IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 16, 2018, accepted December 28, 2018, date of publication January 1, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890507

Blockchain for AI: Review and Open Research Challenges

KHALED SALAH[1], (Senior Member, IEEE), M. HABIB UR REHMAN[2], NISHARA NIZAMUDDIN[1], AND ALA AL-FUQAHA[3]

[1]Department of Electrical and Computer Engineering, Khalifa University of Science and Technology, Abu Dhabi 127788, UAE
[2]Department of Computer Science, National University of Computer and Emerging Sciences, Lahore 54770, Pakistan
[3]NEST Research Lab, Computer Science Department, College of Engineering and Applied Sciences, Western Michigan University, Kalamazoo, MI 49008, USA

Corresponding author: Khaled Salah (khaled.salah@ku.ac.ae)

ABSTRACT Recently, artificial intelligence (AI) and blockchain have become two of the most trending and disruptive technologies. Blockchain technology has the ability to automate payment in cryptocurrency and to provide access to a shared ledger of data, transactions, and logs in a decentralized, secure, and trusted manner. Also with smart contracts, blockchain has the ability to govern interactions among participants with no intermediary or a trusted third party. AI, on the other hand, offers intelligence and decision-making capabilities for machines similar to humans. In this paper, we present a detailed survey on blockchain applications for AI. We review the literature, tabulate, and summarize the emerging blockchain applications, platforms, and protocols specifically targeting AI area. We also identify and discuss open research challenges of utilizing blockchain technologies for AI.

INDEX TERMS Artificial intelligence, machine learning, blockchain, cybersecurity, smart contracts, consensus protocols.

I. INTRODUCTION

Blockchain is one the most hyped innovations these days, and it has been gaining a lot of traction as a horizontal technology to be widely adopted in various fields [1]–[3]. Since its inception in 2008, blockchain continued to emerge as a disruptive innovation that will revolutionize the way we interact, automate payments, trace and track transactions [4]. Blockchain can be highly cost effective in eliminating the need for a centralized authority to govern and verify interactions and transactions among several participants. In blockchain, every transaction is cryptographically signed and verified by all mining nodes which hold a replica of the entire ledger which contains chained blocks of all transactions. This creates a secure, synchronized and shared timestamped records that cannot be altered [5]. Another prominent field that is gaining huge traction is artificial intelligence(AI) which allows a machine to have cognitive functions to learn, infer, and adapt based on data it collects. Recent market research predicts that AI market will grow up to 13 trillion US dollars by the year 2030.

The massive production and generation of data by sensing systems, IoT devices, social media, and web applications have contributed to the rise of AI [6]. Such data can be utilized by various machine learning and deep learning techniques [7] to perform variety of analytics. To date, the majority of machine learning and deep learning methods of AI rely on a centralized model for training in which a group of servers run a specific model against training and validating datasets and many organizations like Google, Apple, Facebook and Amazon manage the huge volumes of data to make informed decisions [8]. However, the centralized nature of AI may lead to the possibility of data tampering, as data can be subject to hacking and manipulation as it is managed and stored in centralized manner [9]. Moreover, the data provenance and authenticity of the sources generating the data are not guaranteed [10]. This may lead to AI decision outcomes that can be highly erroneous, risky, and dangerous.

The concept of decentralized AI has been recently emerging. Decentralized AI is basically a combination of AI and blockchain [8]. The decentralized AI enables to process and perform analytics or decision making on trusted, digitally signed, and secure shared data that has been transacted and stored on the blockchain, in a distributed and decentralized fashion, without Trusted Third Parties or intermediaries [8], [9]. AI is known to work with huge volumes of data, and blockchain has now been foreseen as a trusted platform to

store such data. The feature of blockchain smart contracts gives the ability to program the blockchain to govern transactions among participants involved in decision making or generating and accessing the data [11]. Smart contract-based autonomous systems and machines can learn and adapt to changes over time, and make trusted and accurate decision outcomes that are verified and validated by all mining nodes of the blockchain. Such decisions cannot be refuted, and can be traced, tracked and verified by all participating entities. AI techniques that utilize blockchain can offer decentralized learning to facilitate a trust and secure sharing of knowledge and decision outcomes across a large number of autonomous agents, which can contribute, coordinate, and vote on further decisions [12], [13].

To date, the literature lacks comprehensive reviews and studies on the role that blockchain plays in the context of AI. Existing literature reveals that researchers studied blockchain and AI in isolation, and their applications in various vertical domains and businesses [14]–[27]. A couple of studies discussed the integration of AI and blockchain, and the implications of such integration on the way we live, work, interact, and transact [9], [28]. The primary contributions of this paper can be summarized as follows:

- We give an overview of blockchain basics and key features and how these features can be leveraged for AI.
- We discuss how the integration of AI and blockchain can help in developing a new ecosystem of decentralized economy. In addition, we outline the key benefits brought by this integration.
- We present a detailed taxonomy of blockchain platforms, architecture and infrastructure types, and consensus protocols, along with existing decentralized AI applications.
- We report and discuss multiple practical use cases of AI applications and implementations utilizing blockchain in different vertical domains.
- We identify and outline open research challenges in adopting and leveraging blockchain features for future AI applications.

The rest of the paper is organized as follows. Section II discusses the background of blockchain and AI technologies and how blockchain helps in transforming existing AI techniques. Section III presents the detailed taxonomy and Section IV describes blockchain applications for AI. Various open research challenges and issues are categorized in Section V. Section VI concludes the paper.

II. BACKGROUND

In this section, we give an overview of blockchain and AI and discuss how blockchain technology can be leveraged to transform, in many radical ways, AI and its applications.

A. BLOCKCHAIN

Blockchain is a distributed, open source, immutable, public digital ledger which is distributed among networked peers [4]. Fundamentally, blockchain is a chain of blocks that make up the ledger. This ledger holds a permanent record of transactions and interactions that took place among participants accessing the distributed and decentralized blockchain network [11]. Each block contains the details of the transaction and the asset exchanges (*i.e.*, Ether or Bitcoin) that took place between the users [4], [11]. Smart Contracts are codes that can be executed by the blockchain mining nodes. A smart contract is a self-executing code that can verify the enforcement of predefined terms and conditions [29]. Instead of validating digital currencies, as in Bitcoin, the blockchain mining nodes execute, verify and store data in blocks. A smart contract is triggered by consigning a transaction to its Ethereum address and executing it depending on the input given for that transaction. Ethereum is a blockchain based open source distributed platform that enables to program smart contracts [11]. Ethereum uses Ether as a currency for making payments for the transactions carried out on the Ethereum blockchain. Each participant in the Ethereum network is identified uniquely by an Ethereum Address (EA).

Conventional blockchain is a very expensive medium for storing large amounts of data. For example, storing large files or documents on Bitcoin blockchain is very expensive as the size limit per block is limited to one megabyte [35]. To solve this problem, a decentralized storage medium is used for storing such data and hashes of the data are linked with the blockchain blocks or used within the blockchain smart contract code. Among the popular decentralized storage technologies are the Interplanetary File System (IPFS) [35], Swarm [36], Filecoin [37], BigChainDB [38], Storj [39], and many others. IPFS is a peer-to-peer, distributed and decentralized file system that is connected across nodes of computers that share a common file system [35]. It is content-addressable, which means that the contents of IPFS can be accessed using IPFS hash addresses. Moreover, this file system becomes indisputable, since it works similar to the blockchain network by having a list of nodes, and does not allow any tampering of files. Therefore, providing high throughput and content-addressed block storage model, with content-addressed hyperlinks. In addition, due to its decentralized nature, there is not a single point of failure *i.e.*, if one device gets disconnected, the file can still be accessed [35].

B. ARTIFICIAL INTELLIGENCE (AI)

The field of AI research defines itself as the study of ''intelligent agents,'' *i.e.*, any device that perceives its environment and takes actions that maximize its chance of success at some goal [40]. Most AI systems in development today are typically specialized expert systems that use a database of knowledge to make decisions. However, many researchers are working to build AI systems that can apply truly intelligent decision making processes to a restricted set of problems, some of which may positively impact our daily lives. Table 1 shows few emerging trends in AI applications such as explainable AI [9], [30], digital twins [31], automated machine learning [32], hybrid learning models [33], and lean and augmented data learning [34], and the perceived benefits

TABLE 1. Latest trends in AI applications and benefits of using blockchain.

Trends	Objective(s)	Applications	Blockchain Benefits
Explainable AI [9], [30]	Designing trustworthy and interpretable transparent AI algorithms to know why the algorithm is reaching a specific decision	- Healthcare - Military - Autonomous Vehicles	- Trust - Tracing Executions - Reliability
Digital Twins [31]	Translating data and intelligence from complex physical systems into applications and simulations in digital world	- Wind Turbines - Aircraft Engines - Offshore Vessels	- Trust - Provenance - Reliability
Automated Machine Learning [32]	Automating the whole process of machine learning from raw data acquisition to knowledge management in order to reduce manual work and faster application development	- Big Data Analytics - Industry 4.0 Systems - Massive Production of Intelligent Devices	- Permanence - Immutability
Hybrid Learning Models [33]	Combining different machine learning models to reach better informed decisions	- Real-time - Decision-agnostic - Data source-agnostic	- Trust - Provenance - Performance
Lean and Augmented Data Learning [34]	Enabling transfer learning among different AI applications to ensure high availability of relevant and accurate data	- Low data availability applications	- Trust - Provenance - Reliability

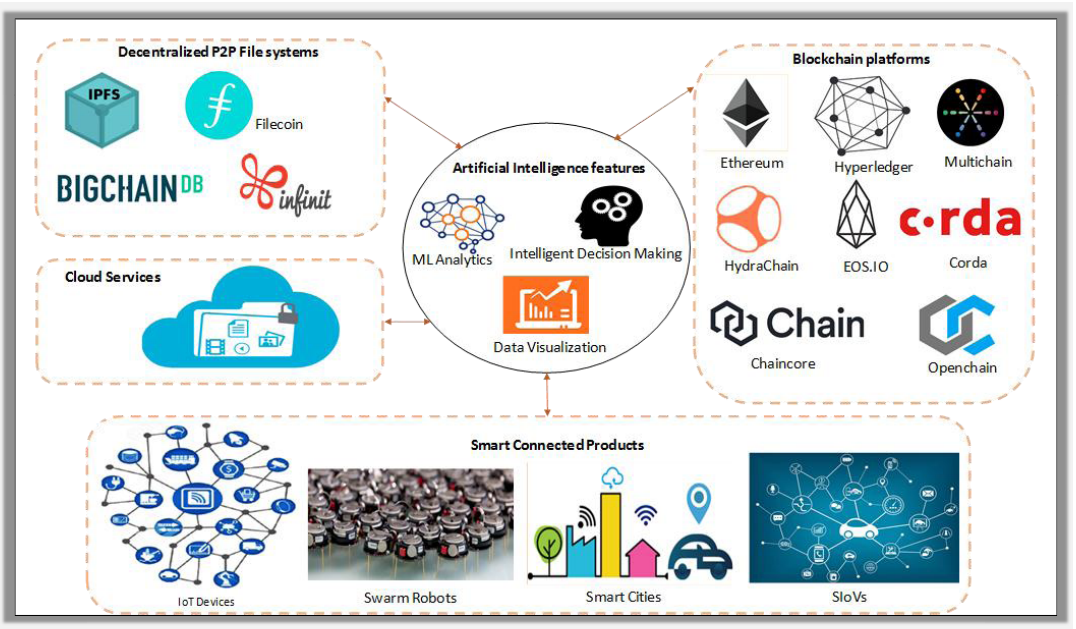


FIGURE 1. An overview of AI systems and features in relation to blockchain and IoT-enabled ecosystems.

of using blockchain technologies. By integrating AI and blockchain technologies, decentralized AI applications and algorithms can be developed, with access to an identical view of a secure, trusted, shared platform of data, logs, knowledge, and decisions. Such platform can also be used to host a trusted trail of all records taken by AI algorithms before, during, and after the learning and decision making process [19].

C. HOW BLOCKCHAIN CAN TRANSFORM AI

Many shortcomings of AI and blockchain can be addressed effectively by combining both technological ecosystems [19], [41]. AI algorithms rely on data or information to learn, infer, and make final decisions. The machine learning algorithms work better when data are collected from a data repository or a platform that is reliable, secure, trusted, and credible. Blockchain serves as a distributed ledger on which data can be stored and transacted in a way that is cryptographically signed, validated, and agreed on by all mining nodes. Blockchain data are stored with high integrity and resiliency, and cannot be tampered with. When smart contracts are used for machine learning algorithms to make decisions and perform analytics, the outcome of these decisions can be trusted and undisputed. The consolidation of AI and blockchain can create secure, immutable, decentralized system for the highly sensitive information that AI-driven systems must collect, store, and utilize [41]. This concept results in significant improvements to secure the data and information in various fields, including medical, personal, banking and financial, trading, and legal data.

Figure 1 shows that AI can benefit from the availability of many blockchain platforms for executing machine learning

TABLE 2. Key features and benefits of blockchain integration with AI.

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

algorithms and tracing data that are stored on decentralized P2P storage systems. These data are typically originated by smart connected products that include variety of sources such as IoT devices, swarm robots, smart cities, buildings, and vehicles. The features and services of the cloud can be also harnessed for off-chain machine learning analytics and intelligent decision making, and for data visualization. Some of the significant features (as listed in Table 2) of leveraging blockchain for AI can be summarized as follows:

- **Enhanced Data Security.** Information held within blockchain is highly secure. Blockchains are very well known for storing sensitive and personal data in a diskless environment. Blockchain databases hold data that are digitally signed, which means only the ''respective private keys'' must be kept secure [42]. This allows AI algorithms to work on secure data, and thereby ensuring more trusted and credible decision outcomes.
- **Improved Trust on Robotic Decisions.** Any decision made by AI agents becomes dysfunctional when it is difficult for consumers or users to understand and trust. Blockchain is well known for recording transactions in decentralized ledgers on a point-by-point basis, making it easier to accept and trust the decisions made, with confidence that the records have not been tampered with, during the human-involved auditing process [42]. Recording the decision making process of an AI system on a blockchain would increase transparency and it would gain public trust to understand the robotic decisions [43]. The need for a third party auditor can be eliminated in a swarm robotic ecosystem, where the consensus in the swarm can be achieved through an absolutely decentralized approach [42]–[44].
- **Collective Decision Making.** In a robotic swarm ecosystem, all the agents need to work in coordination to achieve the swarm goal [44]–[46]. The decentralized and distributed decision-making algorithms have been adopted in many robotic applications, without the need for a central authority. Robots take decisions by voting and outcomes are determined by majority rules. Each robot can cast its vote in the form of a transaction, where blockchain is public for all robots which can be utilized for verification of voting results. This process is repeated by all robots until the swarm comes to a decisive conclusion.
- **Decentralized Intelligence.** For taking smart high level decisions which involve multiple agents to perform different subtasks that have access to the common training data (*e.g.,* in case of supervised learning), different individual cybersecurity AI agents can be combined to provide fully coordinated security across the underlying networks and to solve scheduling issues [45], [47].
- **High Efficiency.** Multiuser business processes, which involve multiple stakeholders such as individual users, business firms, and governmental organizations, are inherently inefficient due to multiparty authorization of business transactions. The integration of AI and blockchain technologies enables intelligent Decentralized Autonomous Agents (or DAOs) for automatic and fast validation of data/value/asset transfers among different stakeholders [48].

III. TAXONOMY

This section presents a detailed taxonomic discussion of key concepts to enable blockchain technologies for AI applications. Figure 2 shows the classification tree of existing works found in the literature which we categorized in terms of decentralization of AI methodologies and operations, blockchain infrastructure and types, and the underlying consensus protocols utilized for distributed decentralized transaction validations across underlying networks.

A. DECENTRALIZED AI APPLICATIONS

AI applications operate autonomously in order to perform informed decisions by executing different planning, search, optimization, learning, knowledge discovery, and knowledge management strategies. However, the decentralization of AI operations is a complex and challenging task.

1) AUTONOMIC COMPUTING

One of the key goals of AI applications is to enable fully (or partially) autonomous operations whereby multiple intelligent agents (*i.e.*, small computer programs) perceive their constituent environments, preserve their internal states, and perform specified actions accordingly [49]. In order to operate autonomously, modern computing systems need to handle massive heterogeneity at all verticals including data sources, devices, data processing systems, data storage systems, and application interfaces, to name a few. The enablement of multiagent systems at all verticals does not only facilitate the handling of heterogeneity but it also helps in establishing inter-layer and intralayer operability across entire systems [50]. The blockchain architecture can play a vital role by ensuring operational decentralization and keeping permanent footprints of interactions between users, data, applications,

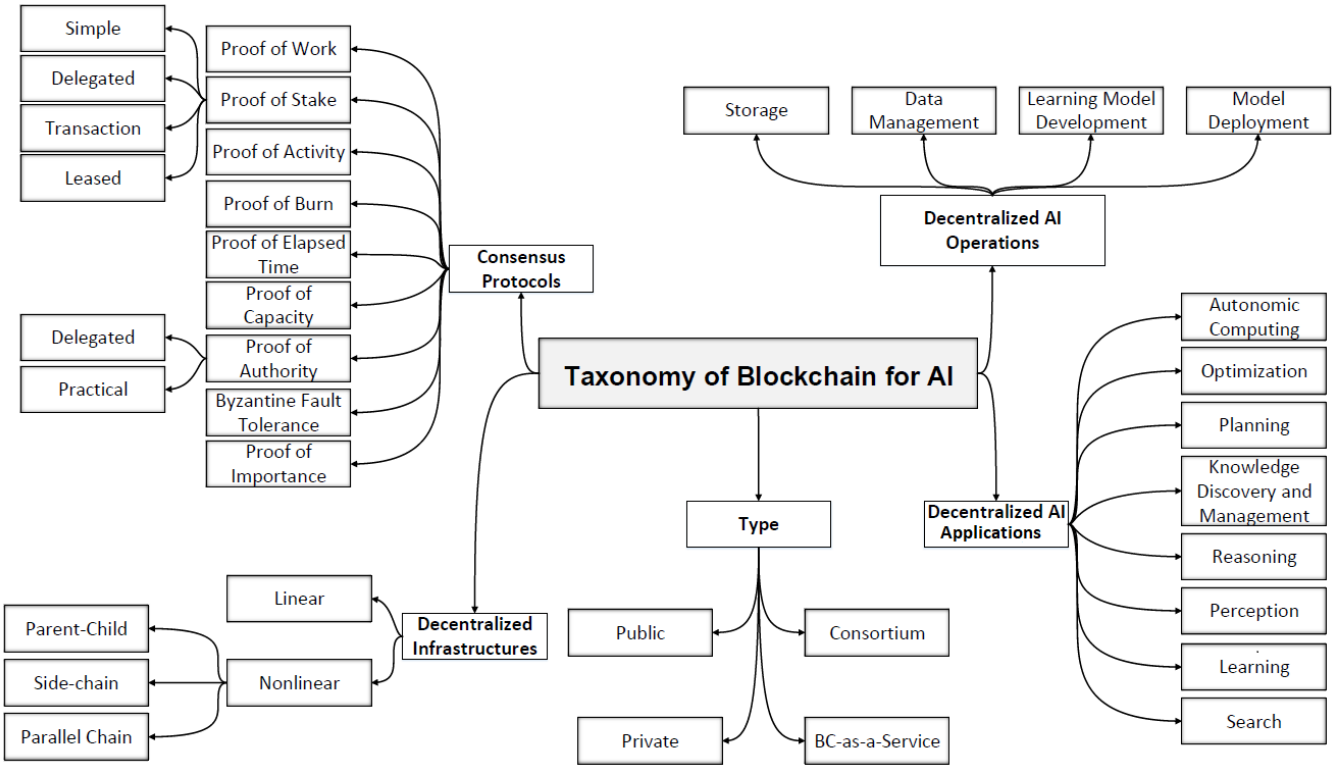


FIGURE 2. Taxonomy of blockchain for AI.

devices, and systems which leads toward the development of fully decentralized autonomous systems.

2) OPTIMIZATION

Finding a set of best solutions from all possible solutions is one of the main features of AI-enabled applications and systems [51]. Modern AI applications and systems operate in various environments including pervasive and ubiquitous environments (*e.g.,* edge computing systems), resource-constrained environments (*e.g.,* mobile devices/systems), geographically bounded systems (*e.g.,* personal area networks, wireless local area networks, etc.), and centralized massively parallel and distributed computing systems (*e.g.,* cloud computing systems) [52]. Based upon application-level and system-level objectives, the optimization strategies work in constrained or unconstrained environments [53]. These strategies facilitate finding best solutions such as selecting most relevant data sources in pervasive environments, best candidate edge or cloud servers for data and application processing, or enabling the resource-efficient data management in large-scale distributed computing environments. Current optimization strategies are executed with centralized control considering system-wide/application-wide optimization objectives which results in extraneous and irrelevant data processing and inferior system/application performance [54]. The enablement of decentralized optimization strategies using blockchain opens a new window of research and development opportunities. The decentralized optimization leads to increased system performance by processing highly relevant data. The decentralized optimization is also beneficial when multiple strategies with different optimization objectives need to be run simultaneously across applications and systems.

3) PLANNING

AI applications and systems execute planning strategies in order to collaborate with other applications and systems and solve complex problems in new environments. Planning strategies help in operational efficiency and resilience of AI applications and systems by taking current input state and executing different logic and rule-based algorithms to reach predefined goals [55]. Currently, the centralized planning is complicated and time consuming task; therefore, blockchain based decentralized AI planning strategies are needed to offer more robust strategies with permanent tracking and provenance history. The blockchain is also useful for devising critical and immutable plans for strategic applications and mission critical systems.

4) KNOWLEDGE DISCOVERY AND KNOWLEDGE MANAGEMENT

Modern AI applications handle large amounts of data streams and require support for centralized big data processing systems. The centralized knowledge discovery and knowledge

management benefits the provisioning of application-wide and system-wide intelligence, however, the applications enable customized knowledge patterns for specific groups of users, applications, devices, and systems [56]. The decentralization of knowledge discovery processes and decentralized knowledge management is envisaged to provide personalized knowledge patterns considering the needs of all stakeholders in the system. In addition, the blockchain technologies can facilitate in secure and traceable knowledge transfer among different stakeholders in AI applications and systems.

5) PERCEPTION

Intelligent agents and bots in AI applications and systems continuously collect, interpret, select, and organize data from their ambient environments using centralized perception strategies which results in monolithic data collection [57]. The decentralized perception strategies can facilitate the collection of data from different views. The blockchain based decentralization facilitates tracing the perception trajectories, secure transfer of collected data, and immutable data storage. The decentralized perception strategies are useful because the applications and systems do not need to collect the data streams for successful and high quality perceptions repeatedly. Considering the permanent nature of blockchain, only the footprints of successful perceptions should be stored on blockchain.

6) LEARNING

The learning algorithms stay at the heart of AI applications in order to enable automation and knowledge discovery processes. Learning algorithms vary in terms of supervised, unsupervised, semi-supervised, ensemble, reinforcement, transfer, and deep learning models. These learning models solve different machine learning problems from classification to clustering and regression analysis to frequent pattern mining. Conventional learning models are trained and deployed using centralized infrastructure to achieve global intelligence. The decentralized learning models can help in achieving highly distributed and autonomous learning systems that support fully coordinated local intelligence across all verticals in modern AI systems [58], [59]. In addition, the blockchain enables immutable and highly secure versioning of learning models by maintaining provenance and historical aspects of data. However, considering the permanent nature of smart contracts, learning models need to be trained and tested well prior to deployment on blockchain.

7) SEARCH

AI applications need to operate in large and sparse search spaces (*i.e.,* big datasets or multivariable high dimensional datastreams); therefore, efficient search strategies become the essence of AI technologies. The search strategies are designed by considering different factors such as completeness, complexity (*i.e.,* time and space), and optimality. These strategies generally operate on nonlinear data structures such as trees and graphs whereby the algorithms start their expansion from an initial state and gradually expand until finding the required variable or completing the traversals in whole search spaces. Normally, search strategies are implemented using large-scale centralized and distributed infrastructure in order to maximize the operational efficiency [60]. However, their implementation using decentralized infrastructure needs careful investigation. It is envisaged that instead of deploying core search strategies, blockchains and decentralized infrastructure should be used to permanently and securely store successful search traces and traversal paths which could provide optimal search solutions of similar operations in the future.

8) REASONING

Logic programming is an essential component of AI applications that allows to develop inductive or deductive reasoning rules to reach decisions. The centralized reasoning in AI applications leads toward generalized global behavior across all application components [61]. To handle this issue, blockchain based distributed reasoning strategies are envisaged to facilitate the development of personalized reasoning strategies which could be more beneficial during perception, learning, and model deployment. In addition, smart contract based decentralized distributed reasoning on blockchain ensures the availability of unforgettable reasoning processes which may help in future executions of similar reasoning strategies.

B. DECENTRALIZED AI OPERATIONS

AI Applications generally handle large amounts of data for better and versatile decision making. However, centralized data storage using clouds, data centers, and clusters, becomes a major bottleneck for developing highly secure and privacy preserving AI applications. In addition, learning model development and deployment become tedious in some situations. Table 3 shows comparisons of some recent blockchain implementations that could potentially be adopted for AI applications.

1) DECENTRALIZED STORAGE

The centralized data storage becomes highly susceptible in terms of privacy and security when it involves personal and sensitive data about users, locations, activities, health records, and financial information. In addition, large-scale data collection exposes the scaling and capacity related issues of centralized infrastructure where AI applications need to process, transform, and store big datasets. Blockchain-based decentralized storage infrastructure facilitate in cryptographically secure data storage across the participating networks [38], [62]–[64]. In these systems, each node keeps a client-centric (a client could be a user, application, or node performing transactions on the blockchain) publicly encrypted copy of whole database in order to ensure data availability for desired clients. The respective clients can mine and use their own data whenever needed.

TABLE 3. Key features and benefits of blockchain platforms.

Platform	Type	Architecture	PL	SC	DD	CD	Scalable	DS	DM
Achain [70]	Public	Parallel Chain	Glua	✔	✔	✗	✔	✗	✗
Ardor [71]	Public, Consortium	Parent-child Chain	Java	✔	✔	✔	✔	✔	✗
Azure Blockchain Workbench [72]	Consortium	BaaS	Java Script, Solidity	✔	✔	✔	✔	✔	✗
Bitcoin [4]	Public	Single Chain	C++	-	✔	✗	✗	✗	✗
Blocko CoinStack [73]	Private	Single Chain	Java, Node.js, Rest API	✔	✔	✔	✗	✗	✗
Chain Core [74]	Private, Consortium	Single Chain	Java, Node.js, Ruby	✔	✔	✔	✗	✗	✗
ChainKit by Pencil Data [75]	Private, Public	BaaS	API	✗	✗	✗	✔	✗	✗
Corda [76]	Open Source	Single Chain	Java	✔	✔	✔	✔	✔	✗
Credits [77]	Public	Single Chain	Java	✔	✔	✔	✔	✔	✗
Elements [78]	Open Source	Sidechain	Python, C#	✗	✔	✗	✔	✔	✗
Eos.io [79]	Open Source	Single Chain	C++	✔	✔	✔	✔	✗	✗
Ethereum [11]	Public, Open Source	Single Chain	Solidity	✔	✔	✔	✔	✔	✗
HydraChain [80]	Private, Consortium	Parallel Chain	Python	✔	✔	✔	✔	✔	✗
Hyperleadger [81]	Private, Consortium	Single Chain	C++, Solidity	✔	✔	✔	✔	✔	✗
IOTA Tangle [82]	Public	Direct Acyclic Graph	Python, Node.js	-	-	-	✔	✗	✗
Multichain [83]	Private	Main chain, Off-chain	C++, API	✔	✔	✗	✔	✔	✔
Nxt Blockchain [71]	Public, Consortium	Single Chain	Java	✔	✔	✗	✔	✔	✔
Quorum [84]	Private, Consortium	Single Chain	-	✔	✔	-	✗	✗	✗
SAP Leonardo [85]	Private, Consortium	BaaS	Java	✔	✔	✗	✔	✔	✔
Stratis [86]	Private, Consortium	Main Chain, Sidechain	C#	✔	✔	✔	✔	-	-

Sharding and Swarming are core solutions for decentralized storage [65]–[67]. Sharding is the process of creating logical partitions of databases whereby each partition is assigned a unique key which is used to access it. The shards are further grouped together and their collected storage is supported by a group of nodes in the network in the form of swarms. Swarms reduce latency in AI applications by enabling parallel data access from multiple nodes in the network. In addition, scalability and reliability of storage increases because of geographically distributed multiparty decentralized storage systems. A few emerging decentralized data storage systems include Storj, Swarm, Sia, FileCoin, and IPFS which are further reviewed later in Section IV-A.

2) DATA MANAGEMENT

In addition to efficient decentralized storage, AI applications need to manage the data such that highly relevant, accurate, and complete datasets are collected from reliable data sources. Traditionally, AI applications run centralized data management schemes which execute across all the nodes in the underlying network [68]. These strategies include data filtration, data segmentation, context-aware data storage and routing in underlying networks, temporal data management and intelligent data management schemes. Considering decentralized storage networks and immutability constraints in blockchains, centralized data management becomes hugely inefficient because it will not only increase data duplication in case of minor changes in the data but it will also need to transfer similar datasets repeatedly. In case of big datasets, this massive data transfer will lead toward quick bandwidth overloading and increased backhaul network traffic; therefore, decentralized data management becomes essential for blockchain based AI applications. The decentralized data management schemes are envisaged to be deployed at node levels in the network considering temporal and spatial attributes in the data. In addition, the decentralized data management schemes can put the metadata on the blockchain in order to maintain security and provenance of the data. The actual data could be stored in traditional large-scale storage systems such as cloud data centers and clusters. In the case of client-centric small datasets, the metadata and actual data are stored on the blockchain and data are managed across

the network using token-based incentives for nodes storing different shards or participating in the swarms.

3) LEARNING MODEL DEVELOPMENT

Learning plays key role in AI applications to understand the environment from current data and perform informed decision making based on new data. Normally, learning models are trained and tested before actual deployment in the real systems. The centralized training is costly because the models need to learn from the whole datasets and tend to be prone to overfitting (*i.e.*, produce outputs based on memorized data), however, modern AI applications need to handle continuously evolving data streams. The decentralization of learning model development process is a feasible approach in order to develop resource-efficient learning models for client applications [58]. Decentralized learning algorithms take the input datasets from relevant swarms and shards and produce highly personalized learning models for each client. In addition, blockchain technologies can facilitate the maintenance of provenance of data as well as immutable history of learning models which may evolve over a certain period of time. Further the decentralized learning models could become benchmark for similar clients in the blockchain network where the users do not need to train the model from scratch, rather, they can incrementally build their own models by tuning and training new models. Once trained efficiently, the learning models could be tested using multiple smart contracts in decentralized applications.

4) MODEL DEPLOYMENT

The real performance of a trained model is assessed after deployment in production environments. However, the model deployment is a frequent and iterative process whereby developers need to continuously improve the models and correct the biases (*i.e.*, producing a specific set of decisions by ignoring rest of possible decisions) in order to produce highly effective and informed decisions. The model deployment in centralized systems is a straightforward iterative process, however, it becomes challenging when deployed in decentralized systems [69]. Smart contract based model deployment addresses these challenges by permanently recording the changes and maintaining the immutable versioning of different models. In addition, model sharing between different AI applications becomes secure and more trustworthy since the developers can track the provenance and all footprints of any specific version of a model.

C. BLOCKCHAIN TYPES FOR AI APPLICATIONS

Blockchain technologies are categorized as permissioned (*i.e.,* only authorized users can access the blockchain applications in private, consortium, or cloud based settings) or permissionless (*i.e.,* publicly accessible for all users via the Internet) systems.

1) PUBLIC

Public blockchains are known to be permissionless systems where users can download the blockchain code into their own systems, modify it, and use it according to their own requirements [4], [11]. In addition, public blockchains are easily accessible and open for read and write operations by all participants on the network. Due to their openness, user identities and transactional privacy information on these blockchain are managed using anonymous and pseudonymous data on the network. Also, these public blockchains use complex protocols for security and consensus mechanisms. The asset and data transfer at these blockchains use native tokens (*i.e.,* cryptocurrencies or value pointers) for each public blockchain. Public blockchains are widely adopted due to their massive decentralization and openness, however, the participants (*i.e.,* users/validators) on these blockchains are always unidentified. Hence, these blockchains are always prone to malicious security attacks which can result in massive value and data theft. Public blockchains need consensus of at least 51% validators and use complex mathematics to break security codes which result in large energy consumption and are also prone to attack in case the attackers gain control on 51% validators on the network. The transaction approval time on public blockchains is relatively longer when compared with private and consortium blockchains. Typically, a transaction on public blockchain is approved in 10 minutes or more but this approval time depends on the number of participants on the network and the mathematical complexity of employed consensus algorithms.

2) PRIVATE

A private blockchain is managed by a single organization. Unlike public blockchains, the private blockchains are designed as permissioned systems where users and participants in the systems are pre-approved for read/write operations and are always known within the network [87]. Private blockchains are comparatively faster due to known identities of validators and pre-approved participants in the network; therefore, it requires less complex mathematical operations to validate transactions on the network. In addition, private blockchains can transfer any kind of indigenous data, values, and assets within the network. The approval of transactions and asset transfers are managed using voting or multiparty consensus algorithms which consume low energy and enable fast transactions. The transaction approval time on private blockchains usually remains lower than one second.

3) CONSORTIUM

Consortium blockchains (also known as federated blockchains) are operated by a group of organizations. The groups are usually formed based on the mutual interests of participating organizations [88]. Different groups such as banks, governmental organizations, and private blockchain companies offer different types of federated blockchains. Like private blockchains, consortium blockchains operate as

permissioned systems, however, few participants can perform both read and write operations on the blockchain. Usually, all the participants on the network can read the data on the blockchain, however, a few authorized and trusted users can write the data on the blockchain. The consortium blockchains are comparatively faster than public blockchains because the participants are always pre-approved with known identities. In addition, these blockchains consume less energy because of voting based or multiparty approval based consensus protocols. A typical transaction on federated blockchains gets approval within one second.

4) BLOCKCHAIN-AS-A-SERVICE (BaaS)

Cloud service providers are focusing on blockchain technologies due to massive adoption and acceptance by governments and large enterprises. Major cloud vendors like Microsoft, Amazon, and IBM are enabling their environments to develop and test blockchain services for their customers [89], [90]. The emergence of BaaS is envisaged to benefit both private and consortium blockchain companies whereby their major focus remains on value addition through application development, testing, and deployment without considering underlying network, storage, and computational infrastructure. The enablement of BaaS not only leads toward new cross-industry public-private consortia but it also helps in leveraging new business opportunities and business-customer interaction models. Developers are also empowered with single-click provisioning of BaaS services in order to write the smart contracts. Since the major cloud vendors already offer a large plethora of cloud services for AI applications, the integration of BaaS with AI services is opening a new world of opportunities for application developers.

D. DECENTRALIZED INFRASTRUCTURE FOR AI APPLICATIONS

Traditionally blockchain architectures were designed as linear infrastructure based on the combination of linked list data structures and hashing strategies. However, nonlinear infrastructure based on graph theory and queuing information models are also emerging to cater the needs of real-time applications and handle big data.

1) LINEAR INFRASTRUCTURE

The single chain based blockchain architectures grow linearly whereby new blocks are appended at the end of the chain. Early decentralized systems operate on single chains, however, these systems have multiple issues. Single chains scale up slowly and compromise the real-time performance of decentralized applications [4], [11]. In addition, separate single chains are required for each business scenario therefore value, information, and asset exchange in multiple chains is impossible. Single chain blockchains for AI applications can be used for single task AI applications performing search, optimization, and learning, or operating autonomously in homogeneous environments. Single chain based blockchains could be more useful when, instead of executing the AI applications using smart contracts, only the performance histories need to be stored permanently. For example, how a deep learning model is producing accurate results when applied to the diagnosis of liver cancer in radiology applications. Another example could be the successful search footprints of remote industrial robots. Since AI applications usually operate in unconstrained environments therefore putting whole AI application components on blockchain is not a feasible choice.

2) NONLINEAR INFRASTRUCTURE

Nonlinear blockchain architectures are implemented in the form of multichain architectures whereby blockchain topologies are used in the form of parent-child chains, main-side chains, and parallel chains [91]. The multi-chain architectures are not only scalable for real-time performance but also support diverse business scenarios and cross-chain value transfers. In multi-chain architecture one or more chains keep information about other chains and serve(s) as main chain. Rest of the chains serve as side, child, or parallel chains. The child and side chains normally operate similarly, however, in child chains, the business scenarios are tightly linked with parent chains but side chains can totally operate independently from main chains. The parallel chains operate independently from other chains. The value transfer between different chains is performed using ''pegging'' approach where a two-way peg process is executed for bidirectional value transfer at a fixed exchange rate between chains. The exchange value is represented by native coins or tokens in the blockchain. The detailed discussion on nonlinear blockchains is presented in following studies for interested readers [71]. Nonlinear blockchains for AI applications facilitate the execution of multiple interrelated or independent AI tasks in the decentralized applications. In addition, the scalability features allow to execute AI applications in both development and deployment phases in parallel. AI components in production environment are deployed on the main/parent chain while the training and testing applications are deployed on the testnets or side chains. Nonlinear architectures also benefit emerging applications such as those using reinforcement and adaptive learning algorithms where the main applications need to continuously update their performance by retraining the learning models. In this case, learning models are developed on side chains and deployed on main chains.

E. THE ROLE OF CONSENSUS PROTOCOLS FOR AI APPLICATIONS

This subsection presents common consensus protocols and how they can impact the performance of AI applications on blockchain. Table 4 shows different implementations of these protocols.

1) PROOF OR WORK (PoW)

PoW is the pioneer consensus protocol proposed by Satoshi Nakamoto, an anonymous founder of cryptoccurency and decentralized distributed ledger technologies. Popular public

TABLE 4. Consensus protocols used by blockchain platforms.

Platform	PoW	PoS	BFT	PoAc	PoB	PoET	PoC	PoA	PoI
Achain [70]	✔	✔	✔	✗	✗	✗	✗	✗	✗
Alfa-Enzo [97]	✗	✗	✗	✔	✗	✗	✗	✗	✗
Ardor [71]	✗	✔	✗	✗	✗	✗	✗	✗	✗
Azure Blockchain Workbench [72]	✗	✗	✗	✗	✗	✗	✗	✔	✗
Bitcoin [4]	✔	✗	✗	✗	✗	✗	✗	✗	✗
Blocko CoinStack [73]	✔	✗	✗	✗	✗	✗	✗	✗	✗
BurstCoin [98]	✗	✗	✗	✗	✗	✗	✔	✗	✗
Chain Core [74]	✗	✗	✗	✗	✗	✗	✗	✔	✗
ChainKit by Pencil Data [75]	✔	✗	✗	✗	✗	✗	✗	✗	✗
Corda [76]	✗	✗	✔	✗	✗	✗	✗	✗	✗
Credits [77]	✗	✔	✔	✗	✗	✗	✗	✗	✗
Eos.io [79]	✗	✔	✔	✗	✗	✗	✗	✗	✗
Ethereum [11]	✔	✔	✗	✗	✗	✗	✗	✗	✗
HydraChain [80]	✗	✗	✔	✗	✗	✗	✗	✗	✔
Hyperledger [81]	✗	✗	✔	✗	✗	✔	✗	✗	✗
IOTA Tangle [82]	✔	✗	✗	✗	✗	✗	✗	✗	✗
Multichain [83]	✔	✗	✗	✗	✗	✗	✗	✗	✗
NEM [99]	✗	✗	✗	✗	✗	✗	✗	✗	✔
Nxt Blockchain [71]	✗	✔	✗	✗	✗	✗	✗	✗	✗
Quorum [84]	✗	✔	✔	✗	✗	✗	✗	✗	✗
SAP Leonardo [85]	✔	✗	✔	✗	✗	✔	✗	✗	✗
SlimCoin [94]	✗	✗	✗	✗	✔	✗	✗	✗	✗
Stratis [86]	✔	✔	✗	✗	✗	✗	✗	✗	✗

blockchain systems, such as Bitcoin and Ethereum, validate transactions after participation of at least 51% nodes on the underlying network using PoW consensus protocol [4], [11]. Since the validating nodes operate anonymously and in large quantity, these nodes need to mine the blocks by solving a complex and random mathematical problem and break the hash code to read the transactions on the blockchain. The successful nodes transmit the solution on peer-to-peer network to receive the rewards. New transactions and data are permanently added to the blockchain when 51% nodes on the network successfully solve the mathematical problem. Although PoW proved to be highly adopted consensus protocol, in large networks it consumes gigantic amount of energy and increases delay in transaction approvals. AI applications have high frequency of write operations because the intelligent algorithms continuously update the decision structures for informed decisions. Therefore, PoW protocols become performance bottleneck in real-time AI applications. In addition, 51% attack on the underlying network can compromise the security of AI applications.

2) PROOF OF STAKE (PoS)

PoS based consensus protocols solve the high energy consumption issue of PoW [92]. The PoS protocols work by defining big stakeholders on the blockchain network and allowing them to create new blocks. These protocols select the validators based on different criteria (*i.e.,* random validators, delegated validators, high frequency transacting validators, or validators holding coins for longer period). PoS proved to be energy-efficient when compared with PoW and it also indirectly solves the security problem by stopping the anonymous validators and allowing only those validators who own the native currency of the blockchains. However, the validators have nothing to lose on the blockchain if they do not validate the transactions; therefore, it may cause delay while creating new blocks. PoS could be useful for delay-tolerant AI applications but these protocols are not suitable when AI applications need to handle streaming data, detect changes, and performed real-time informed decisions.

3) BYZANTINE FAULT TOLERANCE (BFT)

BFT is the majority voting algorithm that rules out validations from malicious nodes on the blockchain network [81]. The malicious nodes are already part of the blockchain but contain malicious intent code that can directly/indirectly lead to incorrect validations and corrupt the data stored on the blockchain. Since all nodes are part of blockchain networks, it becomes challenging for BFT protocol to find these malicious nodes. Although its implementation is difficult, BFT algorithms are historically used in critical systems such as airplane engine systems, large-scale sensory systems, and nuclear systems. Different variants of BFT protocols are used. Simple BFT handles fault tolerance as long as at least two-third non-faulty nodes are present on the network. Other BFT algorithms handle the fault tolerance by enforcing digital signatures and restricting communications between peer nodes on the network. Considering successful implementations of BFT algorithms in critical systems, BFT based consensus could become handy for AI applications.

4) PROOF OF ACTIVITY (PoAc)

The PoAc protocol is a hybrid of PoW and PoS. This protocol initially works on empty blockchains using PoW algorithm and solves the 51% attack problem [93].

Initially, PoAc protocol solves complex mathematical problems and the validators start receiving the rewards which increases their stake on blockchains. The protocol then enables PoS algorithm for validators having acceptable stake on the blockchain. PoAc has been proven to be efficient in terms of security, storage, and network communication. Therefore, it could become handy for AI applications requiring less data availability and more security.

5) PROOF OF BURN (PoB)

The PoB protocol allows the validators only if they spend their coins by sending to a public, verifiable, unspendable, and invalid address. Once the users burn their coins, they are immediately allowed to create new blocks and get rewarded [94]. PoB benefits the users by allowing them to invest initially and create their stake on the blockchain and become authorized validators. It also solves the energy consumption problem of PoW. In addition, coin burning strategy reduces the number of coins on the blockchain; therefore, coin value increases gradually. Coin burning also benefits in balancing the number of coins on the blockchain, spending unsold coins, and paying for transaction fees on the network. AI applications can harness PoB protocols if they want to incentivize the users in order to maintain the value of underlying decisions. For example, the applications which need to maintain a specific level of accuracy, a certain number of clusters, or minimum number of objects to be found, can burn the learning models and search trees in order to maintain the value across the blockchain.

6) PROOF OF ELAPSED TIME (PoET)

Instead of engaging all users in the validation process, PoET protocols find a leader who can create new blocks on the chain. A PoET protocol works by associating a random timer with each node on the network and the node with minimum expiry is selected as the leader [95]. The leader node creates the new blocks and transmits its signature to the whole network. A PoET protocol continuously executes the random leader selection algorithm and finds new leaders all the time. It also enables to find malicious users in case the same nodes are selected as leaders or the minimum timer value is frequently assigned to specific nodes. PoET solves the energy consumption problem of PoW but due to random timer assignment, AI applications could become slow since the system needs to wait until the expiry of time. PoET could be useful when used with delay-tolerant applications.

7) PROOF OF CAPACITY (PoC)

Traditional PoW algorithms become computationally intensive because they need to find random nonce values in order to unlock the blocks. The PoC protocol, also known as proof of space, works as an alternative protocol by discovering the hard drive space on the nodes of the blockchain network [96]. Instead of random generation, it stores all possible nonce values on hard drive and finds the matching nonce-hash pairs to unlock the blocks. Using PoC, the nodes with large disk space get more stake with high probability.

8) PROOF OF AUTHORITY (PoA)

PoA solves high energy consumption issue of PoW. PoA protocols also solve the problem of dependency in PoS whereby validators must have monetary stake on the blockchain. A PoA protocol works by delegating authoritative control to specific nodes that collectively form the consensus based on majority votes to create new blocks on the network [100]. PoA is proved to be energy efficient and minimal delay consensus protocol but it is more suitable for private networks in order to delegate the validation authority to legitimate stakeholders. Therefore, blockchain implementers must consider legal identity of validators, a well-defined eligibility criteria to act as validator, and a universal eligibility criteria for all stakeholders to act as validators. Despite their energy efficiency and cost effectiveness, the security threats to PoA always remain high due to security attacks on validators who can potentially become a source of attack across the network. However, PoA could be used as an alternate consensus protocol for those AI applications that are deployed on private or consortium networks since all the validators are known across the system.

9) PROOF OF IMPORTANCE (PoI)

PoI protocols are similar to their PoA counterpart whereby validating nodes are ranked considering frequency of successful validations. The validators with high frequency get more importance on the blockchain and their approved transactions or blocks over-weigh other validators on the network because PoI sets the minimum threshold that must be met by nodes for successful validations [101]. Since the importance of validators is established considering their previous successful validations, a PoI protocol ensures high trust between participating nodes. Therefore, this protocol can be useful for AI applications on public blockchains. However, in private and consortium networks, PoI can lead to serious conflicts among stakeholders because important stakeholders can potentially monopolize the whole network.

Although we discussed the major implementations, a thorough study of literature reveals that there are many other consensus protocols that could be potentially used for AI applications. Since these studies are relevantly either new or not widely accepted yet, we do not discuss these works in this paper. Interested readers may explore Proof of Luck [102], Proof of Exercise [103], Proof of Ownership [104], Proof of Vote [105], and Proof of Retrievability [106] for further discussions on consensus protocols.

IV. BLOCKCHAIN-ENABLED AI APPLICATIONS

In this section, we describe works reported in the literature on how blockchain can be leveraged in AI to improve the reliability, security, transparency, trust, and management of data and algorithms in AI applications.

A. DECENTRALIZED DATA STORAGE AND MANAGEMENT WITH AI

The combination of AI and blockchain technologies has paved the way for many stable systems that support the interaction of multiple agents; therefore, providing an excellent platform for safe and secure data management, storage and transfer. Some of the key systems that utilize this combination are discussed in this subsection.

A decentralized, multiagent approach for vehicle routing in a large-scale dynamic environment is proposed in [107] and [108]. This approach is based on environment-centric coordination mechanism, inspired by ant colonies. The authors propose an approach where intelligent agents scrutinize the environment on behalf of vehicles and forecast a congestion. This anticipatory vehicle information is collected and distributed in a decentralized fashion. This approach fits the distributed nature of the traffic domain and ensures that scalability requirements are more easily met when compared to centralized systems. This approach can route vehicles more efficiently by using forecast information; thus, avoiding congested routes and providing better guidance in rerouting. Further, the experimental results of this decentralized approach indicate a performance improvement of 35% in terms of speed; therefore, helping drivers reach their destinations faster [107], [108]. The intelligent approach utilized by multiple agents in a decentralized environment guarantees to not only avoid existing congestions but also to prevent congestions in the near future.

The combination of AI and blockchain technology adds progressive value to biomedical research and healthcare sector [109]. The authors present a novel, decentralized model to assess the value of time and the combined value of personal data in an AI-moderated healthcare data exchange on the blockchain. An overview of AI and blockchain technologies is presented in this paper which may be used to accelerate biomedical analysis, improve predictive analysis techniques and empower patients with new tools to manage and control their own data and help them monetize their exclusive personal data with incentive benefits to undergo perpetual monitoring of their health. An AI-blockchain based system can dramatically simplify data acquisition. They allow the user to upload her/his data directly to the system and grants permission to use her/his data if it were bought through the system using transparent pricing formula determined by a data value model and it guarantees fair tracking of all data usage activities. Mamoshina *et al.* [109] discuss various promising machine learning techniques in practice and in development that include capsule networks, recursive cortical networks, and many other advances that are being made in symbolic learning and natural language processing. However, techniques such as transfer learning, recurrent neural networks, and generative adversarial networks are building up acceptance to be applied to the blockchain based decentralized personal data marketplaces.

The integrated features of these technologies can play a significant role in healthcare assistance too. Socially assistive robots can be employed in elderly care assistance as discussed in [110]. As there is an increasing demand for elder care and a shortage of professional caregivers, socially assistive robots are one of the most promising technologies that can act as a communication interface and identify the needs of the elderly or seriously ill patients. These robots aim to create a positive user experience, motivate the patients and to improve the quality of life by assisting the patients in regular exercise, reduce stress levels and for personal caregiving [110]. Though AI techniques are efficient classifying and analyzing large datasets in the healthcare sector with the availability of huge volumes of raw medical data from the sensors of connected IoT devices, there are severe issues of integrity in terms of data collection and storage [43]. Also, it is a jeopardy to trust a robotic agents' decision or activity in the medical field where all medical records need to be accurate and tamper-proof during a critical decision-making process. However, the combination of blockchain and AI technology could personalize medicine, quadrate treatments and health recommendations based on a patient's medical history, genetic lineage, stress levels, geography, atmospheric conditions, past medical conditions and aid in improving trust on robotic decisions. The information can be securely stored on a distributed, decentralized and immutable patient record, as well as a graph-based relationship database, can be formulated [43] for storing unstructured data and the relationships amongst the data. Figure 3 presents an outline of the combined features of AI and blockchain technologies for the medical field which include various stages such as diagnosis, analytics, critical decision making and validation of medical test reports, etc.

Machine learning algorithms can use the graph database to extract data, classify patterns and predict future prescriptions. Bayesian network, a graph database built on relationships of cause and effect, is an example of machine learning algorithms that use graph data to compute latent variables [43]. The vitality of a Bayesian network lies in its capability to regulate probabilities and predictions. When applied to health data, it can make effective predictions between unrelated data. The relationship of all entities in the healthcare graph database (such as physicians, specialists, medical researchers, drug manufacturers, patients, etc. and their activities which include treatment methods, prescriptions, and intake of drugs by patients) can be recorded on the immutable transaction log.

The importance of handling vast volumes of data, exponential increase in computing power, and tremendous growth in people's acceptance of connected applications and systems to register actions have become top priorities in AI and machine learning research [111]. Since artificial neural networks require large sets of data and high computing power for training purposes, a significant amount of resources to create powerful data centers to acquire large datasets have become essential [40], [112]. Woods [111] emphasizes the importance of combining AI techniques and blockchain infrastructure to tackle the security threats faced by the Internet, where bots-bots and human-bots interactions have increased, as 52% of

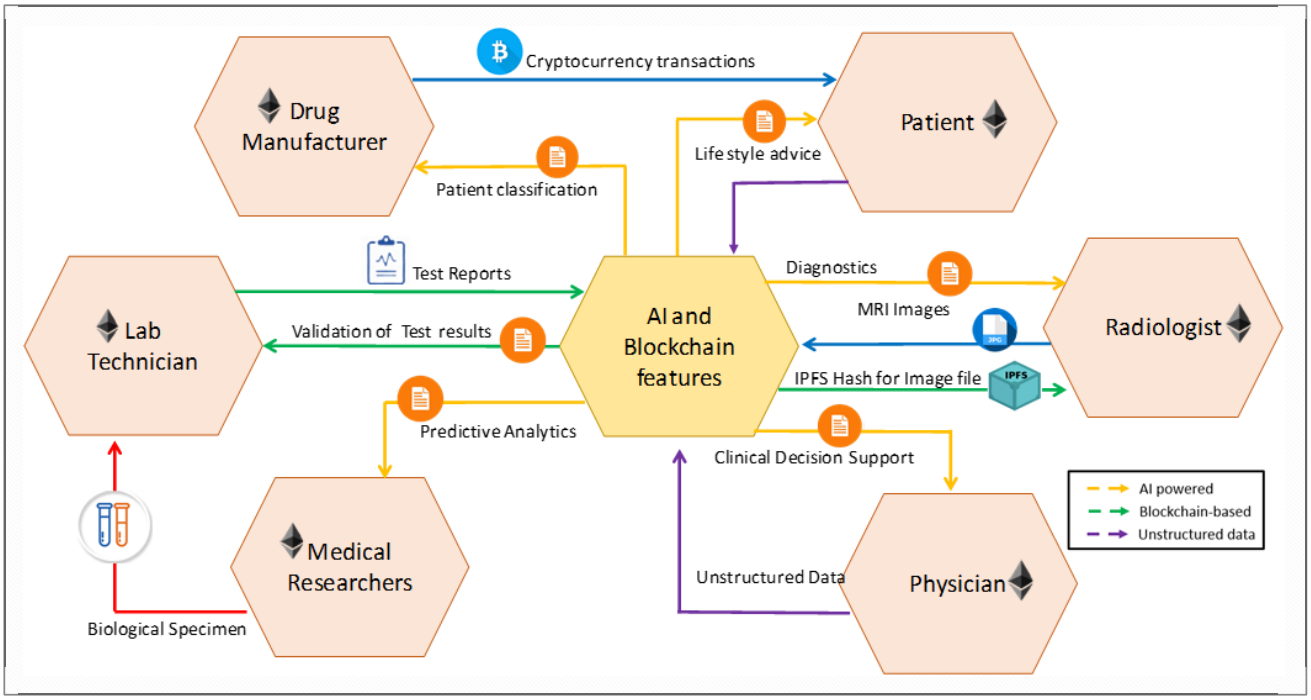


FIGURE 3. Collective intelligence for decentralized healthcare.

the web traffic is generated by bots. Due to increased bot traffic, it is estimated that in the near future the bot-bot communications will outpace the human-bot interactions. Bots will need to be able to query each other for identification and then look up the history of the data and ratings before interactions. During an audit process, the query information and data can be stored on blockchain and a higher level of transparency and security can be achieved [111]. The integration of blockchain and machine learning technologies is a stronger combination that provides an immutable, strong consensus mechanism, ultra-secure decentralized, self-sovereign identity which has the stupendous potential to rebalance and improve machine learning algorithms.

B. DECENTRALIZED INFRASTRUCTURE FOR AI

Blockchain infrastructure introduced three new characteristics to the traditional distributed architectures which include decentralized and shared control, immutable audit trails, and native asset exchanges [11]. Combined with AI techniques, this infrastructure provides users with qualitatively new data models, shared control of AI training data and models, and leads to improved trustworthiness on data. AI requires huge data, which is provided by blockchain, to produce better data models. This subsection discusses existing decentralized infrastructure and frameworks for AI applications.

An open source platform that incentivizes individuals to build a distributed and decentralized AI agents thereby creating a synergy between distributed AI and decentralized blockchain is carried out by ChainIntel [113]. ChainIntel is aimed to deploy and use AI models in decentralized applications (DApps). This platform aims to reinforce and consign the execution of AI models to various parts of the network, enabling scalable, robust and smart applications. ChainIntel is currently working to allow distributed AI model execution, where some parts of a deep neural network run on local devices and other parts run on a set of active nodes in the ChainIntel P2P network [113]. This work aims to incorporate various AI features into decentralized applications such as facial recognition, speech and image recognition, semantic analysis, disparity identification, smart homes, smart cities and countless more domains. Decentralized networks such as Ethereum and IPFS can handle the huge computational resources and data storage respectively, thereby providing a high level of privacy and tamper-proof records [44], [113]. This open-source decentralized AI platform aims to phase out monopolization of AI services provided by big companies in which the miner-nodes should be optimized to solve a huge number of matrix computations and directs it to be effectively decentralized.

The energy-based infrastructure can reap huge benediction by combining the AI and blockchain technologies and their features. Mylrea and Gourisetti [114] have explored how blockchain technology could possibly modernize and automate energy and IoT infrastructure toward a stable system. The author highlights how AI enabled blockchain solutions can assist in increasing cyber resilience and augmenting the exchange of energy resources in a distributed environment by using encryption techniques and by automating the transaction. Mylrea and Gourisetti [114] discuss how AI-enabled

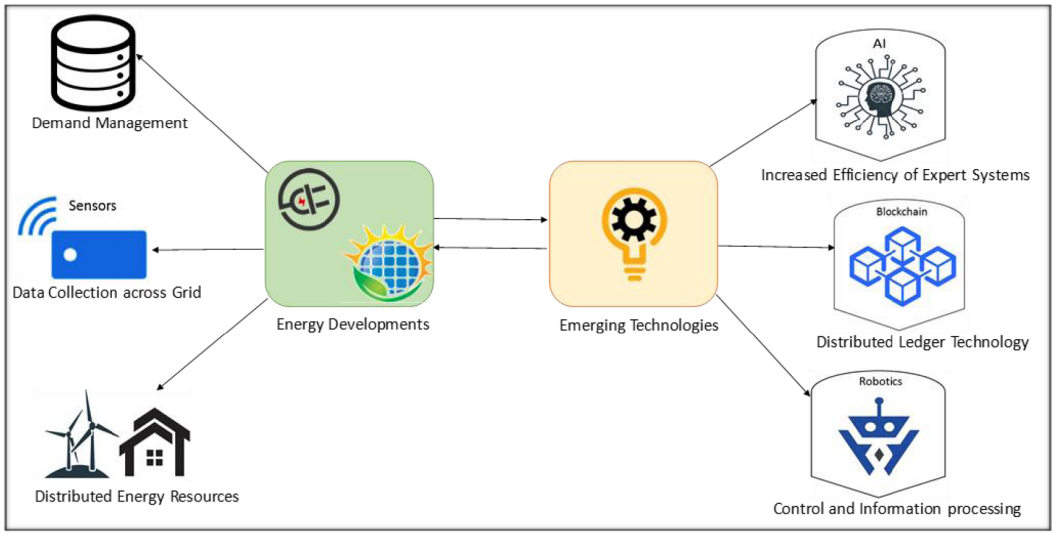


FIGURE 4. Future energy industry leveraging capabilities of blockchain and AI.

blockchain solutions can help to analyze huge datasets gathered from numerous platforms such as frequency and load changes, industrial control anomalies and frequency changes, and classify the datasets into weighted relationships, which can be tracked and automated with the help of blockchain technology. Artificial neural networks are being employed to analyze and understand the data patterns whereas blockchain based smart contracts can be exercised to secure the energy data and its transactions on the decentralized network.

An overall vision for transforming the energy market and utility industries with blockchain, robotics, and AI techniques is presented in Figure 4. A key-less signature blockchain infrastructure (KSBI) is highlighted in this work, as KSBI differs from PoW and retains integrity of original data and its ability to scale to industrial applications to add one trillion data items to the blockchain each second, and to verify the data item from the blockchain within the next second [114]. Optimization and security issues in the energy grid can be resolved and improved by blockchain by providing a verifiable distributed ledger which helps in improving transparency and integrity in the energy delivery sector [114]. If implemented successfully, this approach can replace traditional energy meters with a dynamic and decentralized distributed ledger. This disruptive combination may endow stakeholders and investors in renewable energy infrastructure with the power to vote, efficiently automate the energy-bidding auction, and monitor and deliver services based on the agreements made on smart contracts in a transparent and distributed environment [114]. Yu *et al.* [115] designed a high-performance blockchain platform for smart devices. This platform enables a stable connection between devices through the node-to-node mapping mechanism using technologies such as distributed network architecture, intelligent devices node mapping, as well as PBFT-DPOC consensus algorithm. Yu *et al.* [115] propose a new Delegated Proof of Contribution (DPOC) algorithm to facilitate any node to run as a Block Producer (BP). In this method, all the candidates need to contribute their own hardware infrastructure which includes computing power, storage, and bandwidth, such that all nodes take part in the voting process. The final ranking is determined by votes and miner's weight-sum seniority ranking. During this voting process, many super-nodes and substitute nodes are generated. The super-nodes reach consensus by generating blocks through the PBFT algorithm [115] and each block has the digital signature of remaining BP nodes. If a node is found to be dishonest or inactive in the network during the block verification process, it is blacklisted and replaced with a substitute node. This platform tested the transaction throughput and system delay of the intelligent device blockchain and compared it with the performance of public blockchains such as Bitcoin and Ethereum [115]. The experimental results showed that the intelligent device blockchain has higher transaction throughput and lower transaction latency than that of Bitcoin and Ethereum and provided higher efficiency.

C. DECENTRALIZED AI APPLICATIONS

Decentralized Intelligence and collective decision making can play the main role in identifying the malicious behavior of byzantine robots. Byzantine robots are those that exhibit malicious or faulty behavior arbitrarily in a swarm environment. Strobel *et al.* [46] propose a proof of concept for handling security issues in swarm robotic ecosystems using the blockchain technology. This approach utilizes the decentralized nature of smart contracts to build a secure swarm systematization mechanism to analyze and exclude the byzantine members from the swarm. This scheme was designed analogous to classical approaches and the behavior of robots is determined by a probabilistic finite state machine which consists of two phases *i.e.,* exploration state

and dissemination state [46]. Each robot in the swarm saves a copy of safety measurement on the blockchain for identifying byzantine robots.

The blockchain based approach creates a number of voting transactions sent by the robots to their neighbors in the swarm and all these votes get stored in the blockchain. This approach proved that a blockchain based swarm ecosystem preserves the integrity of the transactions and provides a direct interface for securely storing the record of events in a decentralized log [46]. This approach also demonstrated that the transactions can be verified even if some of the swarm members are lost or leave the swarm. In the blockchain based network, keys that are publicly available are the foremost available information for an agent to transfer information in a secure manner [114]. With respect to swarm robots, a robot can send information to a specific robot and only a robot that possesses a matching private key will be able to read the message; hence, the possibility of a data breach can be prevented. Digital cryptography of the blockchain ensures that the robots are allowed to use their private keys for encrypting a message. The other robots can then decrypt the message by using the public key of the sender [114]. Digital signature cryptography can ensure the information origin authentication and entity authentication between different robots in a swarm and improve the security during information exchanges.

An analysis of a decentralized intelligent transportation system with distributed intelligence based on classification techniques is discussed in [108]. Researchers conducted an exploratory study on a fully distributed architecture to enable cooperative sensing and management in an intelligent transportation system [108]. This proposed system envelops the process of capturing and managing the road data, thereby enabling services to improve the efficiency of transportation systems. The main contribution of this work comprises of two real-world scenarios related to the prediction of traffic data. The first one being able of detecting traffic congestions and the second one for predicting the pollution level using C4.5 classification technique.

The AI techniques embedded within the decentralized system help to predict and respond to critical incidents and events that may occur in a dynamic transportation environment and provide a befitting solution in a timely manner [108]. The reference architecture of the proposed system makes use of a data distribution platform and collaborative learning nodes connected through gateways to different subsystems to analyze the best traffic routes and to deal with congestion problems. In this work, the prediction of traffic congestion and other anomalies are performed using C4.5 classification technique which is used to generate decision trees from a set of training data a framework named 'KEEL' has been used for providing basic parametrization which is well known to handle continuous attribute value ranges, to prune the result decision trees, and to predict traffic congestion and pollution in a city. Osaba *et al.* [108] have performed the experiments based on real-world situations, with traffic congestion prediction in Lisbon, Portugal and the prediction of pollution in Pisa, Italy. A complete operation of this collaborative learning unit in a real scenario is showcased with a web application which was simulated in a laboratory.

Intelligent Precision farming can utilize the emerging technologies and decentralized business models to tackle the challenges faced by the agricultural sector. The lack of food security has affected 925 million people worldwide, including 42.2 million in the United States alone [116]. With the advent of applied science, IoT technology has gained acceptance across various industries. But due to the their constrained resources, underdeveloped standards, and absence of security in design and development of their software components, IoT devices remain insecure when connected in a distributed environment and abstain to provide a robust structure [117]. From an agricultural production perspective, IoT sensors, AI agents and blockchain technology can be conjointly implemented for crop/variety selection, irrigation method selection, reduce costs, predict yield, monitor crop health, improve yield, improve crop quality, predict input side demands and output aggregation needs leading to optimization of the supply chain and to enhance profits of all stakeholders involved in the agricultural production sector.

IoT sensors can be installed in farming fields to capture data and send information in order to optimize production. These IoT sensors can monitor the nutrient levels in soil and the images captured by sensors can help in monitoring the growth of crops periodically [116]. AI agents, on the other hand, can augment IoT devices to improve the agro-supply chain process via predictive analytics, which helps farmers to grow crops according to historical weather patterns in any specific region and monitor the crop growth with real-time data. Figure 5 shows the benefits and features of combining AI, IoT and blockchain technologies. Blockchain ensures that everyone involved in the network has access to all transactions; hence, reducing the time spent on logistics of agricultural commodity trading and also reducing food safety contingency [116]. An intelligent data-driven decision can assist farmers and stakeholders in making optimum decisions for farming plans to be customized for each farmer based on weather, soil, pest, and crop data on a real-time basis.

Another prominent field to benefit from bringing together blockchain technology and AI is the supply chain industry. When incorporated together, both these technologies have the potential to remodel the entire process into an 'autonomous' supply chain system [118]. Blockchain based research for supply chain industry concentrated on proof of concept experimental systems employing a decentralized application platform [118]. Most of the work in the literature was based on post supply chain management for the detection of counterfeited products as well as for the proof of delivery of these products that may involve multiple transporters. Applying AI techniques to the blockchain-based business transaction flows can assist to refine the supply chain by automating the entire process [118]. AI platforms, when consolidated with blockchain, can capture data from point of sale systems, history of purchase information, identify data patterns and

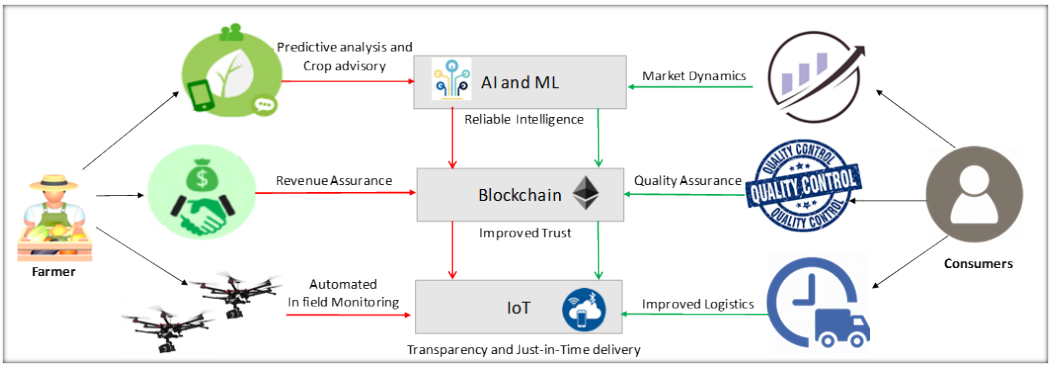


FIGURE 5. Intelligent precision farming with blockchain.

perform a predictive analysis which includes predicting future demand, predicting sales patterns, identifying potential issues in advance, optimizing routes to reach the destination, and handling network traffic.

When unified with blockchain technology and modern cryptography, federated learning can be used to improve the privacy of users' data by ensuring that data are never stored in the cloud [119]. Snips AIR is an AI-powered voice platform that takes advantage of blockchain technology to ensure that users' data are safe. While existing AI-powered voice assistants are pragmatic, there is a potential risk of placing the user's personal data at risk, as the conversations with the voice assistants are stored in the cloud. The technology behind Amazon Echo and Google Home is AI-powered and it stores the history of users' commands and conversations to respond in a smarter way for future commands [119]. Snips AIR ensures that all the personal details of a user remain well within the walls of connected homes instead of storing it on the cloud and that no one has the access to user's data. The environs of Snips incentivizes the users using tokens to store their encrypted data to its blockchain based system [119]. Further, the data are aggregated by application developers, as the AI training is done on the blockchain network following the concept of decentralized learning. Thereby, users need not have to reveal their personal data or trade-off their privacy. Snips AIR is aimed to be delivered by 2019 for consumers and it can be an alternative to Siri, an intelligent assistant that offers an easier way to get things done on IOS applications and stores the conversation data on the cloud [119] and assures that users' data are never at risk.

Robotic agents triggered by AI algorithms have been widely used to explore the deep seabed to find mineral resources, archeological findings or to access the underwater treasures in order to claim ownership or discovery rights by individuals or organizations. These algorithms and techniques assist the swarm to identify obstacles, gather and analyze information on ocean currents, and traverse via the most efficient path to reach the goal thereby saving energy. Ferrer [44] and Brambilla *et al.* [45] outline the nature of swarm robots to purview the objective and to record the key information about the discovery such as the location of the discovered object, time, date, etc. However, the swarm may not always be monitored. Any malicious attacker may gain access to freely observe and tamper with the emergent behavior of the swarm, as the swarm ecosystem is designed to expedite autonomously [120]. However, when swarm agents are powered with blockchain, it can record the discovery documents mechanized with cryptographic techniques such as hashing and time-stamping. The documents' hash can be included on the blockchain based smart contracts and the discovery report itself can be securely stored in a decentralized file system, such as the IPFS. Figure 6 shows how blockchain technology helps to secure the discovery report generated by ocean exploration robots on the IPFS and records its hash on the immutable smart contract. This hash will represent the exact content of the document and can be encoded into the decentralized network without the document's content being exposed [35], [44]. The hash of the document provides a secure, immutable and time stamped function about the recordings of various events during the discovery process and when a specific attestation took place following the consensus received from all active participants during a transaction in a particular time period. Proof of existence and Proof of discovery can be fortified by re-computing the hash and by comparing it with the original document hash stored in the blockchain based smart contract. This technique can be further explored to be implemented in various applications such as landmine detection, disaster relief missions, and military rescue operations which have precarious challenges for humans to work.

Unsupervised machine learning algorithms and techniques have been extensively used for medical image analysis to achieve a high level of accuracy [121]. This approach is proved to improve detection of nodules, classification, and sizing, while also reducing false-positive rates in abnormality detection [122]. However, cross-institutional sharing of sensitive medical data and records becomes a complex pursuit with the potential to improve the techniques for clinical effectiveness and patient's privacy [43], [123]. In a patient-clinic ecosystem, there is a primary need for developing a robust

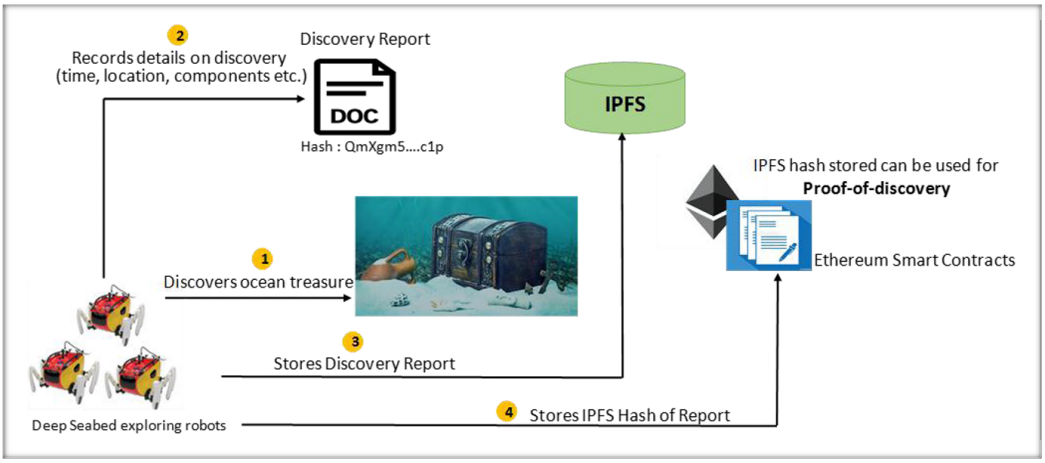


FIGURE 6. Blockhain-based unmanned intelligent ocean bed exploration.

system where data owners share their information in a secure environment and trust the decisions deduced by the AI agents. With the expeditious advancement in computational power and machine learning algorithms, blockchain technology can help facilitate a mechanism to compensate an AI service provider for the development and execution of novel machine learning algorithms [122].

Machine learning algorithms consume a considerable amount of time to diagnose a particular health condition by speculating on a radiology image or CT scan for instance. Peterson *et al.* [122] recommend that, by utilizing blockchain technology, the AI service provider can publish the diagnostic report images containing information about a single diagnostic service performed for a patient on the blockchain. Further, the AI service provider who develops the machine learning algorithms can be allowed to execute their algorithms over the images and publish the AI diagnosis output on the blockchain. By doing so, the radiologists at the clinic could compare his or her diagnoses with the result published on the blockchain [122]. The AI service providers can be incentivized only when the diagnosis results match with that of the diagnosis of the radiologists. As the service providers are incentivized for every accurate diagnosis, they are bound to improve the definiteness of their machine learning algorithms. Thereby, blockchain implements an invincible record of the complete diagnosis reports of both AI service providers and hospitals. AI techniques and deep learning algorithms extract high-level, complex abstractions as data representations through a hierarchical learning process [124], uses data sciences and analytics which can be used to deduce the next course of actions of the treatment by evaluating outcomes and blockchain can hold the record to improve healthcare services.

Recently, the banking industry has started investing in a wide range set of projects and start-ups providing blockchain based solutions as this technology provides a high level of safety for storing and transmitting data, distributed and transparent network infrastructure, decentralization and low cost of operations [125]. Banks have increased conducting tests of decentralized asset technology and implementing blockchain in the business process. As blockchain itself holds an immutable ledger that records all transactions in the chain, if a large number of transactions are being processed by the network, a huge volume of data gets collected and AI techniques can be used to process and classify the data. Telcoin [125] is a new cryptocurrency based on the Ethereum blockchain which will be distributed and accepted by telecom operators, enabling financial payments, remittances, credit, and various financial services on the blockchain. Telcoin suggests that the combined features of blockchain and machine learning can contribute to various applications like anticipating money laundering as AI is better in pattern classification and detection of irregularities in large amounts of data can be handled with blockchain technology. Figure 7 presents a model of AI and blockchain technology that can be used in the banking and finance institutions. Another remarkable outcome of combining both technologies is the handling of a fluctuating range of cryptocurrencies where AI techniques can help reduce the inherent volatility of cryptocurrencies [125]. Xiong *et al.* [126] developed a neural network model that harnesses the potential of deep learning financial time series in the presence of strong noise which proved that, with huge volumes of datasets, AI techniques perform better than other traditional models. Machine learning techniques can analyze the price and details of various stock exchanges and predict the future forecasts accurately and decentralized contracts can be used to freeze the price of currency for a fixed amount of time [125].

The property Management Sector has begun to explore and apprehend the collective potential of blockchain and AI [127]. These technologies can create boundaries by breaking the monopolistic power of firms and hotels using blockchain. Problems faced by the property management sector such as inventory management can be managed by blockchain

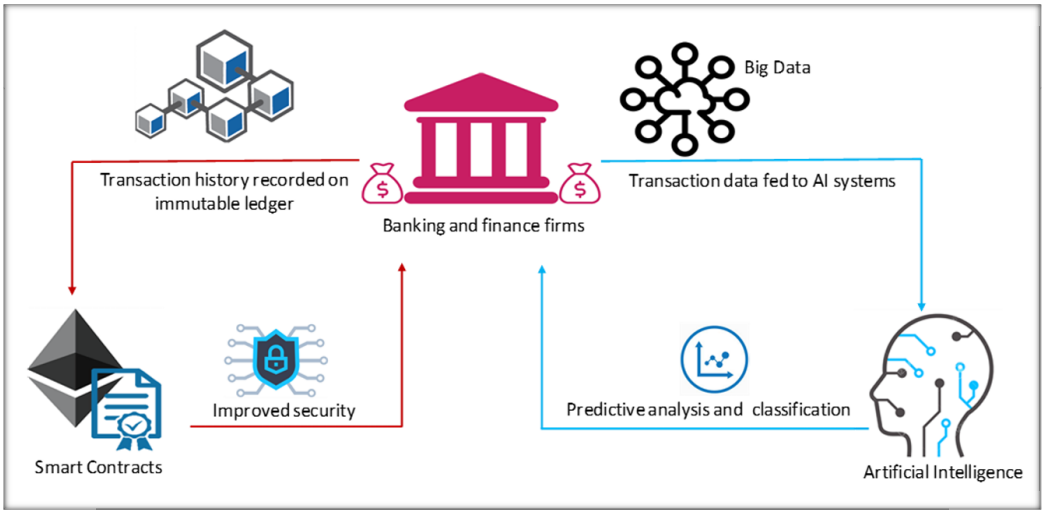


FIGURE 7. Combining AI and blockchain for banking and finance.

and details on bed stock and hotel capacity can be managed by learning techniques of AI. The Dutch land registry department is considering to consolidate AI and blockchain technology into the real estate industry [128]. The land registry department envisions that these new technologies when allied can improve the legal dependence and patronage of business to create a stable process. The Dutch government has already been involved in utilizing the revolutionary benefits of blockchain in various fields such as financing, supply chain, and logistics industry [129]. This organization now aims to implement the inherent benefits of combining both technologies where implementation of AI is aimed to constitute self-learning systems which can predict the outcome whilst blockchain technology can be used for handling and managing huge volumes of data resources saved and produced by the land registry department [128].

Another remarkable pursuit in the property sector is the acceptance of these technologies by the government of Singapore in a program called 'Smart Nation,' which attempts to diminish the paramountcy of sellers over investors and buyers [129]. This is an $73 million worth project that endows the private sectors to test all their new innovations and solutions which includes technology and building management in the real estate sector. With big data, property investors and developers can predict the trends of real estate and merchandise movements. AI techniques can be used for comparative market analysis which helps users to get a thorough knowledge of the investment and blockchain technology-based smart contracts can help in minimizing the transmission process and improving the transparency of payments, thereby saving millions of dollars for investors [129].

To this point, we discussed early implementations of decentralized AI applications in various sectors. However, persistent efforts are still needed in order to fully enable decentralized AI. Considering the limitations in current implementations and our vision of enabling fully decentralized AI applications and systems, in the next section we discuss the major open research challenges in this important research area.

V. OPEN RESEARCH CHALLENGES

In this section, we discuss and highlight to-date challenges for combining AI and blockchain technologies. Some of the foreseeable challenges related to the unification and integration of both technologies are listed below:

- **Privacy.** Public blockchain ledgers enable secure and authentic data processing, however, collected data are publically accessible and available for all readers. This can be a point of privacy evasion and concern. In addition, pervasive sensing systems in IoT continuously collect consumers' personal and sensitive data and putting this data on open ledgers could lead towards privacy issues. Using private blockchain ledgers, the data privacy could be ensured by enabling encryption and allowing controlled access of the ledgers. However, such private blockchain platforms will limit the access and exposure of the large amount of data that can be necessary for AI to process and preform accurate and correct decision making and analytics.
- **Scalability and Side Chains.** Scalability is one of the major concerns for today's blockchain platform. For cryptocurrency blockchain platforms, bitcoin blockchain can perform an average of 4 transactions per seconds, while Ethereum can perform an average of 12 transactions per second. Such performance is really unacceptable when compared with Facebook which handles millions of transactions every second including likes, posts, and comments. Side chains (known also as side channels) are used to accelerate the performance of blockchains, in which transactions are settled between parties in a quick manner outside the main chain, and settled only once per day on the main chain [91]. Many new emerging types of blockchains improve significantly the consensus algorithms of mining nodes.

For example, platforms like Algorand and IoTA can provide substantially better performance than that of Ethereum and Hyperledger blockchains [130], [131]. However, more work is still needed to improve the scalability to be comparable to that of Facebook and its likes.

- **Blockchain Security.** The decentralized power found in blockchain can suffer from abuses and misuses. Though blockchain provides robust schemes for securing IoT and predictive analysis, the blockchain systems are vulnerable to cyber-attacks as that of 51% attack [26]. The consensus mechanism depending upon the hashing power of the miner can be compromised, in which the decentralized platform becomes centralized around a few mining farms that control consensus and settlement finality. This security problem is more evident in public blockchains such as Ethereum and bitcoin. Private blockchain platforms suffer less from this problem, as consensus protocols are predefined among parties. Furthermore, the execution environment of the mining nodes is not protected, especially for private blockchain platforms with a few mining nodes as that of Hyperledger, in which the execution outcomes can be tampered with. To remedy this problem, newly emerging blockchain platforms are equipped with hardware to offer execution in a Trusted Execution Environments (TEEs), such as Intel SGX [132].
- **Smart Contracts Vulnerabilities and Deterministic Execution.** It is crucial to ensure that the implementation of a smart contract is free of bugs and vulnerabilities and secure against attacks. It is important to safeguard the code and the information on the network, as they may be vulnerable to attacks. For example, the smart contract for the DAO which was built on the Ethereum platform had serious code vulnerability and was hacked in 2016. This resulted in a loss of 3.6 million Ethers. There is a definite need for blockchain engineering, addressing this issue posed by smart contract programming and other applications running on blockchain [133]. The vulnerability issues are due to poor and negligent programming practices in the languages used to write the smart contracts code (as that of Solidity and Chaincode). Testing smart contracts for vulnerabilities has become of a critical importance, and some tools have been developed to assess the security state of a smart contract code [134]–[136]. Furthermore, as of today, the execution outcomes of smart contracts are all deterministic and cannot be probabilistic. This can pose a key challenge for decentralized AI in which AI and machine learning-based decision making algorithms get executed as smart contracts by the mining nodes, in which the execution outcome are not usually deterministic, but rather random, unpredictable and most often approximate. This entails a novel solution to deal with approximate computation and to devise consensus protocols for mining nodes for agreeing on results with a particular degree of certainty, accuracy, or precision, and with data input that might be highly fluctuating as that of IoT and sensory readings.
- **Trusted Oracles** Smart contracts are designed to be invoked by external events or outside functions invoked by blockchain participants. Smart contracts are not designed to automatically trigger events, or initiate retrieval of data on their own. In other words, the contracts cannot pull data from the outside world. Data and events have to be pushed to the contracts. To remedy such shortcomings, trusted oracles (which are basically trusted external parties or nodes) are being proposed as alternatives, and used to push events and data to the smart contracts. Oracles add a level of complexity and insecurity for ensuring and managing trust, in which a completely decentralized system becomes centralized around a group of oracles that must be trusted. Voting among trusted oracles is typically employed to reach consensus [137].
- **AI-specific Emerging Consensus Protocols.** Existing consensus protocols considers network and middleware layers of blockchain systems by enabling different proof of X protocols (as discussed in section III-E). A large plethora of research opportunities are available for future researchers to explore if the application level consensus protocols could be designed considering proofs based on quality of learning models, efficient search strategies, quality and provenance of data, and quality of optimization.
- **Fog Computing Paradigm.** Fog computing is a newly emerging computing paradigm that allows for localized computing and storage close to the source of data being generated by customers or IoT devices. Fog nodes are typically used to augment the long delay incurred by computing and storage at the cloud environment. Fog nodes can be thought of as a local small-scale cloud. In the context of AI and blockchain, future fog nodes have to be equipped with AI and machine learning capabilities as well as enabled with blockchain interface, whereby localized management, access, and control of data are performed by the fog nodes.
- **Lack of Standards, Interoperability, and Regulations.** To date, blockchain technology standards are yet to be devised. Work is in progress by IEEE, NIST, ITU, and many standards bodies to put forward standards for blockchain interoperability, governance, integration, and architecture [138], [139]. Moreover, at local and global level, governmental and institutional guidelines, rules, laws, regulations, and policies need to put in place for blockchain deployment, arbitration, and dispute handling, in the context of AI applications and especially for public blockchain transactions involving financing and automated payments using cryptocurrencies. This entails research directed at devising models and proof of concepts that can play a key role in defining the right set of technical standards for blockchain architectural models, services, deployment and interoperability.

- **Quantum Computing.** It is envisaged that future quantum computing will have the ability to break public key encryption in which private keys can be determined. Current blockchain relies on digital signatures which use public key encryption. Many experts believe that quantum computing may render the underlying security of blockchain breakable by the year 2027 [140], [141]. This entails serious research on quantum-safe and secure blockchain that withstand such breakability, and still guarantees high performance and scalability. Also this entails sound migration plans and interoperability with quantum-resilient blockchain platforms.
- **Governance.** Deploying, constructing, and managing a blockchain platform among different participants and stakeholders is a tedious task. Even with a private of consortium blockchain, serious issues arise related to the type of blockchain to deploy (*e.g.,* Hyperledger or Ethereum), who administers and troubleshoots the blockchain, the deployment location of the blockchain nodes, who writes the smart contracts, settlement of disputes, selection of trusted oracles, mechanisms for off-chain activities, deployment of side channels, regulations and standards to comply with, and many others. This entails research targeted at devising sound governance models.

VI. CONCLUSION

In this paper, we surveyed and reviewed the current state-of-the-art related to the use and applicability of blockchain features for AI. We gave an overview of blockchain and decentralized storage on how blockchain technology can enhance and solve key issues related to AI. Moreover, we presented a detailed taxonomic discussion and comparisons of common blockchain implementations in terms of decentralized AI operations, blockchain types and infrastructure, and consensus protocols. An extensive analysis of blockchain applications for intelligent multi-agent systems is reviewed with respect to decentralized data management and infrastructure for AI. Various features of AI for blockchain applications are also summarized. Our literature review shows that adopting blockchain for AI applications is still in its infancy, and there exists many research challenges to be addressed and tackled in areas related to privacy, smart contract security, trusted oracles, scalability, consensus protocols, standardization, interoperability, quantum computing resiliency, and governance.

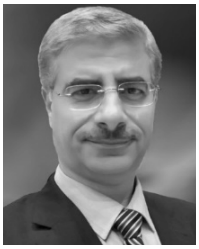
REFERENCES

[1] A. Maxmen, "Ai researchers embrace bitcoin technology to share medical data," *Nature*, vol. 555, pp. 293–294, Mar. 2018.
[2] Z. Baynham-Herd, "Enlist blockchain to boost conservation," *Nature*, vol. 548, no. 7669, p. 523, 2017.
[3] S. Ahmed and N. T. Broek, "Blockchain could boost food security," *Nature*, vol. 550, no. 7674, p. 43, 2017.
[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. Accessed: Jan. 10, 2019. [Online]. Available: https://archive.is/rMBtV
[5] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly Media, 2015.
[6] M. Koch, "Artificial intelligence is becoming natural," *Cell*, vol. 173, no. 3, pp. 531–533, 2018.
[7] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Netw.*, vol. 61, pp. 85–117, Jan. 2015.
[8] *Nebula Ai (NBAI)—Decentralized ai Blockchain Whitepaper*, Nebula AI Team, Montreal, QC, Canada, 2018.
[9] T. N. Dinh and M. T. Thai, "Ai and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, Sep. 2018.
[10] Y. Qi and J. Xiao, "Fintech: Ai powers financial services to improve people's lives," *Commun. ACM*, vol. 61, no. 11, pp. 65–69, 2018.
[11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.
[12] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas. (2016). "Communication-efficient learning of deep networks from decentralized data." [Online]. Available: https://arxiv.org/abs/1602.05629
[13] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, "An overview of smart contract: Architecture, applications, and future trends," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 108–113.
[14] X. Zheng, M. Zhu, Q. Li, C. Chen, and Y. Tan. (2018). "FinBrain: When finance meets ai 2.0." [Online]. Available: https://arxiv.org/abs/1808.08497
[15] T. Baltrušaitis, C. Ahuja, and L.-P. Morency, "Multimodal machine learning: A survey and taxonomy," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 41, no. 2, pp. 423–443, Feb. 2019, doi: 10.1109/TPAMI.2018.2798607.
[16] F. Fioretto, E. Pontelli, and W. Yeoh. (2016). "Distributed constraint optimization problems and applications: A survey." [Online]. Available: https://arxiv.org/abs/1602.06347
[17] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
[18] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[19] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. E2575, 2018.
[20] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[21] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surveys Tuts.*, to be published, doi: 10.1109/COMST.2018.2852480.
[22] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018.
[23] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, to be published, doi: 10.1109/COMST.2018.2863956.
[24] R. B. Uriarte and R. De Nicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 22–28, Sep. 2018.
[25] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.
[26] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, Aug. 2017, doi: 10.1016/j.future.2017.08.020.
[27] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[28] V. Lopes and L. A. Alexandre. (2018). "An overview of blockchain integration with robotics and artificial intelligence." [Online]. Available: https://arxiv.org/abs/1810.00329
[29] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.
[30] W. Samek, T. Wiegand, and K.-R. Müller. (2017). "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models." [Online]. Available: https://arxiv.org/abs/1708.08296
[31] M. Schluse, M. Priggemeyer, L. Atorf, and J. Rossmann, "Experimentable digital twins—Streamlining simulation-based systems engineering for industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1722–1731, Apr. 2018.

[32] M. Feurer, K. Eggensperger, S. Falkner, M. Lindauer, and F. Hutter, "Practical automated machine learning for the automl challenge 2018," in *Proc. Int. Workshop Autom. Mach. Learn. (ICML)*, 2018, pp. 1–12.
[33] C. Lv *et al.*, "Hybrid-learning-based classification and quantitative inference of driver braking intensity of an electrified vehicle," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5718–5729, Jul. 2018.
[34] P. Peng, Y. Tian, T. Xiang, Y. Wang, M. Pontil, and T. Huang, "Joint semantic and latent attribute modelling for cross-class transfer learning," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 7, pp. 1625–1638, Jul. 2018.
[35] J. Benet. (2014). "IPFS-content addressed, versioned, P2P file system." [Online]. Available: https://arxiv.org/abs/1407.3561
[36] J. H. Hartman, I. Murdock, and T. Spalink, "The swarm scalable storage system," in *Proc. 19th IEEE Int. Conf. Distrib. Comput. Syst.*, Jun. 1999, pp. 74–81.
[37] Protocol Labs. (2017). *Filecoin: A Decentralized Storage Network*. [Online]. Available: https://filecoin.io/filecoin.pdf
[38] T. McConaghy *et al.*, "BigchainDB: A scalable blockchain database," BigchainDB GmbH, Berlin, Germany, White Paper, 2016. Accessed: Jan. 10, 2019. [Online]. Available: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf
[39] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," The whitepaper is Storj Labs, Atlanta, GA, USA, Tech. Rep., 2014. Accessed: Jan. 10, 2019. [Online]. Available: https://storj.io/storj.pdf
[40] D. Marr, "Artificial intelligence—A personal view," *Artif. Intell.*, vol. 9, no. 1, pp. 37–48, 1977.
[41] T. Marwala and B. Xing. (2018). "Blockchain and artificial intelligence." [Online]. Available: https://arxiv.org/abs/1802.04451
[42] B. Marr. (2018). *Artificial Intelligence and Blockchain: 3 Major Benefits of Combining These Two Mega-Trends*. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/03/02/artificial-intelligence-and-blockchain-3-major-benefits-of-combining-these-two-mega-trends/
[43] D. Campbell. (2018). *Combining AI and Blockchain to Push Frontiers in Healthcare*. [Online]. Available: http://www.macadamian.com/2018/03/16/combining-ai-and-blockchain-in-healthcare
[44] E. C. Ferrer. (2016). "The blockchain: A new framework for robotic swarm systems." [Online]. Available: https://arxiv.org/abs/1608.00695
[45] M. Brambilla, E. Ferrante, M. Birattari, and M. Dorigo, "Swarm robotics: A review from the swarm engineering perspective," *Swarm Intell.*, vol. 7, no. 1, pp. 1–41, 2013.
[46] V. Strobel, E. C. Ferrer, and M. Dorigo, "Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario," in *Proc. 17th Int. Conf. Auto. Agents MultiAgent Syst.* International Foundation for Autonomous Agents and Multiagent Systems: Stockholm, Sweden, Jul. 2018, pp. 541–549.
[47] S. Janson, D. Merkle, and M. Middendorf, "A decentralization approach for swarm intelligence algorithms in networks applied to multi swarm PSO," *Int. J. Intell. Comput. Cybern.*, vol. 1, no. 1, pp. 25–45, 2008.
[48] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, 2017.
[49] D. Ye, M. Zhang, and A. V. Vasilakos, "A survey of self-organization mechanisms in multiagent systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 3, pp. 441–461, Mar. 2017.
[50] Y. Rizk, M. Awad, and E. W. Tunstel, "Decision making in multiagent systems: A survey," *IEEE Trans. Cogn. Develop. Syst.*, vol. 10, no. 3, pp. 514–529, Sep. 2018.
[51] F. Fioretto, E. Pontelli, and W. Yeoh, "Distributed constraint optimization problems and applications: A survey," *J. Artif. Intell. Res.*, vol. 61, pp. 623–698, Mar. 2018.
[52] M. H. U. Rehman, C. S. Liew, T. Y. Wah, and M. K. Khan, "Towards next-generation heterogeneous mobile data stream mining applications: Opportunities, challenges, and future research directions," *J. Netw. Comput. Appl.*, vol. 79, pp. 1–24, Feb. 2017.
[53] M. H. U. Rehman, A. Batool, C. S. Liew, Y.-W. Teh, and A. U. R. Khan, "Execution models for mobile data analytics," *IT Prof.*, vol. 19, no. 3, pp. 24–30, 2017.
[54] L. Bottou, F. E. Curtis, and J. Nocedal, "Optimization methods for large-scale machine learning," *SIAM Rev.*, vol. 60, no. 2, pp. 223–311, 2018.
[55] M. A. Contreras-Cruz, J. J. Lopez-Perez, and V. Ayala-Ramirez, "Distributed path planning for multi-robot teams based on artificial bee colony," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jun. 2017, pp. 541–548.
[56] S. J. van Zelst, B. F. van Dongen, and W. M. P. van der Aalst, "Event stream-based process discovery using abstract representations," *Knowl. Inf. Syst.*, vol. 54, no. 2, pp. 407–435, 2018.
[57] H. Lu, Y. Li, M. Chen, H. Kim, and S. Serikawa, "Brain intelligence: go beyond artificial intelligence," *Mobile Netw. Appl.*, vol. 23, no. 2, pp. 368–375, 2018.
[58] A. B. Kurtulmus and K. Daniel. (2018). "Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain." [Online]. Available: https://arxiv.org/abs/1802.10185
[59] H. Kim, J. Park, M. Bennis, and S.-L. Kim. (2018). "On-device federated learning via blockchain and its latency analysis." [Online]. Available: https://arxiv.org/abs/1808.03949
[60] M. Hatem, E. Burns, and W. Ruml, "Solving large problems with heuristic search: General-purpose parallel external-memory search," *J. Artif. Intell. Res.*, vol. 62, pp. 233–268, Jun. 2018.
[61] S. Banerjee, P. K. Singh, and J. Bajpai, "A comparative study on decision-making capability between human and artificial intelligence," in *Nature Inspired Computing*. Cham, Switzerland: Springer, 2018, pp. 203–210.
[62] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Secur. Workshop*, 2017, pp. 45–50.
[63] S. Ali, G. Wang, B. White, and R. L. Cottrell, "A blockchain-based decentralized data storage and access framework for PingER," in *Proc. 17th IEEE Int. Conf. On Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1303–1308.
[64] S. Cui, M. R. Asghar, and G. Russello, "Towards blockchain-based scalable and trustworthy file sharing," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul./Aug. 2018, pp. 1–2.
[65] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 17–30.
[66] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: Scaling blockchain via full sharding," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2018, pp. 931–948.
[67] K. R. Özyılmaz and A. Yurdakul. (2018). "Designing a blockchain-based IoT infrastructure with ethereum, swarm and LoRa." [Online]. Available: https://arxiv.org/abs/1809.07655
[68] H. T. Vo, A. Kundu, and M. K. Mohania, "Research directions in blockchain data management and analytics," in *Proc. EDBT*, 2018, pp. 445–448.
[69] L. Lai and N. Suda. (2018). "Rethinking machine learning development and deployment for edge devices." [Online]. Available: https://arxiv.org/abs/1806.07846
[70] T. Cui. (2018). *Achain Blockchain Whitepaper*. [Online]. Available: https://www.achain.com/documents/Whitepaper.pdf
[71] T. Jelurida. (2018). *Ardor, Scalable Blokchain, Proof of Stake Consensus*. [Online]. Available: https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf
[72] Microsoft. (2018). *Azure Blockchain Workbench Documentation*. [Online]. Available: https://docs.microsoft.com/en-us/azure/blockchain/workbench/
[73] *BLOCKO*. (2018). [Online]. Available: https://www.blocko.io/platform.html
[74] (2018). *Chain Core White Paper*. [Online]. Available: https://chain.com/docs/1.2/protocol/papers/whitepaper
[75] (2018). *PencilDATA*. [Online]. Available: https://pencildata.com/
[76] M. Hearn, "Corda: A distributed ledger," R3, New York, NY, USA, Tech. Rep. R3CEV, 2016.
[77] *Whitepaper, Decentralized Financial System Credits*, T. Credits, London, U.K., 2018.
[78] (2018). *Elements by Blockstream*. [Online]. Available: https://elementsproject.org/elements-code-tutorial/overview
[79] (2018). *EOSIO Technical White Paper*. [Online]. Available: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
[80] (2018). *Hydrachain a Permissioned Distributed Ledger Based on Ethereum*. [Online]. Available: https://github.com/HydraChain/hydrachain
[81] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSyst. Conf.*, 2018, p. 30.
[82] R. Alexander, *IOTA—Introduction to the Tangle Technology: Everything you Need to Know About the Revolutionary Blockchain Alternative*. Feb. 2018.

[83] G. Greenspan. (2018). *MultiChain Private Blockchain—White Paper*. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf
[84] T. Quorum. (2018). *Quorum Architecture*. [Online]. Available: https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum_Architecture_20171016.pdf
[85] (2018). *SAP Leonardo*. [Online]. Available: https://cloudplatform.sap.com/capabilities.html
[86] Tag: Stratis. (2018). *Stratis Blockchain White Paper*. [Online]. Available: https://stratisplatform.com/files/Stratis_Whitepaper.pdf
[87] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data*, 2017, pp. 1085–1100.
[88] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[89] D. Joshi, "IBM, Amazon & microsoft are offering their blockchain technology as a service," *Bus. Insider*, vol. 24, Oct. 2017. Accessed: Jan. 10, 2019. [Online]. Available: https://www.thewealthadvisor.com/article/ibm-amazon-microsoft-are-offering-their-blockchain-technology-service
[90] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, Nov./Dec. 2017.
[91] G.-H. Hwang, P.-H. Chen, C.-H. Lu, C. Chiu, H.-C. Lin, and A.-J. Jheng, "InfiniteChain: A multi-chain architecture with distributed auditing of sidechains for public blockchains," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2018, pp. 47–60.
[92] S. King and S. Nadal, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," Tech. Rep., Aug. 2012. Accessed: Jan. 10, 2019. [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper.pdf
[93] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, 2014.
[94] (2018). *Slimcoin|A Cryprocurrency for Long Time*. [Online]. Available: https://github.com/slimcoin-project/slimcoin-project.github.io/raw/master/whitepaperSLM.pdf
[95] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Proc. SSS*, 2017, pp. 282–297.
[96] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.
[97] (2018). *Alfa-Enzo White Paper*. [Online]. Available: https://www.alfaenzo.io/libs/pdf/whitepaper.pdf
[98] (2018). *Burstcoin Wiki White Paper*. [Online]. Available: https://burstwiki.org/wiki/Main_Page
[99] NEM. (2018). *NEM Technical Reference*. [Online]. Available: https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf
[100] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *Proc. ITASEC*, 2018, pp. 1–11. Accessed: Jan. 10, 2019. [Online]. Available: https://eprints.soton.ac.uk/id/eprint/415083
[101] (2018). *NEM—Distributed Ledger Technology (Blockchain)*. [Online]. Available: https://nem.io/
[102] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, 2016, p. 2.
[103] A. Shoker, "Sustainable blockchain through proof of exercise," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Oct./Nov. 2017, pp. 1–9.
[104] S. Dramé-Maigné, M. Laurent, L. Castillo, and H. Ganem, "Augmented chain of ownership: Configuring IoT devices with the help of the blockchain," in *Proc. 14th EAI Int. Conf. Secur. Privacy Commun. Netw. (SECURECOMM)*. Seattle, WA, USA: Springer, Jun. 2018, pp. 1–16.
[105] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun., IEEE 15th Int. Conf. Smart City, IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473.
[106] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in *Proc. ACM Workshop Cloud Comput. Secur.*, 2009, pp. 43–54.
[107] R. Claes, T. Holvoet, and D. Weyns, "A decentralized approach for anticipatory vehicle routing using delegate multiagent systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 2, pp. 364–373, Feb. 2011.
[108] E. Osaba, E. Onieva, A. Moreno, P. Lopez-Garcia, A. Perallos, and P. G. Bringas, "Decentralised intelligent transport system with distributed intelligence based on classification techniques," *IET Intell. Transp. Syst.*, vol. 10, no. 10, pp. 674–682, Dec. 2016.
[109] P. Mamoshina *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, 2018.
[110] A. Lotfi, C. Langensiepen, and S. W. Yahaya, "Socially assistive robotics: Robot exercise trainer for older adults," *Technologies*, vol. 6, no. 1, p. 32, 2018.
[111] J. Woods. (2018). *Blockchain: Rebalancing & Amplifying the Power of AI and Machine Learning (ML)*. [Online]. Available: https://medium.com/crypto-oracle/blockchain-rebalancing-amplifying-the-power-of-ai-and-machine-learning-ml-af95616e9ad9
[112] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*. Kuala Lumpur, Malaysia; Pearson Education, 2016.
[113] Team ChainIntel. (2018). *Distributed Decentralized Artificial Intelligence Framework for DApps*. [Online]. Available: https://blog.chainintel.com/distributed-decentralized-artificial-intelligence-framework-for-dapps-75fefdc554c5
[114] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Proc. Resilience Week (RWS)*, Sep. 2017, pp. 18–23.
[115] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, and B. Zhang, "A high performance blockchain platform for intelligent devices," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw.*, Shenzhen, China, Aug. 2018, pp. 260–261.
[116] ENTEFY. (2018). *Ai and Blockchain are Taking Root in the Global Agriculture Industry*. [Online]. Available: https://www.entefy.com/blog/post/570/ai-and-blockchain-are-taking-root-in-the-global-agriculture-industry/
[117] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[118] ASPENCORE Network. (2018). *Autonomous Supply Chain Will Soon be Empowered by IoT, AI, and Blockchain-Here's How*. [Online]. Available: https://iot.eetimes.com/autonomous-supply-chain-will-soon-be-empowered-by-iot-ai-and-blockchain-heres-how
[119] R. Wolfson. (2018). *Blockchain-Based AI Voice Assistant Brings Data Privacy to Smart Homes*. [Online]. Available: https://www.forbes.com/sites/rachelwolfson/2018/09/14/blockchain-based-ai-voice-assistant-brings-data-privacy-to-smart-homes/#1f965b3b6b50
[120] I. Sargeant and A. Tomlinson, "Maliciously manipulating a robotic swarm," in *Proc. ESCS 14th Int. Conf. Embedded Syst., Cyber-Phys. Syst., Appl.*, 2016, pp. 122–128.
[121] Y. Xu, T. Mo, Q. Feng, P. Zhong, M. Lai, and E. I.-C. Chang, "Deep learning of feature representation with multiple instance learning for medical image analysis," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 1626–1630.
[122] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.
[123] Y. Ge, D. K. Ahn, B. Unde, H. D. Gage, and J. J. Carr, "Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations," *J. Amer. Med. Inform. Assoc.*, vol. 20, no. 1, pp. 157–163, 2013.
[124] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," *J. Big Data*, vol. 2, no. 1, p. 1, Feb. 2015.
[125] Telcoin. (2018). *How Artificial Intelligence Can Support Blockchain Applications Like Telcoin*. [Online]. Available: https://medium.com/@telcoin/how-artificial-intelligence-can-support-blockchain-applications-like-telcoin-1c5bab8a1a68
[126] R. Xiong, E. P. Nichols, and Y. Shen. (2015). "Deep learning stock volatility with Google domestic trends." [Online]. Available: https://arxiv.org/abs/1512.04916
[127] Memoori. (2018). *The Innovative Startups That Could Bring AI & Blockchain to Smart Buildings*. [Online]. Available: https://www.memoori.com/innovative-startups-bring-ai-blockchain-smart-buildings/
[128] N. Graham. (2018). *Dutch Land Registry: How Blockchain and AI Could Benefit the Real Estate Industry*. [Online]. Available: https://www.ethnews.com/author/nathan-graham

[129] A. Couse. (2018). *How Drones, Data and AI are Changing the Property Sector*. [Online]. Available: https://www.weforum.org/agenda/2018/01/proptech-drones-data-ai-property-sector/
[130] X. Boyen, C. Carr, and T. Haines, "Graphchain: A blockchain-free scalable decentralised ledger," in *Proc. 2nd ACM Workshop Blockchains, Cryptocurrencies, Contracts*, 2018, pp. 21–33.
[131] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Oper. Syst. Princ.*, 2017, pp. 51–68.
[132] M. Brandenburger, C. Cachin, R. Kapitza, and A. Sorniotti. (2018). "Blockchain and trusted computing: Problems, pitfalls, and a solution for hyperledger fabric." [Online]. Available: https://arxiv.org/abs/1805.08541
[133] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, "Smart contracts vulnerabilities: A call for blockchain software engineering?" in *Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Mar. 2018, pp. 19–25.
[134] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 254–269.
[135] P. Tsankov, A. Dan, D. D. Cohen, A. Gervais, F. Buenzli, and M. Vechev. (2018). "Securify: Practical security analysis of smart contracts." [Online]. Available: https://arxiv.org/abs/1806.01143
[136] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "Smartcheck: Static analysis of ethereum smart contracts," in *Proc. IEEE/ACM 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, May/Jun. 2018, pp. 9–16.
[137] A. Stradling and E. Voorhees, "System and method of providing a multi-validator oracle," U.S. Patent 20 180 091 316 A1, Mar. 29, 2018.
[138] A. Anjum, M. Sporny, and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Comput.*, vol. 4, no. 4, pp. 84–90, Jul./Aug. 2017.
[139] H. Kakavand, N. K. De Sevres, and B. Chilton. (Jan. 2017). *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*. [Online]. Available: https://ssrn.com/abstract=2849251
[140] E. O. Kiktenko *et al.*, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, p. 035004, 2018.
[141] B. Rodenburg and S. P. Pappas, "Blockchain and quantum computing," The MITRE Corporation, Princeton, NJ, USA, Tech. Rep. MTR170487, 2017.



KHALED SALAH received the B.S. degree in computer engineering with a minor in computer science from Iowa State University, USA, in 1990, and the M.S. degree in computer systems engineering and the Ph.D. degree in computer science from the Illinois Institute of Technology, USA, in 1994 and 2000, respectively. He was with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia, for 10 years. In 2010, he joined Khalifa University, UAE, where he is currently teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. He is a Full Professor with the Department of Electrical and Computer Engineering, Khalifa University. He has authored or co-authored over 190 publications and holds three patents. He has been giving a number of international keynote speeches, invited talks, tutorials, and research seminars on the subjects of Blockchain, the Internet of Things, fog and cloud computing, and cybersecurity. He is a Senior Member of the IEEE. He is a member of the IEEE Blockchain Education Committee. He was a recipient of the Khalifa University Outstanding Research Award in 2014 and 2015, the KFUPM University Excellence in Research Award of 2008 and 2009, the KFUPM Best Research Project Award of 2009 and 2010, and the departmental awards for distinguished research and teaching in prior years. He serves on the editorial boards for many WOS-listed journals including the *IET Communications*, the *IET Networks*, Elsevier's JNCA, Wiley's SCN, Wiley's IJNM, J.UCS, and AJSE. He is the Track Chair of the IEEE Globecom 2018 on Cloud Computing. He is an Associate Editor of IEEE Blockchain Newsletter.

M. HABIB UR REHMAN was an Assistant Professor of computer science with the COMSATS Institute of IT, Wah Cantonment, Pakistan. His Ph.D. dissertation was with the Department of Computer Systems and Technology, University of Malaya, Kuala Lumpur. He is currently an Assistant Professor of computer science with the FAST National University of Computer and Emerging Sciences, Lahore, Pakistan. He focuses on big data analytics, the industrial Internet of Things, and blockchain technologies. He has authored or co-authored in 25 publications including 16 ISI-listed journal and magazine articles, three IEEE conference proceedings, and two book chapters. His research interests include wide spectrum of application areas including smart cities, blockchain, mobile social networks, quantified self, mHealth, and wearable assistive technologies among many others. His key research interests include mobile computing, edge-cloud computing, blockchain technologies, the Internet of Things, data mining, machine learning, and mobile distributed analytics.

NISHARA NIZAMUDDIN received the B.Sc. and M.Sc. degrees in computer science from VIT University, India, in 2010 and 2016, respectively. She was a Software Developer with BOSCH, India, for two years. She is currently a Researcher with the Department of Electrical and Computer Engineering, Khalifa University of Science Technology, UAE. She conducts research on projects involving blockchain, cloud computing, databases, and cybersecuirty. She has published a number of research articles on blockchain applications and infrastructure, Ethereum smart contracts, and cybersecurity.

ALA AL-FUQAHA received the M.S. degree from the University of Missouri, Columbia, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Missouri-Kansas City, in 2004. He is currently a Full Professor and the Director of the NEST Research Lab, Computer Science Department, Western Michigan University. He has authored or co-authored in a number of publications and has extensive experience with many popular private and public blockchain legers and platforms including IOTA, Algorand, Hyeprledger Fabric, and Ethereum. His research interests include the use of public ledgers (blockchain) in support of the security and privacy of the Internet of Things (IoT) and smart city services, the use of machine learning in general and deep learning in particular in support of the autonomic management of large-scale deployments of the IoT, and smart city infrastructure and services.