IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 8, 2020, accepted January 4, 2021, date of publication January 11, 2021, date of current version January 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3050929

Sketching an AI Marketplace: Tech, Economic, and Regulatory Aspects

ABHISHEK KUMAR[1], BENJAMIN FINLEY[1], TRISTAN BRAUD[2], (Member, IEEE), SASU TARKOMA[1], (Senior Member, IEEE), AND PAN HUI[1,2], (Fellow, IEEE)

[1]Department of Computer Science, University of Helsinki, 00100 Helsinki, Finland
[2]Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong

Corresponding author: Abhishek Kumar (abhishek.kumar@helsinki.fi)

This work was supported in part by the Academy of Finland Flagship programme: Finnish Centre for Artificial Intelligence (FCAI), projects funded by the Academy of Finland, under Grant 319669, Grant 325570, Grant 335934, and Grant 324576; in part by the Research Grants Council of Hong Kong under Grant 16214817; and in part by the 2020 HPY Research Foundation Grant from Elisa Corporation.

ABSTRACT Artificial intelligence shows promise for solving many practical societal problems in areas such as healthcare and transportation. However, the current mechanisms for AI model diffusion such as Github code repositories, academic project webpages, and commercial AI marketplaces have some limitations; for example, a lack of monetization methods, model traceability, and model auditabilty. In this work, we sketch guidelines for a new AI diffusion method based on a decentralized online marketplace. We consider the technical, economic, and regulatory aspects of such a marketplace including a discussion of solutions for problems in these areas. Finally, we include a comparative analysis of several current AI marketplaces that are already available or in development. We find that most of these marketplaces are centralized commercial marketplaces with relatively few models.

INDEX TERMS AI marketplace, privacy, AI regulation, AI ethics, AI trade.

I. INTRODUCTION

Artificial intelligence (AI) is predicted to have a major societal impact over the coming decades. Specifically, when widely diffused, AI models have the potential to solve many ubiquitous problems in domains ranging from healthcare to transportation. For example, neural network-based models have shown human and super-human level performance in many health-related diagnostic tasks such as breast cancer detection [1].

However, to achieve widespread diffusion of AI models and thus capture these benefits, an efficient diffusion mechanism is required. Unfortunately, many popular diffusion mechanisms such as collections of Github repositories, academic research project pages, and existing commercial AI marketplaces have major limitations [2]. Github repositories and academic research projects generally do not have straightforward monetization methods [3] and installing, configuring, applying, and supporting models from these sources can be cumbersome, as such concerns are usually not paramount to academic researchers [4]. While existing commercial AI marketplaces (refer to Table 2) are often centralized and controlled by a single company that may have different motives from the majority of the marketplace users thus allowing for conflict and a single point of failure. Additionally, the models available on commercial AI marketplaces may lag behind the state-of-the-art models available on Github or project pages [2]. Finally, the datasets for training such AI models often cannot be provided for privacy or other reasons, thus the traceability of models from these sources is lacking. Traits such as these will be important given new AI regulations currently in development by, for example, the European Union (discussed in the section on regulation).

Given the limitations of existing mechanisms, in this paper, we aim to sketch guidelines for a new AI diffusion mechanism based on a decentralized online marketplace and hereafter known as **AI marketplace**. We consider the technical, economic, and regulatory aspects of creating such a marketplace in order to reach the goal of broad yet ethical AI diffusion (as shown in Figure 1). The AI marketplace we propose would bring together various actors, including AI developers, AI customers, AI auditors, data owners (individual entities or companies of different sizes), and even governmental entities, towards this common goal.

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

TABLE 1. Key roles in AI marketplace.

Role	Description
Developer	An entity which sells pre-trained AI models, or develops customized AI model
Customer	An entity which purchases AI models, or uses services of Developer to develop customized AI model
Data Owner	An entity which sells their data, or training updates for training AI model
Auditor	An entity which verifies the correctness of AI model developed by the Developer
Regulator	An entity which ensures marketplace guidelines/regulations are being respected

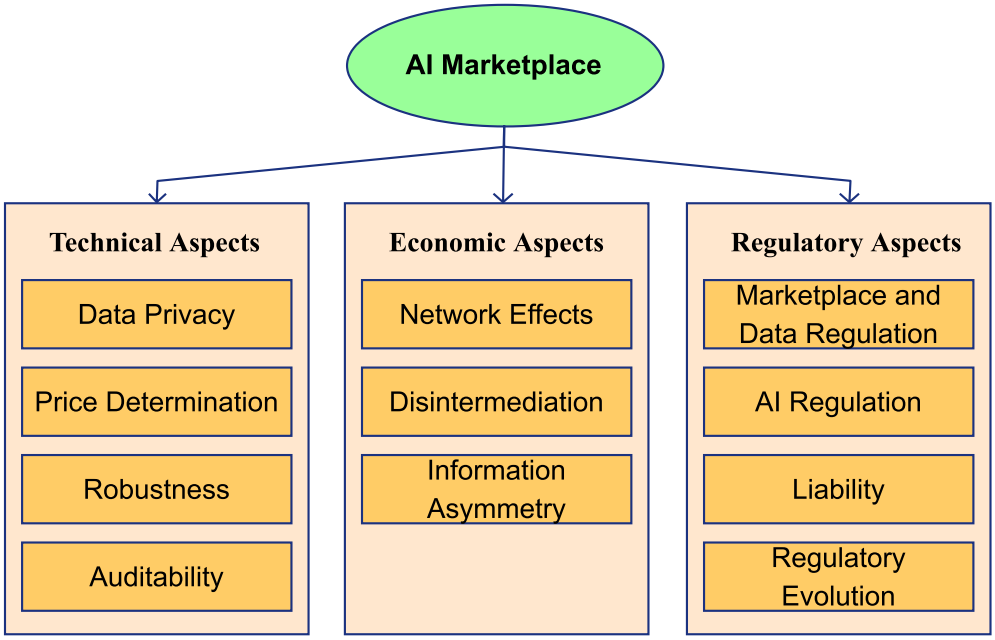


FIGURE 1. Aspects of AI marketplace.

II. WHAT IS THE AI MARKETPLACE?

The AI marketplace is an online marketplace that facilitates the buying and selling of AI models among different actors, such as AI developers (e.g., software engineers from toptal.com), AI customers (e.g., small companies that do not have AI development capabilities or larger companies that want to subcontract). We expect 4 major roles in AI Marketplace, as listed in Table 1. In our vision, the AI marketplace should facilitate several high-level operations: 1) an AI developer should be able to sell their existing pre-trained AI models in the marketplace, 2) an AI customer should be able to request a custom AI model that suits their specific needs, and the marketplace should be able to match the customer with developers who can build such a model. 3) the marketplace should facilitate data sharing (selling and buying) between data owners and AI developers when necessary, e.g., when the AI customer can themselves not provide enough training data to the developer, 4) the marketplace should allow independent expert assessment of AI models by AI auditors for the benefit of AI customers and potentially government regulators, and 5) the marketplace should respect guidelines, or regulation, such as antitrust law (details in Section VI). The flows of these operators are illustrated in Figure 2. Additionally, the marketplace should be flexible in terms of imposing constraints, such as each entity can have at most one primary role, and multiple secondary roles in order to avoid conflict of interests, such as developer should not also act as auditor for the given transaction (more details in Section IV-E).

In a high-level sense, an AI marketplace is similar to other online marketplaces like eBay in terms of business operations and dynamics, i.e, two-sided network effects [5]. However, at the same time, such a marketplace differs from those markets because of the nature of the products in question, i.e., AI Models. Specifically, an AI marketplace is different from a conventional online marketplace in the following ways:

- Developing AI models often requires the sharing of data from the customer side, and such data may be proprietary and or sensitive. Therefore, an AI marketplace may have a mechanism that ensures that developers use that data only for training purposes.

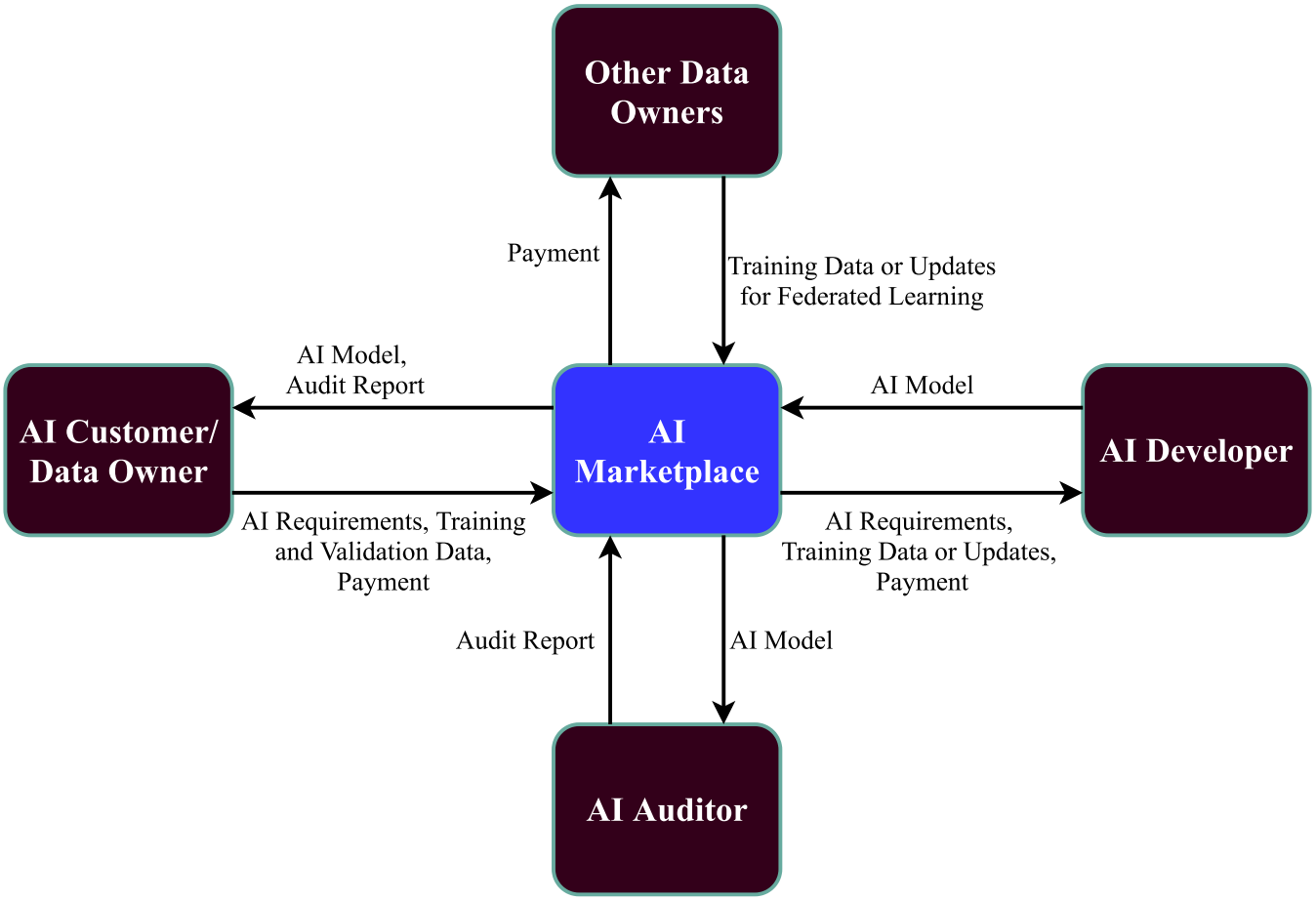


FIGURE 2. Flow diagram of AI marketplace.

- An AI marketplace needs a mechanism that can determine the quality of a final delivered AI model. Conventionally, accuracy has been the primary metric. However, alternative metrics that capture reliability, robustness, and fairness are also now considered important.
- Like in any conventional software system, AI systems also require maintenance over time for various reasons, e.g. to make AI systems compatible with new privacy regulations [6]. In the standard software industry, the company which originally developed the software is usually responsible for providing support. However, in an AI marketplace, specific AI developers may not be available in the future. So, an AI marketplace needs standard guidelines that AI developers should follow while developing models for marketplace customers. Thus maintenance by other AI developers is much easier.

An AI marketplace could also be considered similar to a mobile app store like Google Playstore and Apple App Store. These stores host many AI-enabled applications, however, they still differ from an AI marketplace in some significant ways:

- Unlike in an app store, an AI marketplace would allow customers to request new products on the fly. An AI marketplace can then quickly match AI customers with AI developers with relevant expertise.
- Some AI models are proprietary. So, unlike in an app store, they can not be shared online with a wider audience, as this would further facilitate adversarial attacks and risk leaking intellectual property.

Finally, an AI marketplace is also similar to an online data marketplace. For example, in both marketplaces, the products sold could leak private data. Specifically, attacks against AI models like model inversion [7], [8] and membership inference [9], [10] can extract information about entities whose data was used in training. However, data marketplaces can still be considered closer to conventional online marketplaces, rather than AI marketplaces, since the transferring of data can be considered analogous to the transferring of physical products (assuming that privacy regulations have been followed) as after the transfer (or successful trade) little maintenance is needed, unlike for AI models.

III. DRIVING FORCES BEHIND AI MARKETPLACE

An AI Marketplace aims to respond to several issues within the current AI community. Specifically, in order for AI to diffuse and achieve widespread adoption, it is necessary to address the following concerns:

A. LACK OF INTEROPERABILITY STANDARDS

Currently, there are multiple frameworks for developing diverse AI models. Different developers use different frameworks (TensorFlow, PyTorch, Caffe2), different languages (Python, Java, C/C++), and target different environments (powerful Linux server, smartphone, minimalist IoT device) depending on the intended usage. Each of these elements comes with challenges. A small AI company may want to pipeline a server-based PyTorch AI model with an externally developed smartphone-based TensorFlow AI model. However, the current lack of interoperability standards dramatically limits such opportunities, and adapting existing models is a tedious task (potentially including redeveloping an application-specific AI model) [11], [12].

B. LACK OF INFRASTRUCTURE FOR AI DATA COOPERATION

Many state-of-the-art AI models, especially those based on deep learning, require very large datasets. Unfortunately, the creation, management, and sharing of very large datasets are often difficult for many AI developers and AI customers (due to resource or capability limitations). As a result, AI development with large data is dominated by researchers in large organizations that have significant capabilities and resources [13].

C. RISE OF DATA PROTECTION REGULATIONS

Collecting user's data is increasingly difficult due to privacy regulations around the world, such as the European General Data Protection Regulation (GDPR) or the California Consumer Privacy Act. These regulations put the burden of protecting the user's privacy on the shoulders of data collectors. Users may give consent to collect their personal data at a given point in time, but they can also withdraw their consent later. The data collector is then often required to erase the collected data. Furthermore, fulfilling these requests requires both technical expertise and regulatory expertise. Most AI developers do not possess both of these skills [14].

D. LARGE COST OF AI DEVELOPMENT AND OPERATION

According to a survey of 260 large global organizations, the lack of IT infrastructure (noted by 40% of respondents) and the lack of AI talent (noted by the 34% of respondents) are the two most significant barriers to AI realization [15]. The current lack of qualified AI professionals makes it expensive to hire an AI team. A fully-fledged AI team not only consists of AI developers, but also domain experts, data engineers, product designers, AI sociologists, and IT lawyers. Most small businesses can not afford to hire such an expensive team [16]. Additionally, as mentioned, the infrastructure to collect and store the massive amounts of data required for model development, training, and operation is also costly.

An AI marketplace is a potential solution for overcoming many of these barriers. An AI marketplace can make AI models and datasets accessible to customers and developers, and give developers a way to monetize their models.

IV. TECHNICAL ASPECTS OF AI MARKETPLACE

In a basic AI marketplace setting, an AI customer may arrive with a training dataset, and another smaller dataset referred to as a ''validation'' dataset, and want to build a prediction model that performs well on this validation dataset. The AI marketplace can match the customer with AI developers with the skills needed to build a model. If the model developed by the AI developer based on the training dataset (provided by the customer) shows high accuracy (or other metric(s)), with thresholds set by the customer, on the validation dataset, then customer and developer can move forward with the transaction.

However, the potential AI model (e.g., a deep neural network like ResNet or Inception [17]) may require a large amount of training data which the customer may not have. Furthermore, the original training dataset provided by the customer may itself be from multiple private sources (e.g., mobile crowdsensing) and may follow some multimodal distribution. The AI marketplace should also be able to help the customer by allowing the aggregation of multiple alternative datasets from other data owners in the marketplace while also ensuring the aggregate dataset follows a similar distribution (e.g., using a transfer learning approach [18]) as the validation dataset. This is important since AI learning algorithms suffer from major model quality loss (or even divergence) when trained on non-IID data [19]. In the process, the marketplace should also enable the monetization of data in a trusted, fair manner while preserving data ownership and privacy as much as possible [20].

Let us consider the following scenario in the healthcare domain. The consumer is a newly established cancer treatment hospital, and the data sources are already established cancer treatment hospitals from different geographical locations across the globe.[1] The goal of the new hospital is to construct an ML model that can predict the early onset of a given form of cancer. The model must perform well given the demography of its patients, and therefore it is crucial to collect data similar to the small validation set that is representative of the demography. However, individual data sources have widely different demographics data due to their locations. The goal of an AI Marketplace in such a setting is to enable the collection of a dataset sampled from these sources that match the demography of the new hospital and

[1]Recently, the European Commission adopted a recommendation on a European electronic health record exchange format. The recommendation supports the digital transformation of health and the flow of health data between hospitals within the EU [21].

in the process, to give fair compensation to the different data sources. In other settings, the data owner or consumer may not have sufficient AI expertise or skills. The marketplace should be able to connect the consumer to AI experts (or developers), and at the same time, should provide a platform for AI experts to assess the performance of their models on the consumer's validation dataset without direct access to the dataset (by the AI experts). Importantly, the first version of any AI model may not achieve the target accuracy on the validation dataset. Therefore the developer should be able to assess the performance of model revisions on the validation dataset up to a relatively small fixed number of tests. The total number of validation tests should be small and fixed to avoid developers fitting to the validation dataset rather than actually improving model generalizability.

A model/data exchange mechanism in an AI marketplace should have the following properties:

- All individual data owners should be allowed to modify their data by adding differential privacy noise (a state-of-the-art method used in data publishing to avoid leaking overly sensitive information [22]) in order to maintain their data privacy. Additionally, all data transferred (from the various data owners to the AI developer) should ideally be entirely anonymized, deidentified, and encrypted.
- Transfer learning should be facilitated in the sense that the aggregating entity acquires a summary training dataset that is statistically related to the consumer validation dataset with respect to the requested metrics.
- The AI developer can only learn the pairwise Euclidean distances between the points in the training dataset.
- Consumers having sufficient AI skills, but no or little training data should be able to leverage federated learning on the marketplace to facilitate learning without transferring the actual training data from the owners. However, to facilitate quick convergence, the marketplace should locate data that are nearly identical and independently distributed.
- All entities, i.e., AI developers or data owners, should be fairly compensated for their contribution. Unlike normal goods in online marketplaces like eBay, deciding the fair compensation (or data/model price) is non-trivial in an AI marketplace.
- No collaborating entities such as the data owner (that may also perform model training for federated learning), should be able to cheat in the model building process. In other words, the marketplace should provide robustness against entities who commit malicious or low-quality contributions. Thus the marketplace should incorporate a verification mechanism that will assess the quality of the contribution, and hence will determine compensation accordingly.

In addition to the properties mentioned above, the AI marketplace should also incorporate other relevant properties from conventional marketplaces, e.g., ensuring liquidity in the market [23], providing a framework for conflict resolution between consumer and seller [24]. In the remainder of this section, we discuss potential solutions to address these properties.

A. MAINTAINING DATA PRIVACY IN AI MARKETPLACE

In an AI marketplace context, several major strategies can ensure data privacy for the involved actors.

Federated learning/Peer-to-Peer (P2P) learning as learning paradigms: Under the federated learning framework [25], [26] or the P2P learning framework [27], [28], raw data never leaves the data owners' devices, and thus data privacy is better protected. However, such paradigms add computational overload in the form of local training on the data owner's devices. Additionally, current federated learning frameworks primarily support neural network-based models but federated versions of other ML models (with performance comparable to non-federated versions) are also becoming available, for example, federated random forest [29] and federated SMV [30]. Thus allowing the use of a broad range of ML models.

Using contextual integrity as a design principle for data sharing: The idea of privacy trading is also gaining popularity [31], [32]. Many users who are less privacy-sensitive may be willing to sell their privacy. However, even such users should know the future use of their raw data before selling it. The principle of contextual integrity allows enforcing data privacy by providing a framework for evaluating the flow of personal information between different recipients and explaining why certain patterns of information flow are acceptable in one context but problematic in another [33], [34]. The contextual integrity framework allows users to maintain control of their data even after trading it.

Zero Knowledge as a design principle: According to GDPR, data must not be stored longer than is necessary. The requirement can be met through auto-deletion, i.e., by assigning an expiration date to data gathered from data owners. An AI marketplace can help execute this principle when it manages training data from data owners by making such expiration dates mandatory.

B. MANAGING TRAINING DATASET

Highly performant AI models tend to require a lot of training data. For example, modern deep learning models often have millions of parameters, such as 23 million parameters for ResNet-50 and 5 million parameters for Inception, and require a massive number of samples to train to the state of the art levels [35]. This requirement begets an important question: how can individual developers in the AI marketplace (with limited access to data) compete with giants in this space (e.g., Google) to provide high performance and robust AI solutions? There are several relevant responses.

Firstly, the AI marketplace and large AI development companies have somewhat orthogonal value propositions. Specifically, companies like Google do not provide highly customized services, rather they leverage their massive datasets to provide ready-made standard APIs (like the google

translate API) or they provide cloud ML platforms for customers to build their own models. However, these cloud ML platforms assume a level of data science knowledge that the customer may not have. So, the AI marketplace and these giants can co-exist, since they are not directly competing against each other.

Secondly, the AI marketplace can provide a mechanism, as in Figure 2, which can retrieve either training data or training updates (i.e., Federated Learning) from other data owners on the platform who are willing to contribute (by selling or through the exchange). Towards this goal, recent research on mechanism design theory, for example, has proposed novel valuation mechanisms for selling private data through a real-time auction in marketplaces [36], [37]. Furthermore, the requirement for massive training data can also be reduced through transfer learning. Transfer learning techniques, such as model distillation, allow AI models trained on a dataset from a different yet related domain to be used in training an AI model in the original domain. Specifically, the related pre-trained models can act as starting points for training, thus reducing the amount of training data required.

C. PRICE DETERMINATION IN AI MARKETPLACE

Ensuring that the marketplace is transparent in assigning value based on the quality of the data or model relative to the target is extremely important. Unlike in conventional online marketplaces, deciding the right price of data or an AI model is non-trivial. In conventional online marketplaces, the price in the offline market can serve as a reference. Also, in a corporate setting, experts can estimate the resources required for a project and hence negotiate the price of AI models with potential buyers. However, in an online AI marketplace, an individual AI developer may not possess the skills to determine the right price for their model.

To ensure fairness when deriving the price, the marketplace should provide a bidding mechanism [38]. This bidding mechanism should ideally 1) be a dominant strategy and incentives-compatible. The dominant strategy of each entity is to bid the amount equal to their private valuation. Bidding this true valuation always leads to a non-zero utility for any entities, 2) maximize the social surplus when all entities report their valuations truthfully, and 3) be implementable in polynomial (preferably linear) time in order to enable scalability. Any mechanism satisfying these three conditions can be said to have employed Vickrey auction [39].

Another approach could be to organize contests among AI developers for some pre-defined reward. However, contests and their corresponding reward incentives should be designed based on accurate models of AI developers' strategic behavior to elicit the desired outcomes [40]. Depending on the strategic behavior of the AI developers, different kinds of contests can be organized, e.g., contests that reward a fixed number of AI developers, contests that take the form of a tournament, or contests that award everything to the winner [41], [42].

D. ROBUSTNESS AGAINST MALICIOUS ENTITIES IN AI MARKETPLACE

A Federated learning or P2P learning framework enhances data privacy. However, such a framework also introduces a number of vulnerabilities. Some entities may want to free-ride by trying to capture benefits (or payments) without making honest contributions, e.g., sending random training updates to the server instead of updates calculated on real data after local training [43]. In other scenarios, other competitors/adversaries may try to introduce model poisoning in order to harm said, competitors. An AI marketplace should have a verification mechanism to assess whether the given data or training updates are coming from free-riders [44], malicious entities [45], or honest users. Unfortunately, as research into such mechanisms is underdeveloped, no defense model exists which can prevent such kinds of adversarial attacks [45] on AI models with very high probability. Therefore, during the development phase, the AI marketplace could instead discourage potential malicious behavior from entities involved, e.g., data owner and AI developer, through legal agreements.

Similarly, AI models hosted in the AI marketplace are also subject to model extracting attacks, i.e. malicious users may be able to extract the model without sacrificing significant prediction accuracy which can lead to the loss of valuable intellectual property [46]. This problem can be mitigated by utilizing recent advances in watermarking techniques during the developmental phase [47]. AI marketplace can provide the option of watermarking techniques in its interoperability framework which the developers would be using, or recommend developers to utilize such techniques before uploading their models in the marketplace.

E. AUDITABILITY IN AI MARKETPLACE

The entire operations of an AI marketplace, i.e., matching of AI customers with AI developers, data acquisition from other data owners, auditing of AI models, and payment to/from each actor for their services should be transparent and immutable in order to ensure trust and fairness. On a general trust level, there exist two types of marketplaces: 1) centralized marketplaces, where a trusted entity ensures smooth operations and maintains an immutable log of all operations on the platform, and 2) decentralized marketplaces, with no single trusted entity. Instead, all operations are stored on an immutable public distributed ledger (or a public Blockchain). Both marketplace types have pros and cons. In a centralized marketplace, since the central managing entity typically earns revenue by charging a small transaction fee for each successful transaction, the entity is motivated to maintain smooth operations on the marketplace by verifying the identity of all parties, improving matching mechanisms, supporting buyer-seller conflict resolution, and ensuring liquidity in the market. In a decentralized AI marketplace, many of these goals can be achieved with help of smart contracts. For example, the marketplace can utilize a smart

TABLE 2. Existing AI marketplace frameworks and implementations.

AI Marketplace	Domain	Org[h]	Arch.[j]	Target Market	Domicile	Status
Nuance Comm.	Diagnostic Img.	P	C	USA & Canada	USA	Online
Agorai	Various[a]	P	C	Global	Singapore	Online
IBM Imaging	Healthcare	P	C	USA	USA	Online
Envoy AI	Medical Img.	P	C	USA	USA	Online
GraphGrail AI	Various[b]	P	C	Russia	Russian	Online
Algorithmia	General	P	C	USA	USA	Online
Neuromation	Various[d]	P	C	Global	USA	Online
Ocean Protocol	General	P	D	Global	Singapore	Online
OVHcloud AI	General	P	C	Global	France	Beta
Orange AI	General	P	C	Global	France	Beta
Kynisys	Various[c]	P	C	Global	UK	Beta
Gravity AI	General	P	C	Global	USA	Beta
SingularityNET	General	N	D	Global	Netherlands	Beta
Modzy	General	P	C	USA	USA	Alpha
Alphacat	Fintech	P	C	Global	-	Alpha
Bonseyes	General	P	C	Europe	Switzerland	Dev[i]
Akira AI	General	P	C	Global	India	Dev
Genesis AI	General	P	C	Global	USA	Dev
AI Global	General	N	C	Global	USA	Dev
Synapse AI	General	P	D	Global	USA	Dev
TensorTask	General	N	D	Global	USA	Dev
Nomidman	General	P	D	Global	Estonia	Dev
OSA Decentralized	Various[e]	P	D	Global	BVI[g]	Dev
DaiMoN	General	N	D	-	-	PoC[f]

[a] Finance, Healthcare, Retail, & Advertising
[b] Finance, Travel, Retail, Advertising, & Consumer Goods
[c] Security & IoT, Oil & Gas, Robotics, & Automobile
[d] Surveillance, Retail, Medical Imaging, Industrial Robotics, & Manufacturing
[e] Retail, Manufacturing, & Consumer Goods
[f] Proof of Concept (PoC), Academic Work
[g] British Virgin Islands (BVI)
[h] Organization Type: Profit (P) or Non-Profit (N)
[i] In Development (Dev)
[j] Market Architecture: Centralized (C) or Decentralized (D)

contract to enforce policies market-wide, i.e., every new transaction must follow the policies in this smart contract.

The management of these smart contracts, e.g., making changes to comply with new government regulations, could be achieved in several ways. An independent NGO could have the management power, similar to several existing or proposed decentralized AI marketplaces from Table 2, or consensus (e.g., voting) mechanisms involving marketplace peers could also play a role. Even governments could have a formalized role in such management since they will undoubtedly have a role through AI and marketplace regulation in any case.

Audibility may also be required before finalization for individual transactions to ensure that the AI model is performing as expected and without vulnerabilities or systematic biases. For auditing individual transactions, the AI marketplace should be able to recommend third-party AI auditors (in Figure 2) with expertise in creating similar models. The role and regulations surrounding such auditors could resemble those for financial auditors in the USA, as defined by the Sarbanes-Oxley Act (which provides rules on auditing for public companies [48]). An example regulation from Sarbanes-Oxley is that auditors cannot also be paid consultants for the audited companies, thus helping avoid conflicts of interest. The payment and selection of such certified auditors could be a point of negotiation.

Additionally, for both auditability and regulatory reasons, some AI marketplace models should contain model explainability techniques so that auditors, customers, and regulators can see the decision making processes of the models. For example, input attribution techniques allow the decision to be explained as a function of the input data [49]–[51]. In the case of AI image models, for instance, the model can highlight which parts of the input image were influential in the decision.

F. DOMAIN KNOWLEDGE-BASED MATCHING AND TRANSFER

Many customer companies work in areas, such as healthcare or finance, where specific domain knowledge is very important in creating robust and performant AI models. Therefore, the AI marketplace matching mechanism should also consider the domain knowledge need of customers and the domain knowledge of AI developers. This can be accomplished by having AI developers specify a few areas where they have significant domain knowledge and customers also specifying their domain knowledge needs. Although the self-selection of domain areas means that customers may be suspicious of domain knowledge claims of AI developers, limiting the self-selection to only a few fixed-number of pre-defined areas without the option to frequently change

should provide more confidence (according to warranting theory [52]).

Additionally, the collaboration between the customer and developer (wherein important domain knowledge is transferred) can be guided by a standard or domain-specific smart contract (and non-disclosure agreement) signed through the marketplace. This provides more confidence for customers in sharing proprietary or sensitive domain knowledge with developers.

V. ECONOMIC ASPECTS OF AI MARKETPLACE

Online marketplaces represent an interesting business model in that they facilitate transactions between suppliers and customers often without taking ownership or physical possession of products or services; thus they have very low-cost structures and very high gross margins (e.g., 70% for eBay, 60% for Etsy). Additionally, network effects make them highly defensible. For example, Alibaba, Craigslist, eBay, and Rakuten are more than 15 years old but still dominate their sectors. In the past ten years, the number of online marketplaces worth more than $1 billion has gone from two (Craigslist and eBay) to more than a dozen in the United States (Airbnb, Etsy, Groupon, GrubHub Seamless, Lending Club, Lyft, Prosper, Thumbtack, Uber, and Upwork). This number is expected to double by the end of 2020 [53].

In order to build a successful AI marketplace, a critical number of customers and suppliers of AI models are needed, just like in any other online marketplace. As previously mentioned, potential suppliers for such a marketplace could be individual AI developers or small companies, whereas potential customers could be companies that can not afford their own team of AI experts.

A. (ECONOMIC) NETWORK EFFECTS

A network effect is a phenomenon whereby the value of a platform or service (to an individual participant) is proportional to the number of participants. This phenomenon is often the single-most-important factor behind the success or failure of any online platform. Platforms like eBay and Facebook continue to dominate their respective markets partly because they exploit these network effects very well, whereas platforms like Google Plus did not take off partly due to being on the wrong end of such network effects [54], [55]. Network effects can thus be a crucial element for the success or failure of an AI marketplace.

Additionally, the current AI ecosystem favors major players like Google and Facebook as they also exploit so-called data network effects very well [5]. Specifically, AI-based products or services from these companies become more performant as they train on more data from more users [56], [57]. In turn, more performant products and services attract more new users, thus creating a feedback loop.

With the adoption of two-tier model training architecture like federated learning [26] (with the first tier being a general global model and the second tier being a personalized local model), challenging the dominance of these companies will be even more difficult. Specifically, this architecture allows these large companies to provide personalized model training to AI customers. The companies provide a pre-trained general model (trained on datasets either owned by the company or procured by the company), and the AI customer personalizes the model by training on their local dataset. This training paradigm works well even with smaller amounts of customer training data.

So, if an AI marketplace wishes to challenge the dominance of these companies, the marketplace needs to support interoperability between datasets and models so that developers can efficiently aggregate enough smaller training datasets, federated training users, or even models (into an ensemble) to compete or at least reach a minimum performance threshold.

B. DISINTERMEDIATION

Conventional online marketplaces fear that once they facilitate a successful transaction, the buyer and the seller will agree to conduct their subsequent interactions outside the marketplace [58], a tactic known as disintermediation. However, such a risk could be minimized for an AI marketplace. Specifically, the AI marketplace could offer customers additional added-value services such the AI auditing and traceability services. Additionally, given the assumption of small size but large numbers of AI customers and developers, even a moderate amount of disintermediation might not majorly impact the AI marketplace.

C. INFORMATION ASYMMETRY

In terms of matching AI customers with AI developers, an AI marketplace is an online freelance marketplace that matches buyers of electronically deliverable services with freelancers. Just like in any freelancing marketplace, AI customers may also face the issue of ''information asymmetry'', i.e., they may face uncertainty over the quality of individual AI developers. A solution to this dilemma is a trust or reputation mechanism to help facilitate transactions between strangers [59], [60]. Unlike in a conventional online marketplace where transactions mostly involve products/services and monetary payments, transactions in an AI marketplace may also involve training datasets, which may themselves have economic value; therefore mechanisms of an AI marketplace should ensure an even greater degree of trust. Luca *et al.* [61] found that in an online freelance marketplace, customers are forward-looking and that they place significant weight on a seller's reputation. Though, not controlling for buyers' inter-temporal trade-offs and dynamic selection can considerably bias such reputations. Thus, an AI marketplace should not rely entirely on a reputation mechanism built on reviews from buyers and sellers to tackle the issue of information asymmetry [62]. Instead, the marketplace should play an active role in ensuring fairness in these reputation mechanisms. A potential solution could be to base the reputation mechanism partly on the aforementioned

independent AI auditing mechanism that would be a part of many transactions.

VI. REGULATORY ASPECTS OF AI MARKETPLACE

The regulation of AI marketplaces, as well as the regulation of AI in general, is still a significant unknown with major countries only beginning to grapple with the difficult task. The regulation of any AI marketplace as such would combine the regulatory frameworks from several different domains: regulation of the often sensitive training/testing data, regulation of the application of the AI model (often in sensitive domains), and regulation of online marketplaces.

A. MARKET AND DATA REGULATION

The regulation of online marketplaces and sensitive data have historical precedents (e.g., Sherman Act and Health Insurance Portability and Accountability Act (HIPAA) in the USA) due to the analogues of offline marketplaces and physical data. These regulations are thus being overhauled (e.g., GDPR in Europe) to better deal with the issues brought by the internet and AI eras. Therefore, an AI marketplace must comply with these new regulations. As discussed, the fundamental architecture of an AI marketplace can help ensure compliance through data privacy mechanisms such as differential privacy and federated learning and prevention of marketplace monopoly through open interoperability standards (no lock-in and low switching costs). Unfortunately, even current regulations like GDPR are vague in many cases, thus creating uncertainty and cautiousness in companies that may deter participation in an AI market. These uncertainties are compounded by the differing approaches to such regulations in varying markets [63]. We discuss this topic further in the Section on regulatory aspects of the AI marketplace.

B. AI REGULATION

In terms of AI itself, the regulation is currently very sparse but developing. For example, the EU recently released a draft paper outlining its vision for AI regulation in high-risk areas (e.g., transportation or health care) [64], [65], as well as ethical guidelines for building trustworthy AI systems [66], [67]. The draft includes an overarching framework that would cover the training data (including data traceability and coverage to ensure fairness), model explainability (to understand why certain decisions are taken), and liability (in case of harm).

Similar to the data-centric regulations, an AI marketplace can ensure that at least some subset of the marketplace (e.g., a high-risk area section) enforces or checks that the AI follows these regulations. For example, data traceability can be ensured (at least up to the point of individual marketplace actors) through the use of the public ledger to track the actors providing the data [68]. Similarly, adequate training data coverage (to prevent discrimination or bias by AI [69]) can be ensured through the use of diverse third party (e.g., even government or conformity bodies) validation datasets enforced in a smart contract.[2] The EU already discusses in the draft paper the potential for ''support structures'' and ''online tools [that] could facilitate compliance'' to help especially small and medium-size businesses [64]. The marketplace could also periodically re-verify compliance as models evolve as such regulations apply both ex-ante and ex-post.

Finally, novel unlearning AI mechanisms could help in removing users' data already embedded within a trained AI model without completely retaining the model (which can be costly) [70]–[72]. Such mechanisms would help with GDPR compliance when users withdraw their consent to use their data. Such withdrawal requests could be formally tracked (as transactions) through the AI marketplace, however, the actual unlearning would be the responsibility of the AI developer or maintainer, though possibly validated by the aforementioned AI auditors. Similarly, data privacy in the visual domain could be ensured by incorporating novel privacy-respecting mechanism in vision-based applications [73].

Interestingly, in the US, for example, the healthcare domain does have some regulations for AI/ML models partly derived from existing regulations on healthcare software. In fact, many of the models available on existing commercial AI marketplaces are healthcare based (refer to Table 2). As an example of a current regulatory problem, the US regulator is discussing how to regulate AI/ML models that frequently or continuously learn without requiring a regulatory review after every model update (which could be the case under current regulations) [74]. Again, such future regulations could potentially leverage automated testing on independent government or conformity body validation datasets through the AI marketplace.

Additionally, the misuse of models or data could be deterred by existing and novel punitive measures such as fines and, in some cases, the criminal liability that already applies in the case of, for example, GDPR. In GDPR the fines scale with the revenue of the company as max(20M, 4% worldwide turnover), thus ensuring even large companies notice the deterrent. We discuss civil liability further in Section on regulatory aspects of AI marketplace.

Even unconventional organizations are delving into the area, with the Vatican organizing a workshop denoted as ''The 'Good' Algorithm? Artificial Intelligence: Ethics, Law, Health'' [75]. Additionally, AI regulation and governance have been the subject of recent interdisciplinary academic research by computer scientists, lawyers, and others [76], [77].

C. LIABILITY REGULATION

Liability in the case of such an AI marketplace is also a difficult problem stemming from the difficulty of liability in both AI and online marketplace platforms contexts. Hereafter,

[2]Though, even validation datasets might not be enough to prevent bias and additional measures like the aforementioned AI auditing (e.g., with teams that include sociologists, ethicists, statisticians, etc.) will be necessary in some cases. These audits could even take inspiration from the double-blind review processes of academic conferences and journals.

given the context, we focus on civil liability as opposed to criminal liability.

Firstly, civil liability, in general, must balance the need to incentivize product safety and compensate victims of harm with the need to encourage business innovation. This balance is especially difficult given the rapid innovation in AI and the potential economic and societal benefits of AI. Additionally, in many legal systems, such as the EU, for compensation, the victim must prove damage, a product defect, and a causal link between the two [78]. With complex AI or software-based systems, identifying the liable person can be burdensome, or in cases, with human-AI collaborative systems, the liable person may be unclear. A possible solution is to alter the burden of proof requirement, for example, by inverting the burden to rest with the producing company. This inversion requires companies to have very clear and coherent tracking and documenting of AI models which the AI marketplace inherently enables.

In terms of online marketplaces, the liability of companies such as Amazon for products from third-party sellers on their platform (about 58% of Amazon sales) is a matter of ongoing legal debate [79], [80]. For example, in the US, the issue of liability currently revolves around whether Amazon is considered in a legal sense ''a seller'' or simply ''a platform for sellers and buyers''. This, in turn, is primarily related to how much power they have over the third party sellers (along with several other considerations). Court cases (e.g., Oberdorf v. Amazon) are currently in progress, and a case may eventually reach the US supreme court. Currently, the status quo in the US is that amazon is not liable. The situation in Europe is similar, with on-going work on developing new regulations and eventually adapting the EU Product Liability Directive [80]. Given this background, under current trends, if the AI marketplace does not exert strict control and gain excessive power over sellers, then liability could be minimized by maintaining the status of a platform.

D. REGULATORY EVOLUTION

Overall, any AI marketplace would need to evolve along with novel regulation (e.g., safety or export regulations) or risk becoming unusable by legitimate users. Specifically, several distinct marketplaces or strict marketplace access controls may be necessary given new export regulations. For example, new US regulations require companies to have a special license to export certain geospatial AI software [81]. The justification for the new regulations is based on national security (with especially China in mind [82]). Additionally, a marketplace may need to follow the strictest common safety regulations given the potential for safety regulatory divergence between the US, EU, China, and others. For example, with data privacy, many global internet companies are now GDPR compliant even if they are primarily domiciled elsewhere because they have European interests or customers.

Unfortunately, even in the long term, regulatory convergence may be difficult because AI is also viewed as strategic security and economic asset to many countries, and thus some do not want to impede any technological progress with regulation [63]. As regulations in certain locales change, the main responsibility for tracking and implementing new regulation enforcement mechanisms will primarily fall to the management power of the platform (though this depends on the specific nature of the regulation). As mentioned previously, this power could be, for example, an independent NGO or could be decentralized through consensus mechanisms involving marketplace peers. Overall, regulation should plan a strong part in the operation and governance of the AI marketplace.

VII. AI MARKETPLACE SCENARIO

In this section, we sketch out a realistic scenario to illustrate how the different components of the AI marketplace would work as an integrative whole.

We consider the following scenario: *A hospital contracts a medical AI company to develop an AI-powered system for the triage of brain injuries using CT images in the emergency room (inspired by an actual commercial product* [83]). However, the hospital does not have an existing broad dataset of brain CT images (that also contain granular patient metadata) and open imaging datasets fall short. The hospital only has a smaller validation dataset from a subset of their patients. As such, the AI company must use the AI marketplace to either acquire training data or training updates (for federated learning), develop and train the model, and then validate the model with AI auditors.

Within this scenario, we envision the following AI development workflow centered around the AI marketplace.

1) The hospital provides metadata about the validation dataset to the marketplace so that the validation dataset cannot be unilaterally changed later on.
2) The hospital describes the AI problem and the marketplace requests bids from matching AI companies. The hospital then selects a specific AI company for development.
3) The AI company (in collaboration with the hospital) uses the marketplace to send a data request to acquire training data or training updates. The AI marketplace sends the request to suitable matching data providers. The AI company and hospital weigh the cost and benefit of the responding providers in terms of, for example, dataset size, dataset demographics, and dataset patient diagnosis distribution.
4) After the data provider selection, the AI company develops and trains an initial model using, in this case, training updates from federated learning across the data providers. The AI marketplace can also track these updates through a blockchain and ensure that the updates are reliable and not malicious, partly through the smart contract agreements.
5) After suitable training, the AI company submits the model to the marketplace for checking performance against the validation dataset. As previously

mentioned, the maximum number of submissions is small and fixed to prevent fitting to the validation dataset.

6) After reaching a performance threshold, the AI company sends the model through the AI marketplace to auditors which consist of both independent AI auditors (to ensure performance and fairness) and government auditors (from an agency like the Food and Drug Administration in the USA, which regulates medical devices).
7) The AI model might need to go through changes before approval, therefore the AI company might repeat several steps.
8) After approval, the AI company might still perform model maintenance and process user requests to remove their data (withdrawing their consent in GDPR terminology). As mentioned, for these requests, technical solutions (like machine unlearning) exist, however, model performance may change and there will be a need for at least basic re-validation. In the case of a performance decrease below a threshold, there might also be a need for additional data providers.

The marketplace facilitates the actual payment to the data providers for their data or training updates along with the payment to the AI developer for the model development. The marketplace logs these transactions through the previously mentioned blockchain mechanism. Additionally, the transactions and development interactions can be governed by smart contracts also signed through the marketplace.

VIII. WHERE WE ARE NOW?

In Table 2, we provide the list of companies that are either providing an AI marketplace or in the process of building such a marketplace. To find such companies, we searched on Google using the keywords: ''online marketplace'', ''data marketplace'', and ''AI marketplace'' and extracted the first ten pages. We then manually visited all links from these pages and checked which describe an entity providing for the trading of AI models, a service to enable trading of AI models, or are in the process of building either of these. After six pages, the search results no longer provided any meaningful links. Eventually, we identified the 24 companies or frameworks listed in Table 1.

Most of these companies are based in either the USA or Europe. Among those which are currently available, none list more than 24 different models (Nauance Communications lists 24, Gravity AI lists 12, and IBM Imaging lists five models), thus suggesting that none have seen major or widespread adoption. The marketplaces which are somewhat mature primarily focus on the healthcare domain. However, these marketplaces are not operating in multiple countries potentially due to the need for regulatory approval of such models in each country or economic area (for example, by the US Food and Drug Administration).

The overarching goal of most of these AI marketplaces aligns with our vision of a general marketplace where buyers and sellers engage in transactions for AI models. In terms of the technical aspects for a successful AI marketplace, from the section above on technical aspects, most of the marketplaces have not yet incorporated these though they do often acknowledge the need for such aspects. For example, only two of them mention that they support scalable privacy-preserving model training paradigms like federated learning. As for architecture, most of the marketplaces are proprietary and are based on a centralized architecture. Though the few decentralized marketplaces are primarily based on distributed ledgers, similar to our vision. With regard to the pricing mechanism, most of them are using fixed pricing per model.

A. TECHNICAL LANDSCAPE OF CURRENT MARKETPLACE

As mentioned in Table 2, most of these marketplaces are still under development and their underlying technical details and planned functionalities are not public. However, given the available public information, current marketplaces fall into the following categories:

1) **AI model Trading:** In such a marketplace, an AI developer can upload their pre-trained model to a marketplace and customers can purchase access (an API) to use the model. SingularityNET and IBM imaging are examples.
2) **Data Trading:** In this type of marketplace, data owners make their data available to AI developers in a privacy-preserving manner. The marketplace also focuses on ensuring the quality of data including preventing malicious data. OSA Decentralized, Ocean Protocol, and Agorai are examples.
3) **Developer-Customer Matching:** This type of marketplace matches the varying AI customers and developers based on the customers' specific requirements and the developers' skills and domain knowledge. Nomidman, AI Global, Genesis AI, Bonseyes, Alphacat, Modzy, SingularityNET, and Orange AI are examples.
4) **Interoperability Standard:** Interoperability standards for AI models allows AI developers the freedom to create their model with their preferred tools and frameworks. This type of AI marketplace focuses on developing such a standard as an SDK. TensorTask, Genesis AI, Akira AI, Bonseyes, SingularityNET, Gravity AI, Kynisys, OVHcloud AI, Neuromation Algorithmia, GraphGrail AI, Agorai, IBM Imaging, and Nuance Communications are examples. As such, none of these marketplaces have publicly released their standards for use.

Among all these marketplaces, SingularityNET seems to be the most developed and has released beta versions of many components (that fulfill the stated objectives). Also, SingularityNET has the most ambitious goals with a final objective to build a comprehensive marketplace similar to the marketplace described in Section II.

Overall, the landscape of current AI marketplaces is still far from the one we envision in Section II. For example, in two

relatively developed marketplaces, i.e., SingularityNET and IBM Imaging, we find less than 30 total AI models even two years after these marketplaces launched. In contrast, major B2B software marketplaces (which were also launched recently) have thousands of applications. For example, the Microsoft Azure Marketplace,[3] Amazon AWS Marketplace,[4] and Google Cloud Platform Marketplace[5] have 14998, 9848, and 4088 applications respectively. Additionally, we find that current AI marketplaces primarily host models only from large well-known companies like Google DeepMind, IBM Watson, etc. Thus supporting the argument that smaller companies have a harder time entering the AI model marketplace (for a number of reasons as previously discussed) and thus helping motivate our work.

In terms of future developments, many of the marketplace companies look to help solve some of the current bottlenecks in model availability. For example, as mentioned, several marketplaces (refer to the prior section) are developing interoperability standards for AI development. Additionally, several marketplaces are developing comprehensive reputation systems to rate AI developers and companies. These systems have multiple objectives: they can help with the problem of malicious AI models and can provide a signal of developer quality. Finally, several other marketplaces, like Akira AI, are developing data sharing frameworks. These frameworks aim to integrate data from different relevant databases and create unified virtual datastores for use in model training.

IX. CONCLUSION

In this work, we outlined principles for a marketplace for AI models based on a decentralized online structure. Such a marketplace could help diffuse AI technology to smaller actors (like small and medium-size companies). We discussed the technical, economic, and regulatory aspects to consider while designing such a marketplace. We also described (often novel) technologies and solutions that can help address problems in these areas. For example, utilizing federated learning for privacy-preserving machine learning across marketplace actors. Finally, we studied the current state of various AI marketplaces and provided a comparative analysis of these marketplaces based on properties such as architecture, domain, and status. We found that most of these currently available marketplaces are centralized and company-driven with relatively few models per marketplace, thus suggesting that the development of AI marketplaces are still in their infancy.

REFERENCES

[1] M. Alloghani, D. Al-Jumeily, A. J. Aljaaf, M. Khalaf, J. Mustafina, and S. Y. Tan, "The application of artificial intelligence technology in healthcare: A systematic review," in *Applied Computing to Support Industry: Innovation and Technology*, M. I. Khalaf, D. Al-Jumeily, and A. Lisitsa, Eds. Cham, Switzerland: Springer, 2020, pp. 248–261.

[3] azuremarketplace.microsoft.com
[4] aws.amazon.com/marketplace
[5] cloud.google.com/marketplace

[2] SingularityNET, "SingularityNet Whitepaper 2.0: A decentralized, open market and network for AIS," SingularityNET, Amsterdam, The Netherlands, Tech. Rep. 02, Feb. 2019.
[3] Jed Record. (2017). *The Challenges of Open Source Monetization*. hackernoon.com. [Online]. Available: https://hackernoon.com/the-challenges-of-open-source-monetization-824bccbfe49b
[4] D. A. Norman, "The research-practice gap: The need for translational developers," *Interactions*, vol. 17, no. 4, pp. 9–12, Jul. 2010.
[5] J. Haucap and U. Heimeshoff, "Google, facebook, amazon, eBay: Is the Internet driving competition or market monopolization?" *Int. Econ. Econ. Policy*, vol. 11, nos. 1–2, pp. 49–61, Feb. 2014.
[6] A. Etzioni and O. Etzioni, "Keeping ai legal," *Vand. J. Ent. Tech. L.*, vol. 19, p. 133, Feb. 2016.
[7] M. Fredrikson, S. Jha, and T. Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 1322–1333.
[8] M. Veale, R. Binns, and L. Edwards, "Algorithms that remember: Model inversion attacks and data protection law," *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 376, no. 2133, Nov. 2018, Art. no. 20180083.
[9] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 739–753.
[10] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 3–18.
[11] I. GAMBO, O. Oluwagbemi, and P. Achimugu, "Lack of interoperable health information systems in developing countries: An impact analysis," *J. Health Informat. Developing Countries*, vol. 5, no. 1, pp. 1–12, 2011.
[12] M. Lehne, J. Sass, A. Essenwanger, J. Schepers, and S. Thun, "Why digital medicine depends on interoperability," *NPJ Digit. Med.*, vol. 2, no. 1, pp. 1–5, Dec. 2019.
[13] The Economist. (2017). *Google Leads in the Race to Dominate Artificial Intelligence*. economist.com. [Online]. Available: https://www.economist.com/business/2017/12/07/google-leads-in-the-race-to-dominate-artificial-intelligence
[14] V. A. Mehri, D. Ilie, and K. Tutschku, "Privacy and DRM requirements for collaborative development of AI applications," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–8.
[15] Teradata. (2017). *State of Artificial Intelligence for Enterprises*. [Online]. Available: www.multivu.com/players/English/8075951-teradata-state-of-artificial-intelligence-ai-for-enterprises
[16] WebFX. (2020). *Ai Pricing: How Much Does Artificial Intelligence Cost*. [Online]. Available: https://www.webfx.com/internet-marketing/ai-pricing.html
[17] S. Hershey, S. Chaudhuri, D. P. W. Ellis, J. F. Gemmeke, A. Jansen, R. C. Moore, M. Plakal, D. Platt, R. A. Saurous, B. Seybold, M. Slaney, R. J. Weiss, and K. Wilson, "CNN architectures for large-scale audio classification," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2017, pp. 131–135.
[18] J. Wang, Y. Chen, W. Feng, H. Yu, M. Huang, and Q. Yang, "Transfer learning with dynamic distribution adaptation," *ACM Trans. Intell. Syst. Technol.*, vol. 11, no. 1, pp. 1–25, Feb. 2020.
[19] K. Hsieh, A. Phanishayee, O. Mutlu, and B. P. Gibbons, "The non-IID data quagmire of decentralized machine learning," 2019, *arXiv:1910.00189*. [Online]. Available: https://arxiv.org/abs/1910.00189
[20] John Lucker. (2015). *The Dangers of Monetizing Data*. [Online]. Available: https://deloitte.wsj.com/cio/2015/06/30/the-dangers-of-monetizing-data/
[21] European Commission. (2020). *Exchange of Electronic Health Records Across the Eu*. europa.eu. [Online]. Available: https://ec.europa.eu/digital-single-market/en/exchange-electronic-health-records-across-eu
[22] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.
[23] N. Vulkan, *The Economics of E-Commerce: A Strategic Guide to Understanding and Designing the Online Marketplace*. Princeton, NJ, USA: Princeton Univ. Press, 2003.
[24] M. Tzanetakis, G. Kamphausen, B. Werse, and R. von Laufenberg, "The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets," *Int. J. Drug Policy*, vol. 35, pp. 58–68, Sep. 2016.
[25] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," 2016, *arXiv:1610.05492*. [Online]. Available: http://arxiv.org/abs/1610.05492

[26] A. Hard, K. Rao, R. Mathews, S. Ramaswamy, F. Beaufays, S. Augenstein, H. Eichner, C. Kiddon, and D. Ramage, "Federated learning for mobile keyboard prediction," 2018, *arXiv:1811.03604*. [Online]. Available: http://arxiv.org/abs/1811.03604

[27] A. Bellet, R. Guerraoui, M. Taziki, and M. Tommasi, "Personalized and private peer-to-peer machine learning," in *Proc. Int. Conf. Artif. Intell. Statist.*, Mar. 2018, pp. 473–481.

[28] H. Cheng, P. Yu, H. Hu, F. Yan, S. Li, H. Li, and Y. Chen, "LEASGD: An efficient and privacy-preserving decentralized algorithm for distributed learning," 2018, *arXiv:1811.11124*. [Online]. Available: https://arxiv.org/abs/1811.11124

[29] Y. Liu, Y. Liu, Z. Liu, J. Zhang, C. Meng, and Y. Zheng, "Federated forest," 2019, *arXiv:1905.10053*. [Online]. Available: http://arxiv.org/abs/1905.10053

[30] E. Bakopoulou, B. Tillman, and A. Markopoulou, "A federated learning approach for mobile packet classification," 2019, *arXiv:1907.13113*. [Online]. Available: http://arxiv.org/abs/1907.13113

[31] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, "MockDroid: Trading privacy for application functionality on smartphones," in *Proc. 12th Workshop Mobile Comput. Syst. Appl. HotMobile*, 2011, pp. 49–54.

[32] W. Jin, M. Xiao, M. Li, and L. Guo, "If you do not care about it, sell it: Trading location privacy in mobile crowd sensing," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Apr. 2019, pp. 1045–1053.

[33] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, no. 1, p. 119, 2004.

[34] M. Zimmer, "Addressing conceptual gaps in big data research ethics: An application of contextual integrity," *Social Media + Soc.*, vol. 4, no. 2, Apr. 2018.

[35] A. Khan, A. Sohail, U. Zahoora, and A. S. Qureshi, "A survey of the recent architectures of deep convolutional neural networks," *Artif. Intell. Rev.*, vol. 53, no. 8, pp. 5455–5516, 2020.

[36] A. Ghosh and A. Roth, "Selling privacy at auction," *Games Econ. Behav.*, vol. 91, pp. 334–346, May 2015.

[37] M. M. Pai and A. Roth, "Privacy and mechanism design," *ACM SIGecom Exchanges*, vol. 12, no. 1, pp. 8–29, Jun. 2013.

[38] R. J. Kauffman, H. Lai, and C.-T. Ho, "Incentive mechanisms, fairness and participation in online group-buying auctions," *Electron. Commerce Res. Appl.*, vol. 9, no. 3, pp. 249–262, May 2010.

[39] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, no. 1, pp. 8–37, Mar. 1961.

[40] A. Ghosh and R. Kleinberg, "Optimal contest design for simple agents," *ACM Trans. Econ. Comput.*, vol. 4, no. 4, pp. 1–41, Aug. 2016.

[41] D. Easley and A. Ghosh, "Behavioral mechanism design: Optimal crowdsourcing contracts and prospect theory," *ACM SIGecom Exchanges*, vol. 14, no. 1, pp. 89–94, Nov. 2015.

[42] O. Gürtler and M. Kräkel, "Optimal tournament contracts for heterogeneous workers," *J. Econ. Behav. Org.*, vol. 75, no. 2, pp. 180–191, Aug. 2010.

[43] L. Su, "Defending distributed systems against adversarial attacks: Consensus, consensusbased learning, and statistical learning," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 47, no. 3, pp. 24–27, Jan. 2020.

[44] J. Lin, M. Du, and J. Liu, "Free-riders in federated learning: Attacks and defenses," 2019, *arXiv:1911.12560*. [Online]. Available: http://arxiv.org/abs/1911.12560

[45] A. N. Bhagoji, S. Chakraborty, P. Mittal, and S. Calo, "Analyzing federated learning through an adversarial lens," in *Proc. Int. Conf. Mach. Learn.*, 2019, pp. 634–643.

[46] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction apis," in *Proc. 25th USENIX Secur. Symp. (USENIX Secur.)*, 2016, pp. 601–618.

[47] H. Jia, C. A. Choquette-Choo, and N. Papernot, "Entangled watermarks as a defense against model extraction," 2020, *arXiv:2002.12200*. [Online]. Available: http://arxiv.org/abs/2002.12200

[48] *Sarbanes-Oxley Act*, Sarbanes-Oxley Act, Washington, DC, USA, 2002.

[49] A. Kapishnikov, T. Bolukbasi, F. B. Viégas, and M. Terry, "XRAI: Better attributions through regions," in *Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV)*, Seoul, South Korea, Oct./Nov. 2019, pp. 4947–4956.

[50] A. Ghorbani, J. Wexler, J. Y. Zou, and B. Kim, "Towards automatic concept-based explanations," in *Proc. Adv. Neural Inf. Process. Syst.*, 2019, pp. 9277–9286.

[51] Y. Chai and W. Li, "Towards deep learning interpretability: Atopic modeling approach," in *Proc. 40th Int. Conf. Inf. Syst. (ICIS)*, vol. 1, H. Krcmar, J. Fedorowicz, W. FongBoh, J. M. Leimeister, and S. Wattal, Eds. Munich, Germany: Association for Information Systems, Dec. 2019, pp. 359–367.

[52] D. C DeAndrea, "Advancing warranting theory," *Commun. Theory*, vol. 24, no. 2, pp. 186–204, 2014.

[53] A. Hagiu and S. Rothman, "Network effects aren't enough," *Harvard Bus. Rev.*, vol. 94, no. 4, pp. 64–71, 2016.

[54] F. Zhu and M. Iansiti, "Why some platforms thrive and others don't," *Harvard Bus. Rev.*, vol. 97, no. 1, pp. 118–125, Jan. 2019.

[55] M. Landeweerd, T. Spil, and R. Klein, "The success of Google search, the failure of Google health and the future of Google plus," in *Grand Successes and Failures in IT. Public and Private Sectors*, Y. K. Dwivedi, H. Z. Henriksen, D. Wastell, and R. De', Eds. Berlin, Germany: Springer, 2013, pp. 221–239.

[56] H. Mitomo, "Data network effects: Implications for data business," in *Proc. 28th Eur. Regional ITS Conf.*, Geneva, Switzerland: International Telecommunications Society (ITS), 2017, Art. no. 169484.

[57] S. Li, Y. Liu, and S. Bandyopadhyay, "Network effects in online two-sided market platforms: A research note," *Decis. Support Syst.*, vol. 49, no. 2, pp. 245–249, May 2010.

[58] Y. Gu and F. Zhu, "Trust and disintermediation: Evidence from an online freelance marketplace," *Acad. Manage. Proc.*, vol. 2018, no. 1, Aug. 2018, Art. no. 13315.

[59] S. Ba, B. Andrew Whinston, and H. Zhang, "Building trust in the electronic market through an economic incentive mechanism," in *Proc. 20th Int. Conf. Inf. Syst., ICIS*, P. De Janice and I. DeGross, Eds. Charlotte, NC, USA: Association for Information Systems, Dec. 1999, pp. 208–213.

[60] C. X. Ou, W. P. Wong, and M. Robert Davison, "Beyond institution-based trust: Building effective online marketplaces with social mechanisms," in *Proc. Int. Conf. Inf. Syst., ICIS*, R. Sabherwal and M. Sumner, Eds. Saint Louis, MI, USA: Association for Information Systems, Dec. 2010, p. 207.

[61] M. Luca, "Designing online marketplaces: Trust and reputation mechanisms," *Innov. Policy Economy*, vol. 17, pp. 77–93, Jan. 2017.

[62] H. Yoganarasimhan, "The value of reputation in an online freelance marketplace," *Marketing Sci.*, vol. 32, no. 6, pp. 860–891, Nov. 2013.

[63] David Shepardson. (2020). *White House Proposes Regulatory Principles to Govern Ai Use*. [Online]. Available: https://www.reuters.com/article/us-tech-ces-ai-white-house/white-house-proposes-regulatory-principles-to-govern-ai-use-idUSKBN1Z60GL

[64] European Commission. (2020). *White Paper on Artificial Intelligence a European Approach to Excellence and Trust*. [Online]. Available: https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[65] Nicholas Wallace. (2020). *Europe Plans to Strictly Regulate High-Risk ai Technology*. [Online]. Available: https://www.sciencemag.org/news/2020/02/europe-plans-strictly-regulate-high-risk-ai-technology

[66] High-Level Expert Group on Artificial Intelligence, "Ethics guidelines for trustworthy AI," Eur. Commission, Brussels, Belgium, Tech. Rep. KK-02-19-841-EN-N, Apr. 2019. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[67] A. Kumar, T. Braud, S. Tarkoma, and P. Hui, "Trustworthy AI in the age of pervasive computing and big data," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2020, pp. 1–6.

[68] J. Singh, C. Millard, C. Reed, J. Cobbe, and J. Crowcroft, "Accountability in the IoT: Systems, law, and ways forward," *Computer*, vol. 51, no. 7, pp. 54–65, Jul. 2018.

[69] E. Ntoutsi *et al.*, "Bias in data-driven AI systems—An introductory survey," 2020, *arXiv:2001.09762*. [Online]. Available: http://arxiv.org/abs/2001.09762

[70] Y. Cao and J. Yang, "Towards making systems forget with machine unlearning," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 463–480.

[71] L. Bourtoule, V. Chandrasekaran, C. A. Choquette-Choo, H. Jia, A. Travers, B. Zhang, D. Lie, and N. Papernot, "Machine unlearning," 2019, *arXiv:1912.03817*. [Online]. Available: http://arxiv.org/abs/1912.03817

[72] L. Graves, V. Nagisetty, and V. Ganesh. (2020). *Does Ai Remember? Neural Networks and the Right to be Forgotten*. [Online]. Available: http://hdl.handle.net/10012/15754

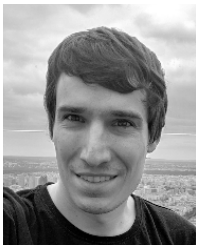
[73] J. Shu, R. Zheng, and P. Hui, "Cardea: Context-aware visual privacy protection for photo taking and sharing," in *Proc. 9th ACM Multimedia Syst. Conf.*, Jun. 2018, pp. 304–315.

[74] U.S. Food and Drug Administration, "Artificial intelligence/machine learning (ai/ml)-based software as a medical device (SAMD) action plan," U.S. Food Drug Admin., White Oak, MD, USA, Tech. Rep. 145022, Jan. 2021.

[75] Benedict Mayaki. (2020). *Vatican Workshop on Ethics and Ai*. [Online]. Available: https://www.vaticannews.va/en/vatican-city/news/2020-02/vatican-airtificial-intelligence-ethics-workshop.html

[76] C. Cath, "Governing artificial intelligence: Ethical, legal and technical opportunities and challenges," *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 376, no. 2133, Nov. 2018, Art. no. 20180080.
[77] O. Lynskey, "Criminal justice profiling and EU data protection law: Precarious protection from predictive policing," *Int. J. Law Context*, vol. 15, no. 2, pp. 162–176, Jun. 2019.
[78] European Commission, "Report on the safety and liability implications of artificial intelligence, the Internet of Things and robotics," Eur. Commission, Brussels, Belgium, Tech. Rep. COM(2020)64 final, Feb. 2020. [Online]. Available: https://shorturl.at/cfhlJ
[79] J. Lehman and M. Dolan. (2020). *Strict Products Liability: One More Thing the Internet is Disrupting*. [Online]. Available: https://www.law.com/thelegalintelligencer/2020/01/22/strict-products-liability-one-more-thing-the-internet-is-disrupting/
[80] C. Busch, "When product liability meets the platform economy: A European perspective on oberdorf V. Amazon," *J. Eur. Consum. Market Law*, vol. 8, pp. 173–174, Oct. 2019.
[81] Reuters. (2020). *U.S. Government Limits Exports of Artificial Intelligence Software*. [Online]. Available: https://shorturl.at/nvyzI
[82] E. S. Medeiros, "The changing fundamentals of US-China relations," *Washington Quart.*, vol. 42, no. 3, pp. 93–119, Jul. 2019.
[83] P. Ojeda, M. Zawaideh, M. Mossa-Basha, and D. Haynor, "The utility of deep learning: Evaluation of a convolutional neural network for detection of intracranial bleeds on non-contrast head computed tomography studies," *Proc. SPIE* vol. 10949, pp. 899–906, Mar. 2019.

ABHISHEK KUMAR received the M.S. degree in knowledge service engineering from KAIST, in 2016. He is currently pursuing the Ph.D. degree in computer science with the University of Helsinki. His research interests broadly include security and privacy in ubiquitous computing, extended reality space, and applied machine learning.



BENJAMIN FINLEY received the B.S. degree in software engineering from the Milwaukee School of Engineering, Milwaukee, WI, USA, and the M.S. and D.S. degrees in telecommunication engineering from Aalto University, Helsinki, Finland. He is currently a postdoctoral researcher with the Department of Computer Science, University of Helsinki. His current research interests include big telecom data analysis and user quality of experience.

TRISTAN BRAUD (Member, IEEE) received the M.Sc. degree from Politecnico di Torino, Italy, and Grenoble INP, France, and the Ph.D. degree from Université Grenoble Alpes, France, in 2016. He is currently a Postdoctoral Fellow with the HKUST-DT Systems and Media Lab (SyMLab), Hong Kong University of Science and Technology. He was an engineering student at Grenoble INP Phelma/Ensimag, France. His major research interests include pervasive and mobile computing, cloud and edge computing, human cantered system designs, and AR.

SASU TARKOMA (Senior Member, IEEE) is currently a Professor of computer science with the University of Helsinki, the Head of the Department of Computer Science, the Director of the Nokia Centre for Advanced Research, and the Director of the Helsinki Centre for Data Science. He has seven granted U.S. patents. His research interests are Internet technology, distributed systems, and mobile and ubiquitous computing. He was a recipient of several best paper awards, e.g., the IEEE PerCom, ACM SIGCOMM Computer Communication Review, and ACM SIGOPS Operating System Review.

PAN HUI (Fellow, IEEE) received the bachelor's and M.Phil. degrees from the University of Hong Kong, and the Ph.D. degree from the Computer Laboratory, University of Cambridge. He is currently the Nokia Chair Professor of data science and a Professor of computer science with the University of Helsinki. He is also the Director of the HKUST-DT System and Media Laboratory, Hong Kong University of Science and Technology. He has published around 300 research articles and with over 17,000 citations. He has 29 granted and filed European and U.S. patents in the areas of augmented reality, data science, and mobile computing. He is an ACM Distinguished Scientist and a Member of the Academy of Europe.