, *1*. [CrossRef]
180. Ji, R.; He, N.; Wu, L.; Wang, H.; Bai, G.; Guo, Y. Deposafe: Demystifying the fake deposit vulnerability in Ethereum smart contracts. In Proceedings of the 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS), Singapore, 28–31 October 2020; pp. 125–134. [CrossRef]
181. Anjum, A.; Sporny, M.; Sill, A. Blockchain standards for compliance and trust. *IEEE Cloud Comput.* **2017**, *4*, 84–90. [CrossRef]
182. Kakavand, H.; Kost De Sevres, N.; Chilton, B. The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. Available at SSRN 2849251 2017. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 (accessed on 25 March 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.