future internet

MDPI

Review

Survey of Artificial Intelligence Model Marketplace

Mian Qian, Abubakar Ahmad Musa, Milon Biswas, Yifan Guo, Weixian Liao and Wei Yu *

Department of Computer and Information Sciences, Towson University, Towson, MD 21252, USA; mqian2@students.towson.edu (M.Q.); aahmadm1@students.towson.edu (A.A.M.); mbiswas1@students.towson.edu (M.B.); yguo@towson.edu (Y.G.); wliao@towson.edu (W.L.)
* Correspondence: wyu@towson.edu

Abstract: The rapid advancement and widespread adoption of artificial intelligence (AI) across diverse industries, including healthcare, finance, manufacturing, and retail, underscore the transformative potential of AI technologies. This necessitates the development of viable AI model marketplaces that facilitate the development, trading, and sharing of AI models across the pervasive industrial domains to harness and streamline their daily activities. These marketplaces act as centralized hubs, enabling stakeholders such as developers, data owners, brokers, and buyers to collaborate and exchange resources seamlessly. However, existing AI marketplaces often fail to address the demands of modern and next-generation application domains. Limitations in pricing models, standardization, and transparency hinder their efficiency, leading to a lack of scalability and user adoption. This paper aims to target researchers, industry professionals, and policymakers involved in AI development and deployment, providing actionable insights for designing robust, secure, and transparent AI marketplaces. By examining the evolving landscape of AI marketplaces, this paper identifies critical gaps in current practices, such as inadequate pricing schemes, insufficient standardization, and fragmented policy enforcement mechanisms. It further explores the AI model life-cycle, highlighting pricing, trading, tracking, security, and compliance challenges. This detailed analysis is intended for an audience with a foundational understanding of AI systems, marketplaces, and their operational ecosystems. The findings aim to inform stakeholders about the pressing need for innovation and customization in AI marketplaces while emphasizing the importance of balancing efficiency, security, and trust. This paper serves as a blueprint for the development of next-generation AI marketplaces that meet the demands of both current and future application domains, ensuring sustainable growth and widespread adoption.

Keywords: artificial intelligence (AI); machine learning (ML); model marketplace design; digital marketplace; marketplace service; AI marketplace; AI security; marketplace security; AI platform

Academic Editor: Gianluigi Ferrari

Received: 10 December 2024
Revised: 2 January 2025
Accepted: 8 January 2025
Published: 14 January 2025

Citation: Qian, M.; Musa, A.A.; Biswas, M.; Guo, Y.; Liao, W.; Yu, W. Survey of Artificial Intelligence Model Marketplace. *Future Internet* **2025**, *17*, 35. https://doi.org/10.3390/fi17010035

1. Introduction

Artificial intelligence (AI) has become rapidly ubiquitous in various industries and has opened new business opportunities, affecting various smart-world systems [1,2]. As the adoption of AI continues to accelerate, companies and individuals face challenges in sourcing, integrating, and customizing AI solutions that meet their unique needs. In the recent past, just like the case of big data marketplace [1] that trades data as commodities, the rise of AI marketplaces aims to solve these challenges by providing centralized and decentralized platforms where businesses or individuals can access a wide range of AI models. These platforms act as a bridge to establish relationships between AI developers,

businesses, and researchers for AI development and deployment. The demand for the AI marketplace has increased significantly; this includes marketplaces capable of trading both predictive and generative AI models [3–5]. According to the Precedence Research report, the AI market's average Compound Annual Growth Rate (CAGR) is projected to increase by 19.1 % from 2024 to 2034 [6–8].

Like traditional markets, the AI marketplace, which is a good example of digital commodity-based markets, helps to control and manage the distribution and utilization of the AI model. An ideal AI marketplace also offers scalability and flexibility, enabling organizations to explore existing and customizable models for their use cases. This type of marketplace will revolutionize e-commerce, cloud computing, and software development. However, the design and development of AI marketplaces are still in the infancy stage [9].

On the other hand, it is trivial that new technologies always give rise to corresponding marketplaces for innovation and growth. For example, the development of the MPEG audio layer revolutionized traditional music by converting it into digital formats, bringing about a digital music marketplace like Spotify. Spotify allows artists to be compensated based on streams instead of distribution channels [10]. Similarly, global positioning system (GPS) technology enables the establishment of Uber, turning people with cars into service providers, thus monetizing personal transportation [5,11,12].

With the rapid expansion of AI-based technology in recent years, innovators and researchers have begun exploring the establishment of AI marketplaces to promote the development and sharing of AI models. Unlike traditional physical products or bonds, AI model markets do not transfer ownership to the buyer upon sale. Instead, AI model trainers often seek to maintain control over their models' distribution and post-sale performance. Thus, an ideal AI marketplace should focus on the growing demand for flexible, customizable solutions and shared platforms accessible to various stakeholders. Currently, there exist several challenges that are militating against the development of an effective AI marketplace, including:

- *Model Distribution Management*: Unauthorized reselling of AI models might be possible in the AI marketplace. For example, a consumer might purchase an AI model and then resell it without the original developer's awareness, which violates intellectual property rights and diminishes the value of the original product [13].
- *Standard Governing Policies:* Lack of universally accepted policies or regulations to govern the AI marketplace. Using the California Consumer Privacy Act (CCPA) as an example [14,15]. Under CCPA, AI developers and sellers are required to ensure that sensitive personal data is protected before sale or distribution. However, this level of regulation is not required in other states or countries. An AI model trained on sensitive data might be sold outside California, where the privacy regulations are less stringent, but buyers might use it in California.
- *Customer Feedback System:* The lack of an effective customer feedback mechanism significantly hinders AI developers from improving their models. For example, a customer using a predictive analytics tool might experience substantial performance issues. However, without a structured feedback system integrated into the AI marketplace, developers are left unaware of these problems and are unable to address or resolve them. This disconnection impacts the customer experience and limits the developer's ability to refine and enhance their AI solutions.
- *Low Efficiency:* Multiple AI models have highly similar feature functionalities. Rather than leveraging existing models, significant labor and resources are often spent on redeveloping the same functionalities from scratch. If there is an AI platform that can collect all existing AI models to be utilized by developers in building AI models upon pre-existing models, organizations could significantly reduce development

costs and accelerate deployment timelines while avoiding redundancy in feature development [13,16].

- *High Energy Consumption with Low Productivity:* According to the bank company PCBB, the electricity required to train a single AI model exceeds the annual consumption of approximately 130 U.S. households [17]. According to ClearML 3rd global AI research survey, 15 % used less than 50 % of their GPU utilization, 53 % used 50 % to 70 %, while only 7 % believed their GPU utilization is over 85 %. Optimizing GPU utilization to reduce the overall energy consumption will be a big challenge for the current AI development [18].
- *High Cost:* Stanford researchers replicated models such as GPT-3, OPT-175B, GPT-4, and Gemini Ultra. According to their testing result, training ChatGPT-4 incurred a cost of $40 million, while the R&D expenses for Gemini Ultra accounted for 49 % of the total cost [19]. How to promote cooperation between developers to reduce overall costs is a challenge for the AI marketplace.
- *Imprecise Pricing Strategy:* Lack of an effective pricing strategy guiding AI developers and model buyers creates significant challenges in AI marketplaces. Relying solely on sellers to determine prices can lead to biased or unfair pricing strategies, potentially alienating buyers and undermining trust in the marketplace. This imbalance highlights the need for mechanisms that improve pricing efficiency by identifying a fair and balanced price point that aligns the interests of both sellers and buyers. Developing such mechanisms will be a critical task for ensuring the long-term sustainability and fairness of AI marketplaces [20].
- *AI Ethics, Security and Privacy Issues:* The Lack of a robust guiding framework on AI ethics, privacy, and security issues militates against the establishment of an ideal AI marketplace. For example, an AI model might produce biased or discriminatory results or operate as a "black box" with little transparency, raising ethical concerns. Privacy issues also arise, as AI models are often trained on sensitive data (i.e., healthcare-related, etc.) that, if mishandled, could lead to breaches or misuse. Security risks further complicate the landscape, with vulnerabilities in AI (a double-edged sword) potentially exposing users to harm or exploitation. Without addressing these critical areas, trust in the marketplace is eroded, limiting its ability to foster responsible innovation and deliver reliable, ethical, and secure AI solutions [9,15,21–23].

Based on the identified challenges above and the existing efforts summarized by Table 1, there is room for more efforts guiding the end-to-end design of an effective marketplace for AI models. To address these issues, this article aims to examine the unique characteristics of an effective AI marketplace, reviews existing AI marketplaces to identify areas that need improvement, and proposes a three-dimensional problem space to evaluate AI marketplaces from its efficient, secure, and user-centric perspective. Furthermore, the article emphasizes the importance of fostering collaboration between customers, developers, and the AI marketplace to ensure that AI marketplaces meet technical and business needs and adhere to ethical and regulatory standards [9,20,24]. Similarly, a thorough review has been conducted across the various phases of the model development life-cycle to determine the ideal marketplace design that best fits AI models to improve overall efficiency.

The contributions made by this paper are as follows:

- We compared AI marketplaces with application stores and identified six unique characteristics of an effective AI marketplace. This will serve as a reference point for developers when designing an AI marketplace.
- We evaluated and compared the existing AI marketplace performance and pointed out the strengths and weaknesses to enable developers to make continued improvements in their AI marketplace design.

- We defined a model development life-cycle and proposed a problem space to guide the conduct of a literature review across the pricing and trading phases to identify areas of challenges that need to be addressed by future marketplace design.
- We identified the key challenges faced by marketplaces and future directions for an ideal AI marketplace design. Furthermore, a threat taxonomy was presented to identify the emerging security and privacy challenges faced by marketplaces and the feasible ways of dealing with those threats.

Table 1. Existing surveys on model trading.

Reference, Year	Focus	Marketplace Structure	Trading Platforms	Pricing Schemes	Problem Spaces	Threat Taxonomy
Ref. [25], 2020	Progression of data pricing from economic theories to modern data science	×	×	✓	×	×
Ref. [26], 2022	Pricing in the three model development pipelines	✓	×	✓	×	×
Ref. [27], 2023	Progression of data pricing from economic theories to computational intelligence	×	×	✓	×	×
Ref. [28], 2023	Taxonomy of data pricing methods in data marketplaces	✓	×	✓	×	×
Ref. [29], 2023	Taxonomies of data pricing solution models	×	×	✓	×	×
Ref. [30], 2024	Data marketplace design	✓	✓	✓	×	×
Ours, —	Primer on real AI model marketplace design	✓	✓	✓	✓	✓

The remainder of this paper is organized as follows: Section 2 reviews the existing AI marketplaces. Section 3 defines the model development life-cycle. Section 4 reviews the existing pricing schemes and trading platforms. Section 5 discusses model tracking and marketplace security. Section 6 identifies the several challenges guiding future research, and Section 7 concludes the paper, respectively.

2. AI Marketplace Overview

The evolution of technology has brought various digital platforms, such as application stores and AI marketplaces [9,20,31,32]. Even though both serve as ecosystems for distributing technological solutions, their structures and operational models differ significantly. We choose to have a detailed comparison between the two to clearly distinguish what the general public is familiar with and what we envision as an ideal AI marketplace [9,33–37]. Table 2 compares application stores and AI marketplaces. After the detailed comparison, we found that an effective and ideal AI marketplace should include the following six (6) characteristics as indicated by Figure 1. The six (6) characteristics emerged due to a detailed consideration of the individual characteristics and their relevance towards complementing each other to define an ideal marketplace. The characteristics are briefly elaborated below:

- *Cooperation:* AI marketplace promotes cooperation between sellers and buyers. Unlike traditional application stores, where products are offered as fixed, ready-made solutions, the AI marketplace allows buyers and sellers to work closely to develop and customize AI models. This cooperative model not only ensures that both parties contribute to the creation of tailored AI solutions but also encourages continued

improvement, leading to outcomes that more accurately align with the evolving demands of buyers while offering sellers opportunities to enhance their offerings based on real-time user input [20,24].

- *Utilization:* Rather than developing an entirely new AI model from scratch, AI model developers in the marketplace can leverage the existing models to develop a new model. This practice encourages a crowdsourcing concept for AI model improvement, where multiple parties contribute to the same model. This collaborative framework not only accelerates innovation but also optimizes resources by fostering a more dynamic and cost-effective development environment [38].
- *Flexibility:* Compared to the application store, AI marketplaces provide a flexible environment where the buyer can define the unique features and functions required for an AI model rather than buying a predefined model from the seller [9,20]. This flexibility enables sellers to tailor AI solutions according to the buyer's expectations. Such flexibility not only fosters innovation but also ensures that the AI models are aligned with the exact expectations and objectives of the buyer, enhancing overall market efficiency and satisfaction.
- *AI model platform:* Similar to the way traditional application stores offer a platform for users to browse and select applications, the AI marketplace provides a platform for potential customers to review and choose existing AI models. AI marketplace even allows customers to test key features, functionalities, and performance metrics before making a selection [39,40].
- *Pricing Service with multiple payment options:* Unlike application stores, where sellers solely define the price, the AI marketplace offers multiple pricing strategies for sellers and buyers to ensure the price reflects the actual value of the AI model, benefiting both sellers and buyers [41,42]. The AI marketplace provides multiple flexible payment options, such as pay-per-use, subscription, or milestone-based payments, while the application store generally limits payment options to in-app purchases, upfront payments, or monthly subscription fees. Application store payments are based on a fixed design that may include features that may not be of buyers' interest.
- *Protection:* The AI marketplace protects sellers' intellectual property, preventing unauthorized access or misuse. Additionally, all transactions within the AI marketplace are conducted in full compliance with relevant legal and regulatory requirements such as HIPPA [9,20,38].

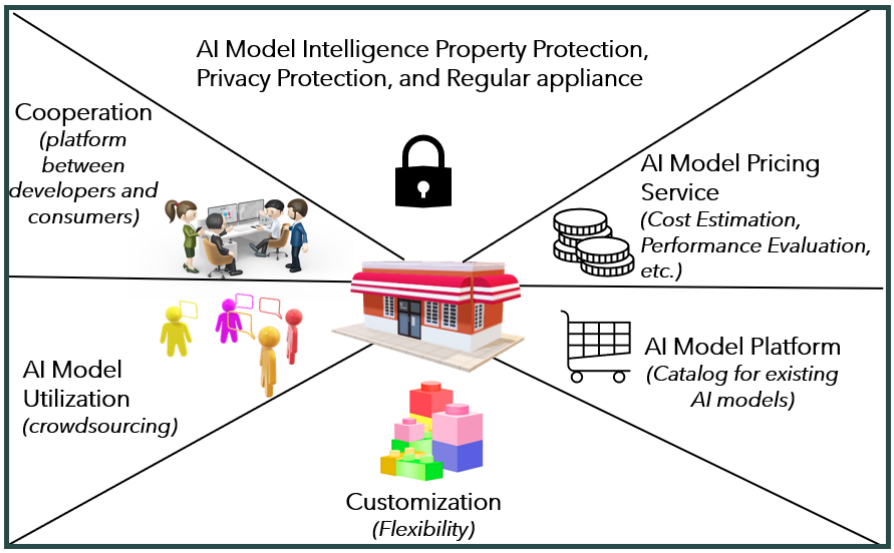

Figure 1. Characteristics of AI model marketplace.

Table 2. The comparison between application store and AI marketplaces.

Items	Application Stores	AI Marketplace	Remarks
Search Engine	Allows users to search based on categories, keywords, or rankings	Same as Application Stores to let buyers discover AI models. Search can also be based on feature functions, price range, or levels of customization	
Product	Does not allow any modifications on the model itself.	Provide options for customers to choose from, such as no modification of the AI model (similar to the application store) or allowing customers to raise requests to the seller to add/remove some feature functions.	AI model should be flexible to allow customization.
Price Strategy	Fixed price with individual model. The seller set the price.	customers should be able to collaborate with the AI model developer to tailor the model to their specific needs. The seller and buyer can set the price together.	AI marketplace can also allow price strategies as the application store and provide multiple payment options.
Asset Management	Application Store needs to maintain asset management to ensure it captures all model information. Application Store also stores individual customer-ordered applications to let sellers continue to upgrade the applications.	Same as the Application store, the AI marketplace also needs to provide such kind of service. In addition, the AI marketplace needs to provide cooperation services such as using building blocks to show individual feature functions and allow sellers and users to use these blocks to customize their designs. Thus, blocks also belong to asset management.	
Customer Feedback	Application store does not care about customer feedback.	AI marketplace allows customers to raise questions or requests to the developer, and the developer can make some modifications to its AI model to comply with the customer's requirements.	Close loop between the customer and the seller for the AI marketplace.
Revision Control	developers push updates to apps. The same updates are for all users.	Customization means AI model revision control can be a mutual agreement between the seller and the buyer.	AI marketplace can be a continuous partnership rather than a one-off purchase as an application store.

To comprehensively describe the AI marketplace from multiple perspectives, we design problem spaces, aiming to capture the complexity and diversity of AI trading environments by considering trading models, pricing strategies, and customization options. Best practices for AI marketplace development involve implementing robust pricing schemes, user-friendly designs, and vigorous policy enforcement to ensure transparency, accessibility, and trust among stakeholders. Successful marketplaces should support model customization for domain-specific needs, provide performance metrics for informed decision-making, and integrate security measures like blockchain to protect transactions. Additionally, standardizing formats and enabling seamless integration with popular tools enhance usability. Incorporating feedback loops and catering to cross-industry use cases further expand the marketplace's reach and relevance, fostering a balanced ecosystem that benefits buyers and sellers. A detailed checklist/matrix showing critical success factors for AI marketplaces is presented in Table 3. Each factor is explained with examples and implementation suggestions.

Table 3. Critical success factors for AI marketplaces [20].

Ref.	Success Factor	Description	Example	Implementation Suggestions
[43,44]	Robust Pricing Models	Transparent, fair, and dynamic pricing strategies that maximize value for buyers and sellers.	Amazon SageMaker charges based on usage. Google AI Platform offers credits for trials.	Implement auction-based or performance-driven pricing strategies.
[45,46]	User-Friendly Design	Simple and intuitive interfaces for both technical and non-technical users.	Hugging Face's intuitive model search and demo system. Gravity AI offers preview demos.	Use clean UI/UX with guided workflows and demo options for models.
[47]	Strong Policy Enforcement	Clear policies for data privacy, intellectual property, and usage terms to build trust among stakeholders.	DataStax ensures compliance with NVIDIA's ethical guidelines. HIPAA-compliant AI in healthcare platforms.	Integrate automated compliance checks and robust policy documentation.
[48]	Customization Support	Allow users to customize AI models to meet domain-specific needs.	AI Planet supports industry-specific models (e.g., medical, education).	Provide APIs and developer tools for customization and configuration.
[49]	Performance Transparency	Offer clear metrics (e.g., accuracy, speed) to evaluate model performance pre-purchase.	Google AI Platform provides performance stats for models. NVIDIA AI shows benchmark tests.	Embed benchmarking and comparison tools with real-time performance metrics.
[50,51]	Marketplace Security	Protect sensitive information and prevent unauthorized access to models or transactions.	Use of blockchain for transaction transparency (e.g., Ethereum-based AI trading).	Implement encryption, blockchain, and secure APIs for transactions.
[52,53]	Standardized Formats	Uniform templates for datasets, models, and metadata to ensure compatibility across use cases.	H_2O.ai uses standardized model formats.	Develop standards for metadata, versioning, and data schemas.
[54]	Integration Capabilities	Ensure seamless integration with existing tools, platforms, and workflows.	Google AI integrates with GCP. Hugging Face integrates with PyTorch and TensorFlow.	Provide SDKs, APIs, and tutorials for popular AI frameworks.
[55]	Feedback Loops	Enable buyers to provide feedback and reviews on purchased models.	Hugging Face has a community-based rating system for models.	Include rating and review systems, and encourage regular feedback cycles.
[56]	Cross-Industry Use Cases	Provide models for multiple industries to expand marketplace reach.	Hugging Face offers models for NLP, computer vision, and healthcare.	Diversify model categories and include industry-specific use case demos.

2.1. Marketplace for Existing AI Models

AI tools are widely used for general use, such as chatbots for customer service, task or schedule development, website generation, etc. Using Workday Marketplace as an example. It provides three categories, Finance, Human Resource (HR), and Planning, for the general purpose of AI tools. Users choose AI models based on predefined feature functions. Using HR as an example, the predefined functions include "HR efficiency", "Talent Optimization", "Rewards and Benefits", "Employee Experience", "Payroll", and "Workforce Management". Each category includes multiple AI models to allow customers to compare and choose [57].

Generative AI (GenAI) has been widely used to develop such kinds of AI models. GenAI can create novel, meaningful content, such as text, images, or audio, based on a limited set of training data [58]. Unlike traditional AI models, which typically rely on well-established techniques such as decision trees and support vector machines (SVM), GenAI leverages advanced neural networks, particularly deep-learning architectures (i.e., the transformer), to generate creative outputs [59]. The release of ChatGPT-4 in 2023 marked a pivotal moment in the development and public awareness of GenAI [58–60].

GenAI can be divided into different types based on different input and output data types, such as text-to-text, text-to-images, text-to-videos, code generation, and website

development [61], as indicated in Table 4. Currently, over 200 startup companies are actively engaged in developing the AI market, spanning more than two dozen distinct categories for GenAI models [62]. Table 5 itemized some of the current Generative AI marketplaces that are designed for existing GenAI models.

Table 4. An overview of generative AI applications.

Type	Features	GenAI Models	Model Example	Price
Text-to-Text	input: text, output: text	Variational Autoencoder (VAE), Transformer-Based Models (TBM), Large Language Models (LLM)	ChatGPT (OpenAI), Gemini (Google)	ChatGPT ($20.00/month), Gemini($20.00/month)
Text-to-Images	input: text, output: images	Generative Adversarial Network (GAN)	DALL.E	$20.00/month
Text-to-Videos	input: text, output: videos	Diffusion Models (DM)	Adobe Premiere Pro, SORA	Adobe ($20.99/month),
Code Generation	input: text, output: code	TBM	Genimi (Google), ChatGPT (OpenAI), Claude (Claude.ai), etc.	Genimi ($20.00/month), ChatGPT ($20.00/month), Claude Pro ($20.00/month)
Website Generator	input: text, output: Website	VAE	Framer	Framer ($10.00/month)

Table 5. Benchmark generative AI marketplace for AI model trading.

Name	Features	GenAI Type	Release Time	Limitations
Workday Marketplace [57]	Finance, HR, Planning, Industries	Text-to-Text, Text-to-Images	June 2024	lack of price information
Gravity AI [63]	Image Recognition, Product Recommendation, Exact Text from Images, Prediction, Search Through text, Production Ready Model, etc.	Text-to-Text, Text-to-Images, Text-to-Videos	March 2024	Must install their API clients. Has various service payment options.
DataStax [64]	chatbots, Data Integration (focus on data mining services)	Text-to-Text, Text-to-Images	October 2024	Must install their API clients. Pay as usage.
AI Marketplace by AI planet [65]	Speech, Natural Language Processing, Computer Vision	Text-to-Text, Text-to-Images, Text-to-Videos	AI planet was established in 2020	must provide personal information before trying the AI models
AKIRA.ai [66]	Text Analysis, Machine Learning, Computer Vision, Deep Learning	Text-to-Text, Text to Video, Text to Image, code generation	August 2023	lack of maintenance, lots of webpages cannot work properly.

Besides GenAI, lots of marketplaces were established to sell machine-learning models, a subset of AI models. These machine-learning models are predefined models that allow customers to train models with their own data. Table 6 itemizes some of the existing machine-learning marketplaces.

Table 6. Industrial machine-learning marketplaces for model managements.

Marketplace	Features	Strengths	Limitations
Amazon SageMaker [67]	Pre-trained models, real-time and batch inference, AWS integration.	Scalable, flexible pricing, secure hosting.	High GPU costs, limited customization, basic IP protection.
Google AI Platform [68]	Pre-trained models, AutoML tools, managed Jupyter Notebooks.	User-friendly, competitive pricing, advanced customization.	Vendor lock-in, privacy concerns, smaller catalog.
H_2O.ai Marketplace [69]	AutoML solutions, on-premises, and hybrid cloud support, explainable AI models.	Enterprise-grade features, open-source foundation, strong explainability.	Smaller catalog, slower innovation, limited user feedback mechanisms.
Hugging Face [70]	Community-driven, pre-trained models for NLP, vision, and speech, open-access API.	Free access, cutting-edge NLP models, and strong community collaboration.	Lacks enterprise-grade security and privacy features, inconsistent quality, and no standard pricing.

Our study employs a three-dimensional problem space as Figure 2 to explore the potential for leveraging existing AI models with commonly shared functional capabilities. The analysis focuses on variations in data resources, potential hardware investment requirements, and labor resource utilization, highlighting the feasibility and implications of these factors in optimizing AI model deployment. For example, ChatGPT 3.0 is a text-to-text GenAI. Based on the problem space designed for the existing AI models marketplace (Figure 2), the data type is text only. The data acquired is public. The GenAI model uses VAE, TBM, and LM; therefore, the training AI model needs a large dataset. According to ChatGPT published data, for ChatGPT3, the pertaining dataset size is 45 TB [71]. Due to the extensive data requirements, ChatGPT relies on GPUs and ASICs to enable rapid response times and manage large-scale language processing tasks. Significant computational resources and multiple AI models are employed to fulfill performance requirements. Suppose a new AI product with similar functionality to ChatGPT is introduced. In that case, pricing for this model can be benchmarked against ChatGPT's current pricing, such as a monthly subscription, which is recommended for the GenAI model itself. A model developed on top of ChatGPT, the recommended selling price would reflect ChatGPT's base price plus an additional amount for any newly introduced features.

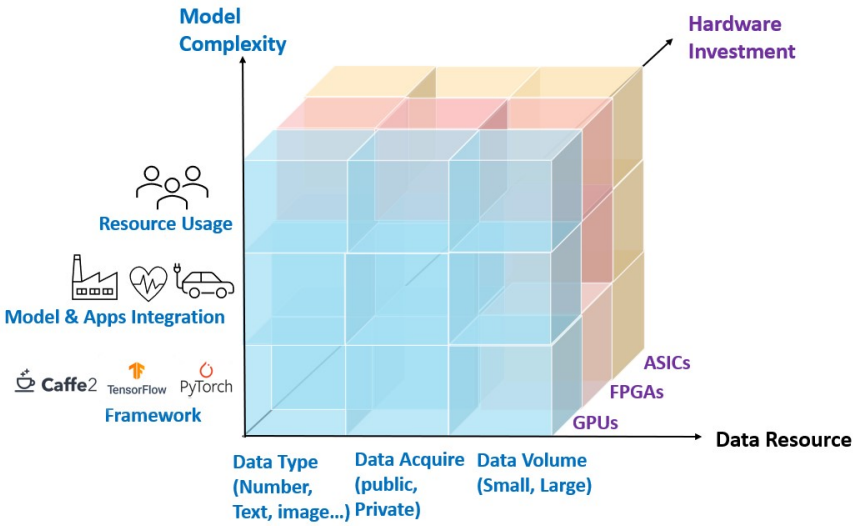

Figure 2. AI marketplace price model (data concentration).

AI marketplace focused on promoting existing AI models should provide services with general tasks such as ChatBots to answer customer questions, HR products to predict

and track employee performance, etc. These AI models should be made available within a predefined catalog to support users' dynamic decisions, enabling key services such as model comparison, differentiation analysis, and price recommendations for sellers and buyers. In addition, if a buyer requests modifications to an existing model, the AI marketplace will mediate between potential sellers and buyers. The platform can even provide a bidding mechanism, allowing both parties to negotiate and reach a mutually agreed-upon price.

2.2. Marketplace for Customized AI Models

GenAI models are typically trained on extensive, diverse datasets, a process that demands significant computational resources, and data access is only available to leading technology giant companies, such as IBM, Google, OpenAI, and Nvidia. In contrast, specific AI or narrow AI products are targeted to finish one specific task. These tailored AI systems require specialized datasets, customized model architectures, and a focused alignment with operational requirements, making them fundamentally different from large, generalized GenAI models. Compared to the GenAI, specific AI heavily relies on specific datasets to train its model. Compared to the problem space designed for the existing AI models, the specific AI model is heavily affected by industry types such as higher education or government. Figure 3 demonstrates the AI trading market according to the different domains on which the AI model needs to focus. Its *X*-axis shows the domains in the AI model that need to be developed, such as manufacturing, finance, hospitals, education, and government. The *Y*-axis still focuses on the complexity of the AI model, and the *Z*-axis indicates the special policies or laws that need to be followed.

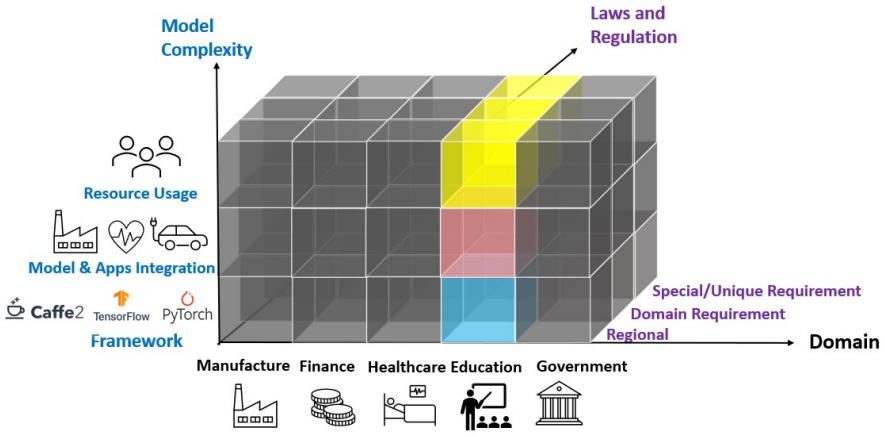

Figure 3. AI Marketplace price model (domain concentration).

Such an AI model demands cooperation between the AI model developer and the AI model seeker. Using the Education System as an example. According to UNESCO, there are six challenges related to AI in education: Comprehensive Policies, Equity and bias, Continuous Development for Educators, High-Quality Data, Robust Agenda, and Ethical Use [72,73].

Southworth et al. [74] proposed to develop a project to create an AI curriculum model for the University of Florida (UF) to be used among all 16 UF colleges. Such kind of AI tools can integrate policies and ethical data usage into curriculum development. Data input will be narrowed down to UF colleges, and the training model framework needs to follow UF's Course-based Undergraduate Research Experience (CURE). Such an AI model needs to be customized to the user's expectations. Thus, cooperation between the model developer and model seeker is needed to develop the AI model, including data input, model test, and model performance evaluation.

In our AI marketplace problem space based on the Domain Concentration (Figure 3), the Domain chosen for this AI model belongs to Education. For the direction of the model

complexity, the framework is CURE (UF's own framework). The model needs to integrate AI models used in the course assessment [74], and resource usage covers students and industry leaders such as NVIDIA [74]. For the direction of the Laws and Regulations, the model needs to follow Domain requirements in the Education system, such as no students' sensitive information being collected or revealed, removal of privacy information during curriculum development, adding future career sections that cooperate with the latest trends in the career area [74], it also needs to satisfy special requirement such as only apply to the UF. Thus, the price for the model needs to be reviewed and discussed between the seller and buyer based on all these specifications.

The AI marketplace should provide the following services to the buyer: potential AI model developer (who can be able to leverage the AI model inventory to identify sellers who have developed similar products), existing AI model samples for performance verification purposes, price and recommended development time for each existing AI model, and similar product in other industries for comparison just like that of the Education.

In the meantime, the AI marketplace will send notifications to potential sellers, asking for their interest in developing a new AI model and the potential cost range for the model. Compared to the GenAI marketplace, the Domain-focused AI marketplace focuses on Cooperation, Utilization, and Customization for AI model development and provides services such as AI model platform reviewing, price, and lead time estimation. Of course, the whole process needs to be protected to avoid information leakage during the AI model negotiation process. Table 7 lists the existing AI marketplace that supports customization for the AI model.

Table 7. Current customized AI marketplace overview.

Name	Features	Release Time	Limitations
AI Marketplace by AI Planet [65]	Based on Deep-Learning Models (such as LLama 3, Zephyr-7B, etc.), or industry (such as medical, tutorial, etc.)	AI Planet was established in 2020	must provide personal information before trying the AI models
DataStax [64]	supports vector, structured, and unstructured graphs, knowledge graphs, and streaming data	October 2024	Must download their API with their service to customize AI models
AI Marketplace by Info-Tech [75]	enable users to choose AI vendors, categories, or use cases	August 2023	Must provide personal information to review individual AI models
Instructure [76]	Develop AI models that can be used by Canvas system	September 2023	Education only. Only AI model for Canvas System
AI Marketplace by Solidus AITECH [77]	various AI models, like application store, let customers review and pick by themselves.	October 2024	Must be a membership of AITEch. Currently, only has 50 AI models.
Gravity AI [63]	Image Recognition, Product Recommendation, Exact Text from Images, Prediction, Search Through text, Production Ready Model, etc.	March 2024	Must install their API clients. Has various service payment options.

2.3. Current AI Marketplaces Review

Based on the identified and adopted six (6) characteristics as depicted in Figure 1, a comparison result is summarized by Table 8. It is evident from Table 8 that most of the current AI marketplaces are focused on providing a platform for existing AI models but with minimal or no room for modification. Most AI marketplaces do not provide pricing information; only if the user provides personal information then the AI marketplace establishes the connection between the user and the seller. Gravity AI is the only platform that provides clear pricing information for users to consider. Akira AI claims to provide a global AI marketplace on its website, but the output is not convincing.

Table 8. Current AI marketplace review.

Name	Exiting Model	Customized Model	Cooperation	Pricing Service	Customization	Utilization	Privacy and Policy	Asset Management
Workday Marketplace [57]	Yes	Yes	No	disclosed only if personal information is provided to the sellers	No	No	Yes	Yes
DataStax [64]	Yes	Yes	Yes	No	Yes	Yes (Nvidia)	No	Yes
AI Marketplace by Info-Tech [75]	Yes	Yes	Yes	No	Maybe	No	No	Yes
Instructure [76]	Yes	No	No	Free	No	No	Canvas Education System only	Yes
AI Marketplace by Solidus AITECH [77]	Yes	No	No	Yes	No	No	No	Yes
Gravity AI [63]	Yes	Under development	No	Yes	No	No	No	Yes
AI Marketplace by AI planet [65]	Yes	Yes	Yes	Free Trial with membership	Maybe	No	No	Yes
AKIRA.ai [66]	Yes	No	No	Free Trial, but most of them are not available	No	No	No	Poor maintenance. Some AI models no longer exist
Amazon SageMaker [67]	Yes	No	No	2 months free trial, then pay by usage	No	No	No	Yes
Google AI Platform [78]	Yes	Yes	No	$300 free credit, then pay by usage	Yes (type in questions to receive recommended AI models)	Yes (integrate multiple models)	No	Yes (based on user case or data type)
H_2O.ai [69]	Yes	No	No	free trial, cloud service is $50,000 per unit per year	No	No	Yes	Yes
Hugging Face [70]	Yes	Yes	Yes	free, pro member needs to pay monthly subscription fee	Yes	Yes	No	Yes

Following the detailed review conducted on the existing AI marketplaces, we have identified a gap in the availability of dedicated comprehensive pricing services. Moving forward, this research will examine the pricing services within the AI marketplace. This component is crucial for AI model developers, as it provides essential guidance for setting competitive and appropriate market prices, which are mostly less considered by the existing AI marketplaces.

3. AI Model Lifecycle

This section defines the AI model lifecycle and reviews the existing efforts in an attempt toward an ideal model marketplace design.

3.1. AI Model Life-Cycle

AI models in marketplaces transit through a sequence of processes as their life-cycle. The cycle ranges from training, pricing, trading, and tracking the intellectual property's performance in the production environment after leaving the marketplaces. Below is a brief description of the different stages in the model life-cycle as depicted in Figure 4.

Problem Definition: In this phase, a potential model seeker defines and formulates the problem to be solved after understanding the use case requirements, its scope, and the specific questions the model needs to answer. Ideal problem definition guides the data selection required for the use case. Ensuring the data are relevant, sufficient, and of good quality is essential. This definition guides the seeker's decision on the best way of finding a model that satisfies the need.

Model Training: When the model seeker decides to explore the marketplace option to find the best-performing model for the problem, it may be due to a lack of efficient training resources from her end or expertise to train models. This phase enables the seeker to join the marketplace as a model buyer. The broker mediates between the buyer and the data owner(s) to train the required model.

Pricing and Trading: This entails assigning financial value to the trained model to facilitate trading. In this phase, the broker assigns prices to the trained model to compensate the data owners, satisfy buyers' utility requirements, and generate a profit for herself based on the services rendered.

Model Tracking: This entails continuously monitoring the intellectual property's (model) performance in the production environment. This includes tracking its accuracy, handling data drift, and updating the model to maintain its effectiveness. Similarly, the sold intellectual property needs to be tracked against any set of impropriety.

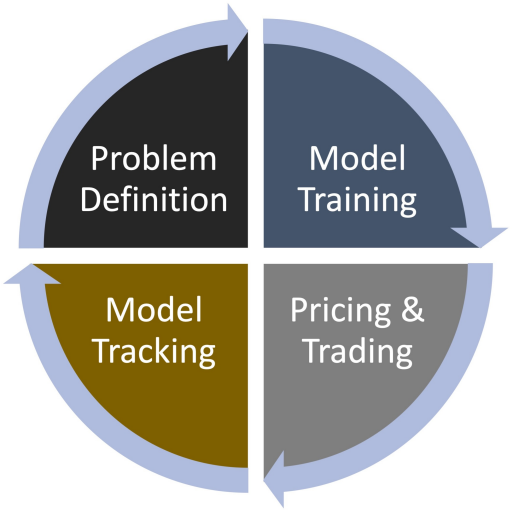

Figure 4. AI model life-cycle in AI marketplace.

Significant research focuses on the model training phase, i.e., centralized, decentralized, or distributed (federated) settings. In the subsequent sections of this article, our focus will be narrowed down to the pricing and trading phase, followed by the tracking, and then finally, the marketplace security. Specifically on pricing and trading, we reviewed the existing pricing schemes and trading platforms, developed a problem space to categorize them, and made some remarks to guide their extension in the future in Section 4.

3.2. AI Model Value Chain

This subsection describes the value chain passed by the model in an ideal marketplace [9,24,79]. The various components of this chain comprise the following: (i) *Buyer:* A market stakeholder joins the marketplace to purchase or license a model to address a specific use case requirement. Model buyers rely on brokers to provide reliable and high-performing models. (ii) *Broker:* The intermediary facilitating transactions between buyers, developers, and data owners. Brokers ensure smooth operations, compliance with marketplace regulations, and trust among the various stakeholders. AI marketplace can be used to take over a broker's role to simplify the overall process. (iii) *Developers:* They are responsible for training models. They depend on data owners for high-quality datasets while collaborating with brokers to sell and distribute the trained models, and (iv) *Data owner:* He or she provides the required dataset for training models, playing a significant role in data quality, diversity, and ethical sourcing. (v) *Standardization:* It connects the various stakeholders (i.e., data owner, developer, broker through the marketplace) to enable interoperability, collaborative development, standards enforcement, and trust. (vi) *Open source:* It is linked to "Developer" and "AI Marketplace" to demonstrate the impact of tools, shared models, and the available resource pools for cost reduction, faster innovation, and transparent democratization of AI. Figure 5 depicts the relationships and dependencies among the various marketplace stakeholders.

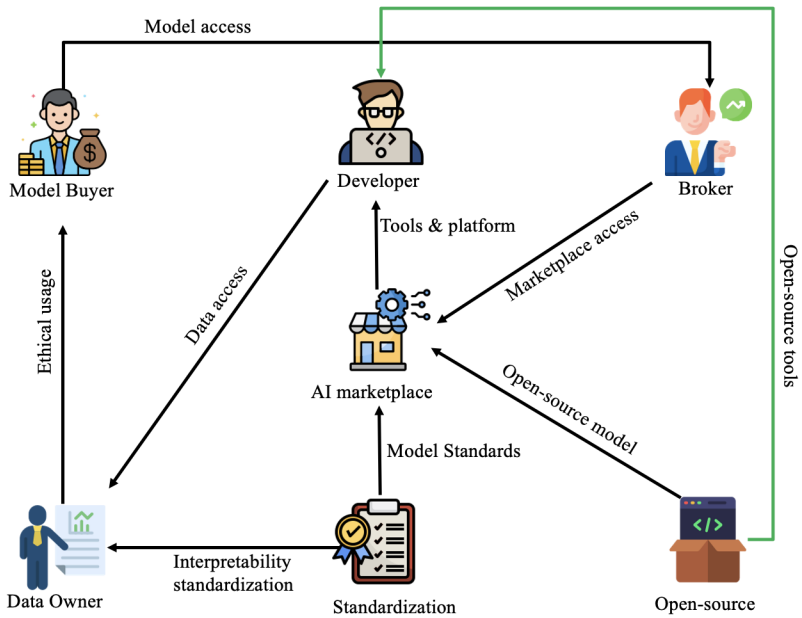

Figure 5. AI model value chain in marketplace.

Some of the constraints in this value chain include ethical (Bias, discrimination, data misuse), legal (i.e., privacy regulations (GDPR, CCPA) and intellectual property laws), economic (pricing disputes and fair compensation for data owners), technical (data quality, interoperability, model transparency), etc. Integrating standardization and open source

in the value chain could mitigate some of the identified constraints in the areas of interoperability, transparency, cost reduction, and regulatory compliance. However, open source and standardization could not resolve all the constraints. There is room for further reinforcement with a strong governing council framework fostering collaboration among the concerned stakeholders to provide continuous updates to address emerging challenges [80–85].

3.3. Frameworks for AI Model Marketplaces

Representative efforts have been recorded proposing frameworks as a reference point for a viable marketplace design. For instance, Kumar et al. [9,20] proposed to provide the regulating guidelines behind the design of AI marketplaces that facilitate the sharing of models between its participants. Dhamange et al. [38] provided the guidelines to catalyze the production of quality data for model training within marketplaces. Likewise, Sarpatwar et al. [86] presented blockchain as a tool that preserves privacy, enables fairness and gives room for audit in AI marketplaces, while Nizamis et al. [32] developed *"KnowlEdge"*, a smart contract-based platform to demonstrate model trading in Industry 5.0. Table 9 summarizes their contributions in an attempt to yield a marketplace suitable for this day's and the next generation's pervasive AI models.

Table 9. Representative AI frameworks for AI marketplaces.

Reference, Year	Objective (s)	Contribution	Future Research Direction
Ref. [86], 2019	Trust and fairness in AI marketplaces	Demonstrated blockchain's suitability in preserving privacy, fairness, and trust in AI marketplaces	Federated learning, blockchain for skepticism and threat-free AI marketplaces
Ref. [20], 2020	Design of AI diffusion mechanisms in decentralized marketplaces	Regulatory guidelines (technical and economic) for enabling the effective and efficient development of decentralized marketplaces.	Federated learning for decentralized, privacy-preserving marketplaces
Ref. [38], 2022	Provision of quality data marketplaces for AI models	Regulatory guidelines governing the operating procedures of AI marketplace actors (producers and consumers)	Modeling and Simulation toolkits for the real-world demonstration of AI markets.
Ref. [32], 2023	Model trading platform for smart manufacturing domain	Knowledge, a smart contract-based market to prototype model trading in industry 5.0	Threats-free, robust and standardized model trading markets for industry 5.0 era.

4. Model Pricing and Trading

Pricing defines a value to the model to satisfy buyers' requirements, compensate data owners based on their training contributions, and allocate the difference between the two as profit for the broker based on the services rendered. This section utilizes the problem space (depicted by Figure 6) to explore pricing and review the existing pricing schemes in the marketplace to determine the most effective scheme that best fits an ideal AI marketplace. Table 10 summarizes their contribution and the areas of improvement.

Table 10. A summary of model pricing schemes.

Ref, Year	Scheme; Technique	Objectives (s)	Approach	Remarks
Ref. [41], 2019	Model-based pricing Noise Injection	Arbitrage Freeness Revenue Maximization	Gaussian noise injection generates model instances with varying accuracy and pricing points. Dynamic programming then determines the optimal pricing strategy to maximize revenue under given constraints.	(i) The pricing function is limited to models with convex objectives. (ii) It lacks support for dynamic features or model selection. (iii) Privacy preservation is not addressed.
Ref. [87], 2020	Dealer Dynamic Programming	Arbitrage Freeness Revenue Maximization Privacy Compensation	Shapley coverage enables budget-based model training, while dynamic programming optimizes arbitrage-free pricing to maximize data owner revenue.	(i) The pricing scheme struggles with Shapley's computational cost and dynamic buyer demands. (ii) Market surveys for buyer price functions add system overhead.
Ref. [88], 2020	Auction Reinforcement Learning	Welfare Maximization	Auction strategies ensure truthfulness and rationality, encouraging data owners to join the wireless federated learning market.	(i) Privacy preservation can further incentivize data owners' participation.
Ref. [89], 2020	Game Theory Sharpley Value	Fairness Welfare Maximization	Shapley value evaluates data contribution, sets model rewards, and optimizes Gaussian noise variance to balance rewards.	(i) Noise injection for model rewards needs privacy-utility trade-off analysis for privacy-critical use. (ii) Privacy-preserving pricing in a federated setting is a good direction.
Ref. [90], 2022	Golden Grain Genetic Algorithm	Fairness Revenue Maximization	Sellers fair revenue allocation and buyer utility, modeled and solved as a bi-level optimization problem using a genetic algorithm	(i) Off-chain datasets for pricing evaluation risk bias and privacy leaks. (ii) Performance-based pricing should adapt to marketplace dynamics like demand and competition.
Ref. [91], 2022	Develop Differential Privacy	Revenue Maximization Privacy Compensation	The broker minimizes training costs by contracting cost-efficient data owners and uses optimal pricing to maximize revenue and profit.	(i) Arbitrage freeness in a federated market setting is a good direction.
Ref. [92], 2022	FL-Market Auction	Privacy Compensation	Employs an auction mechanism to compensate data owners based on the level of private information disclosed for training, while the aggregation mechanism optimizes the utility of the global model.	(i) DM-RegretNet is designed to be approximately truthful. There is room for securing the system against strategic stakeholders. (ii) Arbitrage freeness in privacy-preserving auctions is a good direction.

Table 10. *Cont.*

Ref, Year	Scheme; Technique	Objectives (s)	Approach	Remarks
Ref. [93], 2023	Markov Decision Process Dynamic programming	Revenue Maximization	MILP prices the performance metrics, and buyers' decisions across the several performance metrics were modeled as MDP and solved using dynamic programming	(i) Performance-based pricing may lead to suboptimal outcomes, affecting buyer satisfaction and market efficiency. (ii) Using performance metrics and data augmentation risks privacy leaks, especially with sensitive data.
Ref. [94], 2024	Auction; Federated Auction Template	Truthfulness Welfare Maximization	A performance-based auction ensures fair compensation to data owners, aligned with model quality and performance.	Extending the auction template to address constraints like privacy and exact truthfulness could prevent stakeholder manipulation and enhance effectiveness.
Ref. [95], 2024	Auction; Nash Equilibrium	Revenue Maximization, Fairness	A two-tiered auction; the first-tier optimizes data owner selection, while the second-tier prices the trained models	(i) Relying on data owners' reports may lead to suboptimal selection and pricing, affecting efficiency and fairness. (ii) Privacy considerations are deferred for future research.
Ref. [96], 2024	Auction; Reinforcement Learning	Welfare Maximization Truthfulness	Model performance determines pricing, and the RL-based allocation function optimizes the auction process to maximize revenue irrespective of the market operating dynamics.	(i) Limiting model sales per auction affects market flexibility and trading volume. (ii) Exploring truthfulness and privacy in FL markets is a promising direction.
Ref. [97], 2024	Auction; Homomorphic Encryption	Privacy Preservation Security	Private model auctions implemented under a ciphertext state to demonstrate secure and private pricing	(i) Encryption and secure auctions may hinder real-time applications due to overhead. (ii) Privacy preservation needs privacy-utility analysis to aid buyer decisions.

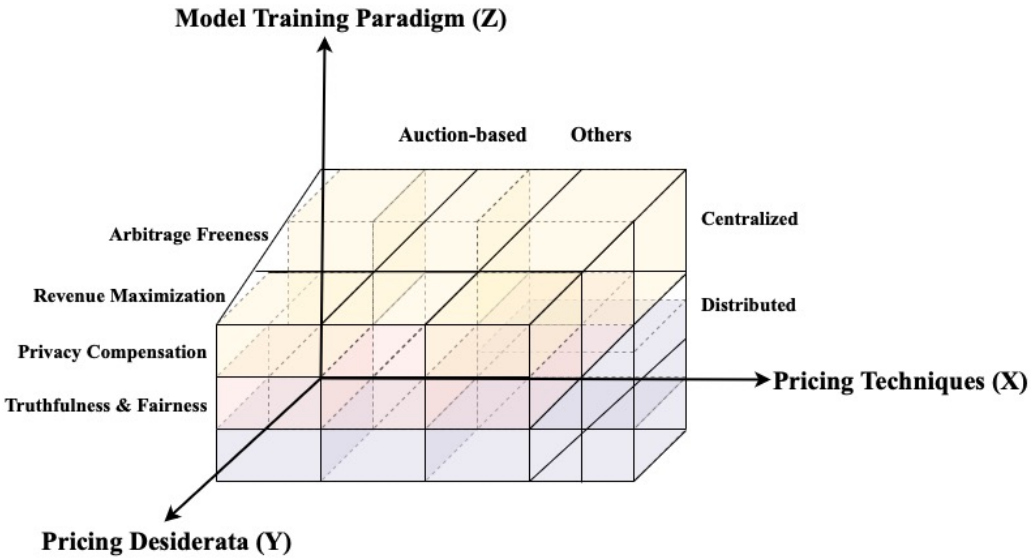

Figure 6. A taxonomy of pricing in model marketplaces.

4.1. Model Pricing Schemes

The framework defines and categorizes the existing pricing schemes described below.

4.1.1. Pricing Desiderata (*Y-Axis*)

Pricing desiderata are the axioms or properties to be satisfied by a pricing scheme to be considered fair, effective, and applicable. Like other digital products markets, in model trading marketplaces, these desiderata ensure that pricing techniques align with both sellers' and buyers' needs and the overall market dynamics. In the following, we brief some of these axioms.

Arbitrage freeness: Arbitrage-free property ensures that buyers cannot exploit pricing inconsistencies. It guarantees that models with higher accuracy or quality are always priced higher than those with lower accuracy or quality. It also prevents buyers from combining cheaper models to replicate the performance of more expensive ones. To achieve this, a pricing scheme must ensure buyers cannot take advantage of price differences among published model instances to maximize their utility at a lower cost, which would otherwise reduce the seller's revenue. A pricing function $F(x)$ is arbitrage-free if it is error-monotone, subadditive, and non-negative [41,87].

Revenue/Welfare Maximization: A pricing scheme is revenue-maximizing when it guarantees profit to the sellers (model owners). In a centralized trading setting, the broker facilitates the transaction between the seller and the buyer in a win-win manner. i.e., by ensuring that sellers' revenue is maximized at the same time, buyers' utility is maximized as well. However, in a distributed setting like federated learning, the welfare (benefit) is evenly distributed across the participating clients based on their active contribution to model training.

Privacy Preservation/Compensation: A pricing scheme should preserve the sellers' privacy or compensate appropriately based on the level of sensitive information (data) disclosed and utilized during model training. Differential privacy is one of the most famous techniques to prevent/minimize the disclosure of sensitive information in model training [91,92].

Truthfulness and Fairness: Truthfulness guarantees fairness in marketplaces, which can be viewed from different perspectives. From the data owners' side, some pricing schemes incentivize the data owners to reveal data of good quality for model training. Similarly, from the buyers' side, an effective pricing scheme should facilitate or guarantee

truthful valuation of model instances to the buyers while ensuring fair allocation of profit or benefit to the sellers. Sharpley value is one of the most famous techniques for guaranteeing fairness in digital commodity markets [98].

4.1.2. Pricing Techniques (*X-Axis*)

Pricing techniques are tools used to yield a financial value for models in the marketplace. The tools balance buyers' and sellers' interests and enable the coexistence of the marketplace stakeholders. The techniques are objectively categorized as below:

Auction-based: This is a dynamic pricing strategy where the price of a product or service is determined through a bidding process. In auctions, the bidding process enables buyers and sellers to interact and establish a fair market price based on demand and supply dynamics. Auction theory has been widely employed in both physical and digital commodity markets ranging from economics, big data, spectrum, electricity, and mobile markets, among others.

The key components and the processes that are assembled to make up the auction-based pricing in model marketplaces are as follows: (i) *Data Owners:* These auction components offer their data for sale or contribute to model updates in collaborative training to yield a benefit; (ii) *Model Buyers:* They are the auction components that bid for the required models to enhance their use case; (iii) *Broker*: It acts as the intermediary facilitating the auction process by collecting bids, determining winners, and managing payments; (iv) *Bidding:* This can be the case for both forward and reverse auctions in the model marketplace. As for the forward, i.e., from buyers to brokers, then brokers to data owners. For example, the buyer submits bids indicating the maximum price they will pay for a model. The broker activates the auction process to enable data owners to submit their bids, then selects the winners to train the model that satisfies buyers' utility; (v) *Allocation and Payment Functions:* The allocation function identifies the buyers that win the auction based on their bids. This function ranks buyer(s) and allocates the trained model to the highest bidder. The payment function calculates the payment to be made by the winner before the broker releases the model. In most marketplaces, payments are mostly based on the second-highest bid (second-price auction) to encourage truthful bidding.

An effective auction-based pricing mechanism is expected to be incentive-compatible, computation-efficient, and preserve individual rationality [91,94,95]. In model trading marketplaces, auction-based pricing can be objectively categorized into incentive-based, performance-based, and privacy-based.

As for the incentive-based approach, data owners are encouraged to actively participate in model training using their best-quality data. The mechanism achieves its goal by encouraging truthful bidding from the data owners using incentives and preserving individual rationality by the pricing function; this ensures that the data owners do not lose anything by accepting to join the trading process.

Related to this, Jiao et al. [88] proposed an auction-based strategy that incentivizes data owners' participation in a services market supported by federated learning. In their study, two auction mechanisms were leveraged so that social welfare could be improved in such a market. The first version employs a greedy approach to select data owners based on their bids and data quality, while the enhanced version leverages deep reinforcement learning and graph neural networks to automate the auction process. Both auction mechanisms ensure truthfulness and individual rationality among the participating data owners. The auction mechanism improves social welfare in the market by providing a better way of handling wireless communication and data distribution complexities.

As for the performance-based approach, some performance metrics are utilized. In that case, buyers bid based on the expected performance a model should provide, and

then data owners are compensated proportionally to the performance their model offers. Concerning this, Li et al. [94] proposed to incentivize resource-efficient data owners' participation in model training using auction-based pricing. The proposed flexible and extensible auction-based pricing mechanism compensates data owners based on the performance improvements achieved in model training. Furthermore, prototypes were utilized to demonstrate the extensibility of the auction scheme. These include *K*-winner federated learning (an auction mechanism that ensures truthfulness and individual rationality with a fixed number of winners), exponential mechanism (an approximate truthful auction that uses stochastic price selection to maximize data owner's profit), and random sampling (a dual-price auction mechanism that ensures truthfulness by partitioning buyers into groups and uses separate pricing for each group).

Sun et al. [95] proposed a two-tiered multi-attribute reverse auction framework. In their work, the first tier optimizes the data owners' selection process for model training. Similarly, the second tier (the pricing framework) leverages Nash equilibrium principles to fairly compensate the selected data owners based on the level of their data quality, computational resources utilized, and quality of the trained models. It maximizes the broker's revenue by strategically setting preference weights in the scoring function to align with the market conditions to guarantee profitability. Cui et al. [96] proposed to integrate auction theory with reinforcement learning (RL) in model marketplaces. The proposed auction mechanism utilizes performance gain as the main criterion to determine pricing. Buyers bid based on the expected performance improvement a model can provide, while the payment to the data owners is proportional to the performance gain their models offer to the buyers. The RL-based allocation function acts as a market operation solver that guides the broker in ranking buyers based on their bids to determine the winning buyers, optimize the auction process to maximize trading volumes, and adapt to dynamic market conditions.

As for the privacy-based approach, data owners submit bids based on their privacy budget and receive compensation based on the level of their privacy loss. Related to this, Zheng et al. [92] proposed *"DM-Regregnet"*, an auction mechanism that determines the level of privacy disclosed in model training and compensates the data owners accordingly. In their method, data owners report their privacy valuations, which reflect their willingness to accept privacy loss in exchange for compensation. Each owner specifies a privacy budget (the maximum privacy loss they will tolerate). The auction mechanism allows data owners to bid on their privacy loss, with the broker determining the privacy parameter and compensation based on these bids. *"DM-Regregnet"* works with an aggregation mechanism *"OptAggr"* to optimize the utility of the global gradient. This involves determining the optimal level of privacy loss for each data owner to maximize the accuracy of the aggregated model. Also, Li et al. [97] integrated privacy-preserving techniques (differential privacy) with an auction-based model to facilitate secure and efficient model sharing in federated model trading marketplaces. Their approach transforms model sharing into private auction models; symmetric homomorphic encryption is employed to securely sort bids and calculate prices without revealing the actual bid values to the parties involved in the auction, attribute-based encryption and the interplanetary file system ensure that only the winner has access to the shared model. In another study, Sun et al. [91] proposed to balance the trade-offs between the data owner's privacy protection, buyer's model quality assurance, and broker's profit maximization. In their method, the broker optimizes the selection of data owners for model training, strategically sets prices for the different model versions trained, and then employs a two-layer optimization framework to maximize her revenue (profit).

Other Techniques: These techniques range from noise injection (Gaussian and Laplacian), differential privacy, Shapley value, genetic algorithm, etc.

In an attempt to prevent arbitrage pricing in marketplaces, Chen et al. [41] proposed a pricing function that leverages the Gaussian noise injection mechanism to produce a range of model instances with different accuracy levels (versioning) and prices them accordingly. The function is designed to be arbitrage-free and error-monotone, ensuring fair pricing based on model accuracy. The function also includes a revenue optimization component to maximize the seller's profit while maintaining the buyer's affordability.

Effective model sharing or trading in marketplaces requires a fair and transparent product-compensation swapping method between the model developers and the users. Weng et al. [90] proposed to promote performance-based pricing (i.e., versioning using different datasets) in model trading marketplaces. In their method, the genetic algorithm jointly solves a bi-level optimization problem where the upper level maximizes the seller's revenue while the lower level maximizes the buyer's utility.

An effective marketplace should facilitate the achievement of its stakeholder's objectives. i.e., the broker should ensure that data owners are compensated while model buyers' utility requirements are ensured. For example, Liu et al. [87] proposed to integrate differential privacy and Sharpley value in the model trading marketplace by formulating compensation and pricing functions that account for the data owner's privacy and model buyer's utility while leveraging dynamic programming to optimize revenue maximization and privacy preservation jointly. The use of Shapley value and differential privacy parameter (i.e., epsilon) in these functions ensures a fair and competitive marketplace, balancing the needs of data owners, brokers, and model buyers.

Also, effective marketplaces shall encourage data owners to participate actively in model training. Along this direction, Sim et al. [89] proposed a structured and fair method for valuing data contributions and distributing rewards in a collaborative model development environment. The proposed approach ensures that parties (data owners) are incentivized to contribute valuable data, which are rewarded with a model in return based on the information gained from the contributed data, leading to the development of high-quality machine-learning models. Similarly, some marketplaces match model training data demand with an appropriate supply. For example, Han et al. [93] proposed to improve pricing in data-augmented model trading marketplaces. Their method leverages mixed integer linear programming (MILP) to yield a price curve that publicly assigns a price to each performance metric. Markov decision processes (MDP) were designed and solved using dynamic programming to facilitate buyers' traversal across the performance metrics and determine the optimal stopping time that balances costs and benefits.

4.1.3. Model Training Paradigm (*Z-Axis*)

From the data point of view, model generation or training can be categorized into centralized and distributed (federated) settings. In the centralized setting, the seller (data owner) transfers the data to the broker (central platform including data center, cloud, etc.), and the broker leverages its computational-efficient platform to train different model instances to be sold to the buyers after the equivalent payment is received. In the federated setting, the data remains within the custody of the data owners, while the broker facilitates the trading process by enabling model aggregation among the distributed data owners to yield a model that satisfies the buyers' utility requirements.

4.2. Model Development and Trading Platforms

Trading and pricing are related concepts that complement each other. Pricing assigns values to the models, while trading enables the sharing and exchange of models between the buyers and sellers. Trading platforms connect model trainers with potential buyers to streamline the process of acquiring high-quality models while providing a marketplace for

AI engineers to monetize their efforts. Table 11 summarizes the various trading platforms and the areas of focus in the future.

Kurtulmus et al. [99] proposed *"Danku"*, a protocol that works on the Ethereum blockchain to facilitate model development transactions between data owners and AI engineers. Somy et al. [100] proposed a ledger-based system deployed on the cloud to facilitate collaborative model development between stakeholders, i.e., data owners and AI developers. Weng et al. [90] proposed to address fairness in model trading marketplaces by ensuring buyers receive a model maximizing their utility. At the same time, sellers also receive equal compensation before the model is released to the buyer. In their method, intel's software guard extension (SGX) is utilized as a trusted off-the-chain execution environment to test and benchmark the advertised model; the recorded performance is offloaded to the Ethereum blockchain as an on-the-chain report that guides and determines the optimum price for the model. Likewise, Li et al. [101] aimed for a marketplace, trading models of high quality. In their proposed platform, smart contracts automate the trading process, while evolutionary game theory guides the interaction between the market participants.

In a model trading marketplace, the seller may aim to maximize its revenue by deceiving buyers. In that regard, Li et al. [102] proposed to prevent deception in model trading marketplaces. In their method, game theory is leveraged to dissolve any discrepancy between the advertised and the delivered model. Nguyen et al. [103] utilized distributed ledger technology to serve as a platform facilitating trustworthy/secure trading in IoT-driven markets. In their method, Shapley value incentivizes data owners' involvement, determines the trained model's quality, and compensates the data owners fairly to maximize the buyer's utility.

Also, Mai et al. [104] proposed a two-way auction strategy that leverages reinforcement learning (RL) to facilitate model trading between data owners and federated learning platforms. The bi-directional auction driven by RL facilitates dynamic decision-making in the multi-agent markets. Yousafzai et al. [105] proposed to encourage/incentivize resource-constrained entity's participation in collaborative model development. Likewise, Song et al. [106] proposed a marketplace that gives room for testing model efficiency/performance on a given use case before purchase.

Table 11. A summary of model development and trading platforms.

Reference, Year	Scheme or Technique	Objective (s)	Approach	Future Research Direction
Ref. [99], 2018	Danku Protocol; Blockchain	Trustless, Broker-free, model generating market	Leverages Ethereum blockchain to yield a model development marketplace	Encryption-based, computation-efficient model development markets
Ref. [100], 2019	Hyperledger Fabric; Blockchain	Collaborative, decentralized model development market	The Hyper-ledger-based market deployed on the cloud facilitates model development between the stakeholders in an ownership-preserving manner	Homomorphic encryption to complement federated learning in decentralized model markets
Ref. [106], 2021	Primal; Cloud-based marketplace	Model training data efficiency testing broker	The platform facilitates collaboration between the model owner and the data shopper in privacy-preserving manner	Primal framework for distributed trading marketplaces
Ref. [90], 2021	Golden Grain; Ethereum Blockchain	Broker-free, fair model trading market	Leverages SGX to test and validate model performance, then passed to Ethereum blockchain for pricing and transaction	Multi-buyers and fault-tolerant trading markets
Ref. [103], 2021	Distributed ledger; Blockchain	Model trading in IoT-driven market	Shapley value determines model quality and guides the fair interaction/transaction between the data owners and model buyers	Fault-tolerant, distributed trading markets

Table 11. *Cont.*

Reference, Year	Scheme or Technique	Objective (s)	Approach	Future Research Direction
Ref. [104], 2022	Auction; Reinforcement learning	Dynamic, multi-agent model trading market	RL-Based double auction for broker-free trading markets	Revenue and welfare maximizing frameworks for multi-agent markets
Ref. [101], 2023	Smart Contracts; Blockchain	Incentive/Feedback to guide model trading markets	Leverages game theory to quantify the received feedback, for high-quality model	Effective pricing scheme for model trading markets
Ref. [102], 2023	Game Theory	Information verification driven markets	Model update and delivery were modeled as a cooperative game process to halt the chances of deception in between.	Multi-buyers with diverging utility functions model trading markets
Ref. [107], 2024	NOSTR protocol	Communication protocol in model trading markets	Leverages NOSTR to demonstrate model training for money compensation in decentralized markets	Smart contracts for information and computation verification in relay-messaging-based markets

In summary, we have reviewed the existing pricing schemes and trading platforms. It is evident from the existing efforts that pricing schemes and trading platforms that are efficient (arbitrage-free, computation-efficient) and robust against privacy and security threats remain open for further research. Among the feasible directions for broadening this area of research is marketplace design (i.e., auction mechanisms) that balance performance efficiency and robustness against privacy and adversarial threats in future AI model marketplaces.

5. Model Tracking and Protection

5.1. Model Tracking

It is natural that model performance can degrade over time. This could be due to a shift or disparity in data distribution that could emerge between the training data and the model application context [42]. Thus, model tracking in this context entails the ongoing process of monitoring AI models deployed in production to ensure their performance, reliability, and compliance over time. This involves tracking metrics such as accuracy, latency, and error rates to detect issues like data drift, where changes in the input data distribution negatively impact model predictions [108]. Advance model tracking also includes techniques like digital watermarking, which embeds unique identities in models or their outputs to trace their usage and ownership, ensuring compliance with intellectual property agreements [109].

Furthermore, blockchain technology is increasingly used for tracking, as it provides an immutable ledger for model transactions and ownership verification, enhancing transparency and trust in AI marketplaces [110]. Tools like API usage monitoring and anomaly detection systems further enable providers to track where and how models are being used, identifying potential misuse or tempering. Regular updates or retraining mechanisms are often incorporated to adapt models to new data, preserving their utility and value in dynamic environments [111]. By combining these technologies, model tracking ensures that AI systems remain robust, secure, and aligned with their intended use cases.

5.1.1. Performance Metrics for Model Tracking

AI model tracking ensures performance, reliability, and compliance in dynamic operational environments. Over time, the deployed AI model performance can degrade due to data drift, i.e., changes in input data distribution or evolving application contexts. This

degradation impacts the models' accuracy, reliability, and utility, making robust tracking mechanisms indispensable for ideal AI marketplace operations.

Key performance metrics play a central role in effective model tracking. Accuracy remains a foundational metric, ensuring the model makes correct predictions or classifications based on current input data. Latency is equally critical, particularly for real-time applications like fraud detection, where low processing times are essential. Error rates, such as mean squared error (MSE) or classification error rates, help identify deviations from expected performance levels. Precision and recall balance false positives and negatives for classification tasks, maintaining the model's effectiveness. Drift detection scores are another important metric, and statistical tools are leveraged to monitor divergences between training and production data distributions, enabling early intervention when issues arise. Resource utilization metrics, such as CPU or GPU usage, help track infrastructure constraints, ensuring models operate efficiently within system limits. Together, these metrics form the backbone of a robust AI model tracking mechanism, ensuring models remain reliable and effective in ever-changing environments. Figure 7 embeds the performance metrics in the chain in an attempt to yield a framework that guarantees the proposed value to the marketplace customer.

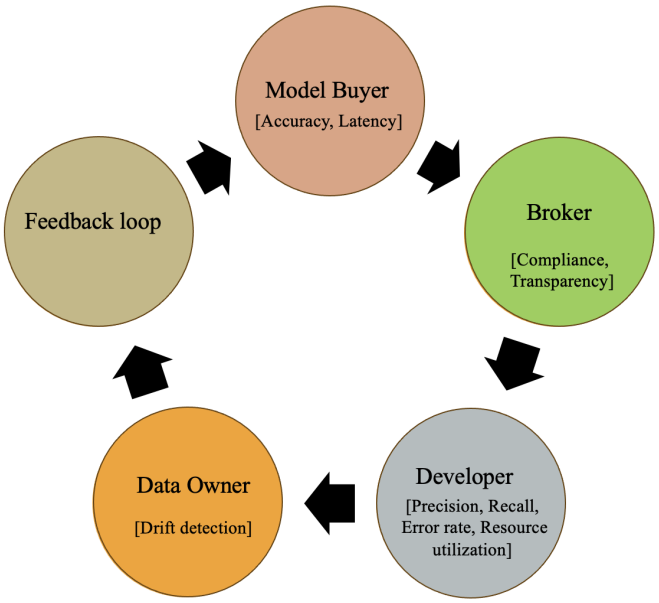

Figure 7. Performance metrics in the model value chain.

5.1.2. Tools and Techniques for Model Tracking

Integrating these performance metrics and tools ensures that the AI marketplace delivers consistent value to its customers. Some of the tools include:

- *Digital Watermarking:* This ensures compliance with intellectual property agreements and prevents unauthorized duplication or usage.
- *Blockchain Technology:* It provides a decentralized and immutable ledger to record model ownership, usage history, and transactions. This enhances transparency and trust in AI marketplaces.
- *API Usage Monitoring:* It tracks the number and nature of API calls made to the model, identifying patterns of misuse or unusual activity. These insights are invaluable for service-level agreement (SLA) compliance.
- *Anomaly Detection Systems:* It detects unusual patterns in model predictions or usage, flagging potential tampering or unauthorized activities.

- *Regular Model Retraining:* It incorporates periodic updates or retraining mechanisms using new data to adapt the model to evolving contexts and preserve its utility.
- *Logging and Monitoring Dashboards:* Tools like Grafana or Prometheus provide real-time insights into performance metrics, enabling rapid responses to detected issues.

Continuous monitoring of latency, accuracy, and error rates guarantees reliability, while blockchain and watermarking enhance transparency by providing verifiable proof of ownership and compliance. Retraining mechanisms ensure adaptability to evolving environments, and anomaly detection safeguards security by preventing tampering or misuse. Additionally, resource utilization monitoring promotes cost efficiency, ensuring optimal operations and reducing unnecessary expenses for both providers and customers.

5.2. Marketplace Security

Security is the last part of every application domain. Hence, the AI marketplace study will not be complete without exploring the privacy and security vulnerabilities that could emerge while the marketplace is operating. Figure 8 presents the threat model depicting the emerging privacy and security concerns, which necessitates the development of a secure and threat-free environment for tomorrow's AI marketplace.

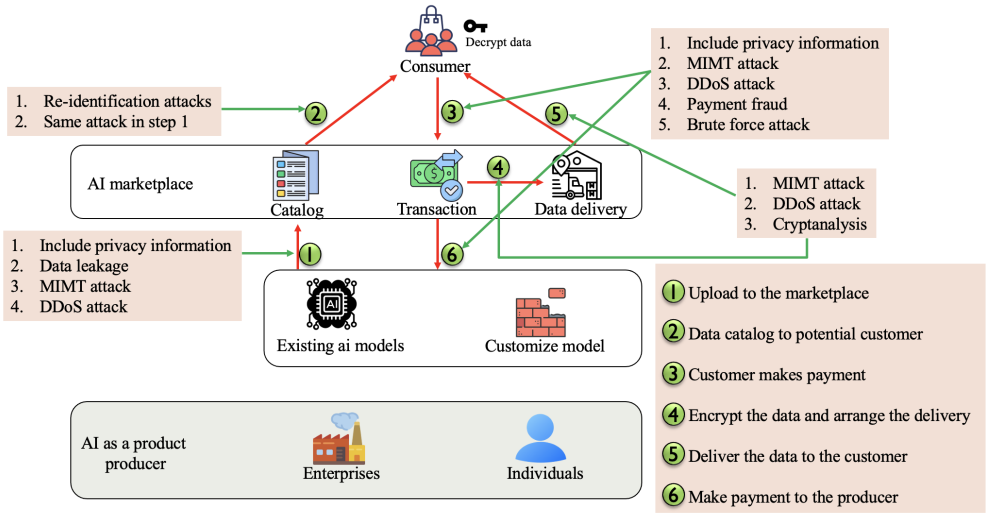

Figure 8. A threat model for AI marketplace.

Evident from Figure 8, adversarial marketplace stakeholders, such as data owners, model buyers, etc., could launch man-in-the-middle (MITM) or distributed denial of service (DDoS) attacks or even infer sensitive information while uploading to or downloading from the marketplace. Similarly, brute attacks could be launched to bypass the system's authentication mechanism and engage in payment fraud by the model buyers. Skilled hackers could also leverage cryptanalysis to intercept and decrypt the system's communication messages without obtaining the actual keys.

Several techniques were explored and utilized to enhance the AI marketplace's robustness against integrity and security threats. For example, blockchain technology, widely used in the financial industry for its transparency and immutability, was proposed to securely record and protect model development transactions [86,99]. Blockchain can avoid security threats such as MITM, preserve marketplace stakeholders' privacy, and avoid data leakages. Other methods, such as token-based authorization, were proposed to ensure that only authorized users have access to the AI models [32]. Some recommendations include implementing multi-factor authentication (MFA) during the authentication process to minimize the risk of re-identification threats [112], even considering adding location

information to ensure only consumers in specific regions have the right to order AI models [113]. Also, to mitigate the distribution of sensitive data across AI models within the AI marketplace, federated learning approaches [88,114] have been adopted, which enables users to train models locally on their devices, eliminating the need to upload data to central servers for integration.

6. Challenges and Future Directions

Our review reveals that most available AI trading markets follow the structure of application marketplaces. These platforms focus on listing various AI models with different categories, leaving the burden on customers to independently select suitable models without providing adequate guidance or support. Representative efforts target the realization of ideal AI marketplaces, such as auctions in distributed (federated learning services) market settings [88,115], performance-based pricing in centralized market settings [116,117], to enhance their structure and functionality. However, challenges in the following areas require the research community's attention.

- *Lack of Standardization:* AI models often lack uniform templates or formats, and the use of diverse datasets for training further complicates their integration and reuse across different platforms. An ideal AI marketplace should address this issue by standardizing feature descriptions, listing comparable attributes across AI models, and providing users with tailored suggestions to facilitate informed decision-making.
- *Price Efficiency:* Many platforms leave price information undisclosed, requiring customers to contact developers directly for demos and pricing details. This approach lacks transparency and shifts the burden onto sellers, who may struggle to determine appropriate pricing, leading to undervalued or overpriced. In addition, it provides risks that customers might contact the developers directly, bypassing the AI marketplace, and the marketplace is only treated as the information provider rather than a platform to control and monitor the trade of the AI model. An ideal AI marketplace should offer price recommendations, ensuring maximum price efficiency while safeguarding the interests of both sellers and buyers and developing loyal customers and suppliers. Several studies have explored pricing efficiency in this context, such as performance-based auctions in the marketplaces to maximize seller's profit. However, these efforts are still in their theoretical conceptual stage, which needs to be transited to fruition to prove their efficiency.
- *Policy:* Policies related to AI models, such as intellectual property protection, as well as industry-specific regulations like HIPAA in the healthcare sector, must be effectively regulated and enforced by the AI marketplace. This oversight is essential to ensure that all AI models sold on the platform comply with applicable legal and ethical standards, therefore safeguarding both developers and end-users [118].
- *Ease of Operation:* Many existing platforms categorize AI products based on technical aspects, such as deep-learning frameworks, rather than industry-specific applications. Some AI marketplaces provide user cases for customers to refer to but lack demo samples for customers to try. This approach creates significant challenges for non-technical customers who may lack expertise in AI model development, making it difficult for them to identify and select appropriate solutions for their needs.
- *Privacy:* To promote AI models, some AI platforms offer free trials, allowing customers to evaluate performance before making a purchase decision. However, these free trials often lack adequate protection measures. Users can gain access to these demos by providing fake information, such as an email address or company details, and then implement the models on their own computers. This creates risks, including the unauthorized distribution of samples to third parties or the replication of demo

models, which cannot be effectively monitored or controlled. How to find a balance point between AI model promotion and AI model protection will be a challenging task for the AI marketplace to consider. The ideal situation should be to provide an easy way for customers to try the AI model in the AI marketplace platform rather than download the AI model to their computers. For instance, DataStax is built with NVIDIA AI and provides a platform for registered members to try the AI models on their designed virtual IDE. Online service is provided if a customer has any questions about the development of the AI model. However, DataStax requires its members to have strong technical backgrounds, understand databases, know how to do data mining, etc.

- *Security*: AI being a double-edged sword. AI models are vulnerable to attacks, such as adversarial attacks, model inversion and evasion, reverse engineering, etc., which can threaten intellectual property and data confidentiality. AI marketplace requires an end-to-end safety and protection mechanism to safeguard and protect AI models and detect any potential threats targeting AI models or even the marketplace itself.
  Similarly, users need to trust the models they are using, especially in critical applications in the field of healthcare or finance. Clear documentation on how models work, their limitations, and their training data is essential. Target training is necessary to provide such kind of support from the AI marketplace. A follow-up evaluation is also needed to ensure users use the AI model properly. Providing such kind of training to users quickly and properly is another challenge that the AI marketplace needs to consider.
- *Future Marketplaces*: In the future, AI model marketplaces could evolve to include small language models (SLMs) [119] and agentic AI models [120] alongside the predictive and generative AI models in the catalog of its trading models, creating a more diverse model trading ecosystem. SLMs, with their efficiency and task-specific focus, will be preferred by buyers needing lightweight, resource-friendly solutions. These models will be particularly valuable for AI on-device, real-time applications, and privacy-sensitive use cases [121]. These Marketplaces may offer SLMs as task-specific tools, customizable solutions, or subscription-based libraries, making them accessible to businesses with limited computational resources.
  Agentic AI models, on the other hand, will introduce autonomy and decision-making capabilities to their operating environment. These models may be employed in complex, goal-oriented tasks like supply chain optimization or autonomous customer support [84,122]. Marketplaces may offer agentic AI as a service, where buyers pay for outcomes rather than owning the models. However, their integration will require robust monitoring tools and strict compliance frameworks to address ethical and regulatory concerns, given the risks associated with autonomous decision-making [120]. In order to handle this diversity, model marketplaces may need to adapt by categorizing models based on their type and use case, ensuring interoperability, and providing tools for customization and fine-tuning. Ethical and regulatory compliance will be critical, especially for agentic AI, while performance metrics and transparency will help buyers evaluate and trust the models. Despite these potentials, challenges like scalability, buyer education, and ethical concerns will persist, requiring ongoing innovation monitoring and governance. By addressing these needs, future marketplaces will empower buyers to effectively leverage the full spectrum of AI models or technologies as they evolve daily.

7. Final Remarks

The rise of AI across various industries and its numerous operating domains has unlocked various business opportunities. AI model marketplace has the potential to promote

innovation and enable the collaborations required by today's and tomorrow's digital world. In this article, we have evaluated the existing AI model marketplaces and identified areas requiring improvement. Specifically, we have identified the unique characteristics needed as an ideal AI marketplace and compared the existing marketplaces with the identified characteristics. Furthermore, we have conducted a literature review based on the different phases of the AI model lifecycle. We have utilized a three-dimensional problem space to evaluate the existing pricing schemes and trading platforms. We have outlined key challenges such as unauthorized model modifications, data leakage, intellectual property rights break, and transparency and identified future research directions that require attention.

We consider that addressing the identified challenges can help a robust AI ecosystem that promotes innovation, enables collaboration, and protects AI models across the pervasive industrial domains. AI marketplaces envision solving real-world challenges and supporting interdisciplinary research, making them a hub of the digital market in the near future. As ongoing research, we aim to broaden this area of research by designing a marketplace, i.e., auction mechanisms that balance performance efficiency, privacy, and security threats while trading AI models.

Author Contributions: Conceptualization, M.Q., A.A.M., M.B., and W.Y.; Methodology, M.Q., A.A.M., M.B., and W.Y.; Writing—original draft preparation, M.Q., A.A.M., M.B., and W.Y.; Writing—review and editing, Y.G., W.L., and W.Y.; Problem space and formalization, M.Q., A.A.M., and W.Y.; Supervision, W.L., Y.G. and W.Y.; Project administration, Y.G., W.L., and W.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

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

References

1. Hatcher, W.G.; Yu, W. A Survey of Deep Learning: Platforms, Applications and Emerging Research Trends. *IEEE Access* **2018**, *6*, 24411–24432. [CrossRef]
2. Liang, F.; Hatcher, W.G.; Liao, W.; Gao, W.; Yu, W. Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly. *IEEE Access* **2019**, *7*, 158126–158147. [CrossRef]
3. Equinox. Tapping Into AI Model Marketplaces to Unlock Value: P1. 2024. Available online: https://blog.equinix.com/blog/2024/04/16/tapping-into-ai-model-marketplaces-to-unlock-value-part-1/ (accessed on 23 December 2024).
4. Equinox. Tapping into AI Model Marketplaces to Unlock Value: P2. 2024. Available online: https://blog.equinix.com/blog/2024/05/30/tapping-into-ai-model-marketplaces-to-unlock-value-part-2/#:~:text=AI%20model%20marketplaces%20have%20become,of%20the%20different%20marketplace%20participants (accessed on 23 December 2024).
5. NfX. The AI-First Marketplace. 2024. Available online: https://www.nfx.com/post/ai-first-marketplace (accessed on 23 December 2024).
6. Research, P. Artificial Intelligence (AI) Market Size, Share, and Trends 2024 to 2034. 2024. Available online: https://www.precedenceresearch.com/artificial-intelligence-market (accessed on 8 December 2024).
7. Insights, F.M. AI Platform Market. 2024. Available online: https://www.futuremarketinsights.com/reports/ai-platform-market (accessed on 23 December 2024).
8. MarketsandMarkets. AI as a Service Market. 2024. Available online: https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-ai-as-a-service-market-121842268.html#:~:text=Overview,compliance%20and%20encouraging%20innovative%20solutions (accessed on 23 December 2024).
9. Kumar, A.; Finley, B.; Braud, T.; Tarkoma, S.; Hui, P. Sketching an ai marketplace: Tech, economic, and regulatory aspects. *IEEE Access* **2021**, *9*, 13761–13774. [CrossRef]
10. Dimont, J. Royalty inequity: Why music streaming services should switch to a per-subscriber model. *Hastings LJ* **2017**, *69*, 675.
11. Danny Iland, Andrew Irish, B.S. Rethinking GPS: Engineering Next-Gen Location at Uber. 2024. Available online: https://www.uber.com/blog/rethinking-gps/ (accessed on 8 December 2024).
12. Nguyen, T. How Uber Makes Money | Understand Uber Business Model. 2024. Available online: https://medium.com/business-thinking/how-uber-makes-money-understand-uber-business-model-da45a38c83db (accessed on 8 December 2024).

13. Chen, X.; Li, B.; Chen, W.; Wu, S. Influences of information sharing and online recommendations in a supply chain: Reselling versus agency selling. *Ann. Oper. Res.* **2023**, *329*, 717–756. [CrossRef]
14. Wiener, R.; Stern, R. Safe and Secure Innovation for Frontier Artificial Intelligence Models Act. 2024. Available online: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB1047/ (accessed on 23 December 2024).
15. General, A. California Consumer Privacy Act (CCPA). 2024. Available online: https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20applies%20to%20for,%2C%20households%2C%20or%20devices%3B%20or (accessed on 25 December 2024).
16. Reuel, A.; Connolly, P.; Meimandi, K.J.; Tewari, S.; Wiatrak, J.; Venkatesh, D.; Kochenderfer, M. Responsible AI in the Global Context: Maturity Model and Survey. *arXiv* **2024**, arXiv:2410.09985.
17. Newsletter, B.D. AI Could Be Eating Up All Your Electricity. Available online: https://www.pcbb.com/bid/2024-08-12-ai-could-be-eating-up-all-your-electricity (accessed on 24 December 2024).
18. ClearML. The State of AI Infrastructure at Scale 2024. 2024. Available online: https://ai-infrastructure.org/wp-content/uploads/2024/03/The-State-of-AI-Infrastructure-at-Scale-2024.pdf (accessed on 25 December 2024).
19. Report, T.A.I. Measuring Trends in AI. 2024. Available online: https://aiindex.stanford.edu/report/ (accessed on 25 December 2024).
20. Kumar, A.; Finley, B.; Braud, T.; Tarkoma, S.; Hui, P. Marketplace for AI models. *arXiv* **2020**, arXiv:2003.01593.
21. Waters, A. Common Ethical Issues in Artificial Intelligence. 2024. Available online: https://connect.comptia.org/blog/common-ethical-issues-in-artificial-intelligence (accessed on 25 December 2024).
22. UNESCO. Ethics of Artificial Intelligence. 2024. Available online: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics (accessed on 25 December 2024).
23. Huang, C.; Zhang, Z.; Mao, B.; Yao, X. An overview of artificial intelligence ethics. *IEEE Trans. Artif. Intell.* **2022**, *4*, 799–819. [CrossRef]
24. DAWEX. Making the AI Promise a Reality with AI Marketplaces. 2021. Available online: https://www.dawex.com/en/news/making-ai-promise-reality-with-ai-marketplaces/ (accessed on 27 December 2024).
25. Pei, J. A survey on data pricing: From economics to data science. *IEEE Trans. Knowl. Data Eng.* **2020**, *34*, 4586–4608. [CrossRef]
26. Cong, Z.; Luo, X.; Pei, J.; Zhu, F.; Zhang, Y. Data pricing in machine learning pipelines. *Knowl. Inf. Syst.* **2022**, *64*, 1417–1455. [CrossRef]
27. Hao, J.; Deng, Z.; Li, J. The evolution of data pricing: From economics to computational intelligence. *Heliyon* **2023**, *9*, e20274. [CrossRef]
28. Zhang, M.; Beltrán, F.; Liu, J. A survey of data pricing for data marketplaces. *IEEE Trans. Big Data* **2023**, *9*, 1038–1056. [CrossRef]
29. Miao, X.; Peng, H.; Huang, X.; Chen, L.; Gao, Y.; Yin, J. Modern Data Pricing Models: Taxonomy and Comprehensive Survey. *arXiv* **2023**, arXiv:2306.04945.
30. Zhang, J.; Bi, Y.; Cheng, M.; Liu, J.; Ren, K.; Sun, Q.; Wu, Y.; Cao, Y.; Fernandez, R.C.; Xu, H.; et al. A Survey on Data Markets. *arXiv* **2024**, arXiv:2411.07267.
31. Martin, W.; Sarro, F.; Jia, Y.; Zhang, Y.; Harman, M. A survey of app store analysis for software engineering. *IEEE Trans. Softw. Eng.* **2016**, *43*, 817–847. [CrossRef]
32. Nizamis, A.; Schlake, G.; Siachamis, G.; Dimitriadis, V.; Patsonakis, C.; Beecks, C.; Ioannidis, D.; Votis, K.; Tzovaras, D. Designing a Marketplace to Exchange AI Models for Industry 5.0. In *Artificial Intelligence in Manufacturing: Enabling Intelligent, Flexible and Cost-Effective Production Through AI*; Springer Nature: Cham, Switzerland, 2023; pp. 27–41.
33. Pei, J.; Fernandez, R.C.; Yu, X. Data and ai model markets: Opportunities for data and model sharing, discovery, and integration. *Proc. VLDB Endow.* **2023**, *16*, 3872–3873. [CrossRef]
34. Nikoletos, G.; Papoutsoglou, I.; Spanos, G.; Nizamis, A.; Lalas, A.; Votis, K.; Tzovaras, D. Digital marketplaces in European research landscape: A systematic literature review. *Open Res. Eur.* **2024**, *4*, 223. [CrossRef]
35. Rochet, J.C.; Tirole, J. Platform competition in two-sided markets. *J. Eur. Econ. Assoc.* **2003**, *1*, 990–1029. [CrossRef]
36. Cisneros-Cabrera, S.; Ramzan, A.; Sampaio, P.; Mehandjiev, N. Digital marketplaces for industry 4.0: A survey and gap analysis. In Proceedings of the Collaboration in a Data-Rich World: 18th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2017, Vicenza, Italy, 18–20 September 2017; Proceedings 18; Springer: Berlin/Heidelberg, Germany, 2017; pp. 18–27.
37. O'Reilly, P.; Finnegan, P. Electronic Marketplaces: Focus and operational characteristics. *Scand. J. Inf. Syst.* **2009**, *21*, 2.
38. Dhamange, P.; Soni, S.; Sridhar, V.; Rao, S. Market dynamics and regulation of a crowd-sourced AI marketplace. *IEEE Access* **2022**, *10*, 54325–54335. [CrossRef]
39. Azcoitia, S.A.; Laoutaris, N. Try Before You Buy: A practical data purchasing algorithm for real-world data marketplaces. In Proceedings of the 1st International Workshop on Data Economy, Rome, Italy, 9 December 2022; pp. 27–33.
40. Gleim, M.R.; Stevens, J.L.; Johnson, C.M. Platform marketplaces: Unifying our understanding of lateral exchange markets. *Eur. J. Mark.* **2023**, *57*, 1–28. [CrossRef]
41. Chen, L.; Koutris, P.; Kumar, A. Towards model-based pricing for machine learning in a data marketplace. In Proceedings of the 2019 International Conference on Management of Data, Amsterdam, The Netherlands, 30 June–5 July 2019; pp. 1535–1552.

42. Gao, J.; Wang, Z.; Wei, X. An Adaptive Pricing Framework for Real-Time AI Model Service Exchange. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 5114–5129. [CrossRef]
43. Hagiu, A.; Wright, J. Multi-sided platforms. *Int. J. Ind. Organ.* **2015**, *43*, 162–174. [CrossRef]
44. Parker, G.G. *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*; WW Norton & Company: New York, NY, USA, 2016.
45. Evans, D.S. The antitrust economics of multi-sided platform markets. *Yale J. on Reg.* **2003**, *20*, 325.
46. Rochet, J.C.; Tirole, J.M.P. Platform competition in two-sided markets. *Compet. Policy Int.* **2014**, *10*, 180–218. [CrossRef]
47. Einav, L.; Farronato, C.; Levin, J. Peer-to-peer markets. *Annu. Rev. Econ.* **2016**, *8*, 615–635. [CrossRef]
48. Hasan, T.I.; Silalahi, C.I.; Rumagit, R.Y.; Pratama, G.D. UI/UX Design Impact on E-Commerce Attracting Users. *Procedia Comput. Sci.* **2024**, *245*, 1075–1082. [CrossRef]
49. Spiekermann, S. *Ethical IT Innovation: A Value-Based System Design Approach*; CRC Press: Boca Raton, FL, USA, 2015.
50. Baldwin, C. *Design Rules, Volume 1: The Power of Modularity*; MIT Press: Cambridge, MA, USA, 2000.
51. Bostrom, N.; Yudkowsky, E. The ethics of artificial intelligence. In *Artificial Intelligence Safety and Security*; Chapman and Hall: London, UK; CRC Press: Boca Raton, FL, USA, 2018; pp. 57–69.
52. Safadi, H.; Lalor, J.P.; Berente, N. The Effect of Bots on Human Interaction in Online Communities. *MIS Q.* **2024**, *48*, 1279–1296. [CrossRef]
53. Binns, R. Fairness in machine learning: Lessons from political philosophy. In Proceedings of the Conference on Fairness, Accountability and Transparency, PMLR, New York, NY, USA, 23–24 February 2018; pp. 149–159.
54. Tapscott, D.; Tapscott, A. *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*; Portfolio Penguin: London, UK, 2016.
55. Dellarocas, C. The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Manag. Sci.* **2003**, *49*, 1407–1424. [CrossRef]
56. Rysman, M. The economics of two-sided markets. *J. Econ. Perspect.* **2009**, *23*, 125–143. [CrossRef]
57. Workday. AI Marketplace. 2024. Available online: https://marketplace.workday.com/en-US/pages/ai (accessed on 7 December 2024).
58. Feuerriegel, S.; Hartmann, J.; Janiesch, C.; Zschech, P. Generative ai. *Bus. Inf. Syst. Eng.* **2024**, *66*, 111–126. [CrossRef]
59. Rani, G.; Singh, J.; Khanna, A. Comparative analysis of generative AI models. In Proceedings of the 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), IEEE, Faridabad, India, 23–24 November 2023; pp. 760–765.
60. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and open problems in federated learning. *Found. Trends® Mach. Learn.* **2021**, *14*, 1–210. [CrossRef]
61. Kanbach, D.K.; Heiduk, L.; Blueher, G.; Schreiter, M.; Lahmann, A. The GenAI is out of the bottle: Generative artificial intelligence from a business model innovation perspective. *Rev. Manag. Sci.* **2024**, *18*, 1189–1220. [CrossRef]
62. Han, L.; Iregbulem, N. AI Enterprise Market Map: Cutting Through the Hype. 2024. Available online: https://lsvp.com/stories/ai-enterprise-market-map-cutting-through-the-hype/ (accessed on 8 December 2024).
63. GravityAI. GravityAI Catalog. 2024. Available online: https://www.gravity-ai.com/ (accessed on 25 December 2024).
64. DataStax. DataStax AI Platform. 2024. Available online: https://www.datastax.com/ (accessed on 25 December 2024).
65. Planet, A. AI Marketplace by AI Planet. 2024. Available online: https://aimarketplace.co/ (accessed on 24 December 2024).
66. Akira. Akira AI Marketplace. 2024. Available online: https://www.akira.ai/ (accessed on 8 December 2024).
67. Amazon. Machine Learning Service-Amazon SageMaker. 2017. Available online: https://aws.amazon.com/pm/sagemaker (accessed on 25 December 2024).
68. Google. AI and Machine Learning Products. 2024. Available online: https://cloud.google.com/products (accessed on 25 December 2024).
69. H_2O.ai. H_2O.ai. 2024. Available online: https://H$_2$O.ai/ (accessed on 25 December 2024).
70. Gradio, H.F. The AI Community Building the Future. 2024. Available online: https://huggingface.co/ (accessed on 25 December 2024).
71. Wu, T.; He, S.; Liu, J.; Sun, S.; Liu, K.; Han, Q.L.; Tang, Y. A brief overview of ChatGPT: The history, status quo and potential future development. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 1122–1136. [CrossRef]
72. Pedro, F.; Subosa, M.; Rivas, A.; Valverde, P. *Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development*; Unesco: London, UK, 2019. Available online: https://hdl.handle.net/20.500.12799/6533 (accessed on 25 December 2024).
73. Smith, J.M. AI in Computer Science Education: Tool, Subdomain, and Wildcard. In Proceedings of the 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 20–24 May 2024; pp. 1267–1271. [CrossRef]
74. Southworth, J.; Migliaccio, K.; Glover, J.; Reed, D.; McCarty, C.; Brendemuhl, J.; Thomas, A. Developing a model for AI Across the curriculum: Transforming the higher education landscape via innovation in AI literacy. *Comput. Educ. Artif. Intell.* **2023**, *4*, 100127. [CrossRef]

75. Tech, I. Info Tech AI Marketplace. 2024. Available online: https://www.infotech.com/ai-marketplace (accessed on 25 December 2024).
76. Instructure. Instructure AI Marketplace. 2024. Available online: https://app.learnplatform.com/marketplace/ (accessed on 8 December 2024).
77. AITech, S. Solidus AI Marketplace. 2024. Available online: https://ai.aitech.io/ (accessed on 24 December 2024).
78. Hsieh, C.Y.; Lee, C.Y. Distilling Step-by-Step: Outperforming Larger Language Models with Less Training Data and Smaller Model Sizes. 2023. Available online: https://research.google/blog/distilling-step-by-step-outperforming-larger-language-models-with-less-training-data-and-smaller-model-sizes/ (accessed on 24 December 2024).
79. Yu, Y.; Yu, J.; Wang, X.; Li, J.; Lin, Y.; He, C.; Yang, Y.; Qiao, Y.; Li, L.; Wang, F.Y. Navigating the Data Trading Crossroads: An Interdisciplinary Survey. *arXiv* **2024**, arXiv:2407.11466.
80. Wladawsky-Berger, I. The Impact of Open Source on the Future of AI. 2024. Available online: https://blog.irvingwb.com/blog/2024/12/the-impact-of-open-source-on-the-future-of-ai.html (accessed on 26 December 2024).
81. America, N. Openness in Artificial Intelligence Models. 2024. Available online: https://www.newamerica.org/oti/reports/openness-in-artificial-intelligence-models/benefits-of-open-source-ai/ (accessed on 26 December 2024).
82. Eiras, F.; Petrov, A.; Vidgen, B.; Schroeder, C.; Pizzati, F.; Elkins, K.; Mukhopadhyay, S.; Bibi, A.; Purewal, A.; Botos, C.; et al. Risks and opportunities of open-source generative AI. *arXiv* **2024**, arXiv:2405.08597.
83. Jeon, J. Standardization trends on safety and trustworthiness technology for advanced AI. *arXiv* **2024**, arXiv:2410.22151.
84. Sinha, S.; Lee, Y.M. Challenges with developing and deploying AI models and applications in industrial systems. *Discov. Artif. Intell.* **2024**, *4*, 55. [CrossRef]
85. Radanliev, P.; Santos, O.; Brandon-Jones, A.; Joinson, A. Ethics and responsible AI deployment. *Front. Artif. Intell.* **2024**, *7*, 1377011. [CrossRef]
86. Sarpatwar, K.; Sitaramagiridharganesh Ganapavarapu, V.; Shanmugam, K.; Rahman, A.; Vaculin, R. Blockchain enabled AI marketplace: The price you pay for trust. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Long Beach, CA, USA, 16–17 June 2019.
87. Liu, J. Dealer: End-to-end data marketplace with model-based pricing. *arXiv* **2020**, arXiv:2003.13103.
88. Jiao, Y.; Wang, P.; Niyato, D.; Lin, B.; Kim, D.I. Toward an automated auction framework for wireless federated learning services market. *IEEE Trans. Mob. Comput.* **2020**, *20*, 3034–3048. [CrossRef]
89. Sim, R.H.L.; Zhang, Y.; Chan, M.C.; Low, B.K.H. Collaborative machine learning with incentive-aware model rewards. In Proceedings of the International Conference on Machine Learning, PMLR, Virtual, 13–18 July 2020; pp. 8927–8936.
90. Weng, J.; Weng, J.; Cai, C.; Huang, H.; Wang, C. Golden grain: Building a secure and decentralized model marketplace for MLaaS. *IEEE Trans. Depend. Secur. Comput.* **2021**, *19*, 3149–3167. [CrossRef]
91. Sun, P.; Chen, X.; Liao, G.; Huang, J. A profit-maximizing model marketplace with differentially private federated learning. In Proceedings of the IEEE INFOCOM 2022-IEEE Conference on Computer Communications, IEEE, London, UK, 2–5 May 2022; pp. 1439–1448.
92. Zheng, S.; Cao, Y.; Yoshikawa, M.; Li, H.; Yan, Q. FL-market: Trading private models in federated learning. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), IEEE, Osaka, Japan, 17–20 December 2022; pp. 1525–1534.
93. Han, M.; Light, J.; Xia, S.; Galhotra, S.; Fernandez, R.C.; Xu, H. A Data-Centric Online Market for Machine Learning: From Discovery to Pricing. *arXiv* **2023**, arXiv:2310.17843.
94. Li, Z.; Ding, B.; Yao, L.; Li, Y.; Xiao, X.; Zhou, J. Performance-Based Pricing for Federated Learning via Auction. *Proc. VLDB Endow.* **2024**, *17*, 1269–1282. [CrossRef]
95. Sun, Y.; Li, B.; Yang, K.; Bi, X.; Zhao, X. TiFLCS-MARP: Client selection and model pricing for federated learning in data markets. *Expert Syst. Appl.* **2024**, *245*, 123071. [CrossRef]
96. Cui, Y.; Yao, L.; Li, Y.; Chen, Z.; Ding, B.; Zhou, X. An Auction-based Marketplace for Model Trading in Federated Learning. *arXiv* **2024**, arXiv:2402.01802.
97. Li, K.; Shi, Y. Towards Incentive with Privacy Preserving Machine Learning as a Service for Crowdsensed Data Trading. *IEEE Internet Things J.* **2024**, *11*, 36494–36507. [CrossRef]
98. Liu, J.; Lou, J.; Liu, J.; Xiong, L.; Pei, J.; Sun, J. Dealer: An end-to-end model marketplace with differential privacy. *Proc. VLDB Endow.* **2021**, *14*, 957–969. [CrossRef]
99. Kurtulmus, A.B.; Daniel, K. Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain. *arXiv* **2018**, arXiv:1802.10185.
100. Somy, N.B.; Kannan, K.; Arya, V.; Hans, S.; Singh, A.; Lohia, P.; Mehta, S. Ownership preserving AI market places using blockchain. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, Atlanta, GA, USA, 14–17 July 2019; pp. 156–165.
101. Li, C.; Wang, H.; Zhao, Y.; Xi, Y.; Xu, E.; Wang, S. Enabling High-Quality Machine Learning Model Trading on Blockchain-Based Marketplace. *Mathematics* **2023**, *11*, 2636. [CrossRef]

102. Li, X.; Huang, J.; Yang, K.; Fan, C. Machine Learning Model Trading with Information Asymmetry. In Proceedings of the ICC 2023-IEEE International Conference on Communications, IEEE, Rome, Italy, 28 May–1 June 2023; pp. 3320–3326.
103. Nguyen, L.D.; Pandey, S.R.; Beatriz, S.; Broering, A.; Popovski, P. A marketplace for trading ai models based on blockchain and incentives for iot data. *arXiv* **2021**, arXiv:2112.02870.
104. Mai, T.; Yao, H.; Xu, J.; Zhang, N.; Liu, Q.; Guo, S. Automatic double-auction mechanism for federated learning service market in Internet of Things. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 3123–3135. [CrossRef]
105. Yousafzai, A.; Khan, L.U.; Majeed, U.; Hakeem, O.; Hong, C.S. FedMarket: A Cryptocurrency Driven Marketplace for Mobile Federated Learning Services. *IEEE Access* **2022**, *10*, 87602–87616. [CrossRef]
106. Song, Q.; Cao, J.; Sun, K.; Li, Q.; Xu, K. Try before you buy: Privacy-preserving data evaluation on cloud-based machine learning data marketplace. In Proceedings of the 37th Annual Computer Security Applications Conference, Virtual Event, 6–10 December 2021; pp. 260–272.
107. Nikolakakis, K.E.; Chantzialexiou, G.; Kalogerias, D. FEDSTR: Money-In AI-Out | A Decentralized Marketplace for Federated Learning and LLM Training on the NOSTR Protocol. *arXiv* **2024**, arXiv:2404.15834.
108. Ackerman, S.; Raz, O.; Zalmanovici, M.; Zlotnick, A. Automatically detecting data drift in machine learning classifiers. *arXiv* **2021**, arXiv:2111.05672.
109. Mohanarathinam, A.; Kamalraj, S.; Prasanna Venkatesan, G.; Ravi, R.V.; Manikandababu, C. Digital watermarking techniques for image security: A review. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 3221–3229. [CrossRef]
110. Ressi, D.; Romanello, R.; Piazza, C.; Rossi, S. AI-enhanced blockchain technology: A review of advancements and opportunities. *J. Netw. Comput. Appl.* **2024**, *225*, 103858. [CrossRef]
111. Cai, H.; Zhou, Z.; Huang, Q. Online Resource Allocation for Edge Intelligence with Colocated Model Retraining and Inference. *arXiv* **2024**, arXiv:2405.16029.
112. Spanaki, K.; Karafili, E.; Despoudi, S. AI applications of data sharing in agriculture 4.0: A framework for role-based data access control. *Int. J. Inf. Manag.* **2021**, *59*, 102350. [CrossRef]
113. Tong, W.; Feng, X. Location Privacy Protection and Location Verification Mechanism of Vehicle in VANET. In Proceedings of the 2023 IEEE 6th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), IEEE, Chongqing, China, 24–26 February 2023; Volume 6; pp. 725–731.
114. Arbaoui, M.; Brahmia, M.-E.-A.; Rahmoun, A. Towards secure and reliable aggregation for Federated Learning protocols in healthcare applications. In Proceedings of the 2022 Ninth International Conference on Software Defined Systems (SDS). IEEE, Paris, France, 12–15 December 2022; pp. 1–3.
115. Liu, P.; Xu, X.; Wang, W. Threats, attacks and defenses to federated learning: Issues, taxonomy and perspectives. *Cybersecurity* **2022**, *5*, 4. [CrossRef]
116. Chen, L.; Wang, H.; Chen, L.; Koutris, P.; Kumar, A. Demonstration of nimbus: Model-based pricing for machine learning in a data marketplace. In Proceedings of the 2019 International Conference on Management of Data, Amsterdam, The Netherlands, 30 June–5 July 2019; pp. 1885–1888.
117. Liu, Y.; Peng, J.; Kang, J.; Iliyasu, A.M.; Niyato, D.; Abd El-Latif, A.A. A secure federated learning framework for 5G networks. *IEEE Wirel. Commun.* **2020**, *27*, 24–31. [CrossRef]
118. Gorwa, R.; Veale, M. Moderating model marketplaces: Platform governance puzzles for AI intermediaries. *Law Innov. Technol.* **2024**, *16*, 341–391. [CrossRef]
119. Magister, L.C.; Mallinson, J.; Adamek, J.; Malmi, E.; Severyn, A. Teaching small language models to reason. *arXiv* **2022**, arXiv:2212.08410.
120. Shavit, Y.; Agarwal, S.; Brundage, M.; Adler, S.; O'Keefe, C.; Campbell, R.; Lee, T.; Mishkin, P.; Eloundou, T.; Hickey, A.; et al. Practices for governing agentic AI systems. *Res. Pap. OpenAI Dec.* **2023**.
121. Ianishgoswami. Small Language Models (SLMs): The Future of Efficient AI. 2024. Available online: https://medium.com/@ianishgoswami/small-language-models-slms-the-future-of-efficient-ai-653b033ab7e5#/ (accessed on 26 December 2024).
122. Stryker, C. Agentic AI: 4 Reasons Why It's the Next Big Thing in AI Research. 2024. Available online: https://www.ibm.com/think/insights/agentic-ai/ (accessed on 26 December 2024).