IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 14, 2022, accepted April 28, 2022, date of publication May 9, 2022, date of current version May 16, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3173297

An Updated Survey on the Convergence of Distributed Ledger Technology and Artificial Intelligence: Current State, Major Challenges and Future Direction

JAGGER S. BELLAGARDA[1] **AND ADNAN M. ABU-MAHFOUZ**[1,2], **(Senior Member, IEEE)**
[1]Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa
[2]Council for Scientific and Industrial Research (CSIR), Pretoria 0184, South Africa

Corresponding author: Jagger S. Bellagarda (u15165702@tuks.co.za)

ABSTRACT In recent times, Artificial Intelligence (AI) and Distributed Ledger Technology (DLT) have become two of the most discussed sectors in Information Technology, with each having made a major impact. This has generated space for further innovation to occur in the convergence of the two technologies. In this paper, we gather, analyse, and present a detailed review of the convergence of AI and DLT in a vice versa manner. We review how AI is impacts DLT by focusing on AI-based consensus algorithms, smart contract security, selfish mining, decentralized coordination, DLT fairness, non-fungible tokens, decentralized finance, decentralized exchanges, decentralized autonomous organizations, and blockchain oracles. In terms of the impact DLT has on AI, the areas covered include AI data privacy, explainable AI, smart contract-based AIs, parachains, decentralized neural networks, Internet of Things, 5G technology and data markets, and sharing. Furthermore, we identify research gaps and discuss open research challenges in developing future directions.

INDEX TERMS Artificial intelligence, distributed ledger technology, blockchain technology, machine learning.

I. INTRODUCTION

AI and DLT are currently two of the largest and most highly discussed sectors in Information Technology. The idea of AI was first introduced in a 1950 academic paper focused on "Computing Machinery and Intelligence" [1], while DLT gained traction nearly half a century later, with the introduction of Satoshi Nakamoto's Bitcoin whitepaper in 2009 [2]. Whether chatbots or self-driving cars, AI has progressed rapidly, aiming to execute both basic and complex tasks across a wide range of application domains [3]–[5]. Based on an article by the International Data Corporation (IDC), spending on AI is expected to double over the next four years (2020-2024) [6]. DLT offers a structured and distributed network of nodes that cryptographically secure and share data in a public verifiable ledger [7]. The World Bank has predicted by 2025, 10 percent of the global GDP could potentially be stored using DLT (specifically blockchain technology) [8].

There are a set of advantages and disadvantages for both AI and DLT. Therefore, research on their convergence could lead to potential benefits, while reducing the risks associated with each individually. Many advancements have focused on the emergence of applications using both technologies. Recent work on the use of AI for DLT, for example, has focused on the development of federated AI models deployed on DLT. This development would have nodes/aggregated nodes participating in a decentralized network responsible for training AI-based Machine Learning (ML) models [9]. The benefits would include reducing the risk of privacy exploitation by limiting the ability of the initial data input into the ML model to be shared. Alternatively, from a DLT in AI perspective, a recent work, for example, focuses on the development of Proof-of-Deep Learning as an alternative proof-of-work consensus algorithm. This design would aim to harness and recycle blockchain computational energy

The associate editor coordinating the review of this manuscript and approving it for publication was Valentina E. Balas.

and re-invest it back into the execution of deep learning models [10].

However, the convergence of these two technologies poses challenging questions regarding the development of non-repudiation in artificial intelligent decision making processes and the use of AI in time sequenced public ledgers. The challenge with decentralized federated AI, as discussed above, is that a limited performance overhead would exist when compared to traditional ML models. Furthermore, from a AI for DLT perspective, the challenge facing Proof-of-Deep Learning is that it is a novice concept and requires more in-depth research in order to make it a potentially viable solution. These are some of the challenges facing the convergence of AI and DLT. Another notable challenge that spans across both technologies is the level of trust we as humans have in participating in the network through the sharing of our financial and non-financial data [11]. The research explored in this paper will show how the convergence of AI and DLT can generate great results that can be used to further advance the potential of both technologies, and, eventually, to expand the benefits of AI and DLT across industry in more real world use cases. Furthermore, it will also highlight the risks and challenges that exist as well as indicate which sectors of convergence require further research.

Due to the rapid development in both technologies, the ability to accurately gather, analyse and process information is a demanding task. Many of the previous review papers, despite crucial additions made to current research, focused mainly on either the use of AI for DLT or the use of DLT in AI but not both [12]. Furthermore, some review papers only observed blockchain technology and did not consider other DLTs [13]. However, a paper by [14] does take all of these aspects into consideration and addresses them. The comprehensive structure of [14] was therefore used as a foundation for this research paper. The novelty achieved in this review is that it aims to add to the current literature of each specific section. In addition, a focus has also been placed on new developments not covered before in other review papers observed. This refers to the development and use of parachains and how they can be used to further improve the development of AI.

This research paper will focus on contributing towards the following research points:

- Gather, analyse and present a detailed review on the convergence of AI and DLT in a visa versa manner.
- Review how AI is impacting DLT by focusing on areas of AI-based consensus algorithms, smart contract security, selfish mining, decentralized coordination, DLT fairness, non-fungible tokens, decentralized finance, decentralized autonomous organizations, decentralized exchanges and blockchain oracles.
- Review how DLT is impacting AI by focusing on areas of AI data privacy, explainable AI, smart contract-based AIs, parachains, decentralized neural networks and data markets, and sharing.
- Identify research gaps and discuss open research challenges in order to develop a future direction.

The research conducted in this paper aims to further develop on the current body of knowledge. This will be achieved by focusing on various topics ranging from those with a long history of research such as explainable AI to novice concepts such as parachains and non-fungible tokens. The ultimate goal will be to identify the current state of research, major challenges and future research directions regarding the convergence of DLT and AI.

In order to comprehensively address these research questions, an understanding of what is meant by the concept of technological convergence is gained, in addition to conducting a narrative literature review on the convergence of AI and DLT, and developing a future research direction. The rest of this research paper is structured in the following manner: the 2nd section focuses on the research methodology; the 3rd section describe the background of AI and DLT; the 4th and 5th sections explore the current literature review of DLT for AI and AI for DLT respectively; section 6 compares and discusses the main topics gained in the previous two sections; section 7 focuses on identifying current applications and use cases; and finally, the 8th section focuses on identifying research gaps and developing a future research direction, before drawing to a conclusion in section 9.

A. ABBREVIATIONS AND ACRONYMS

TABLE 1. Abbreviations.

Abbreviation	Description
AGI	Artificial General Intelligence
AI	Artificial Intelligence
BTC	Bitcoin
DAG	Directed Acyclic Graph
DDOS	Distributed Denial-of-Service
DLT	Distributed Ledger Technology
IOT	Internet of Things
MDP	Markov Decision Process
MITM	Man-in-the-middle
ML	Machine Learning
PoDL	Proof-of-Deep Learning
PoKW	Proof-of-Kernel Work
PoW	Proof-of-Work
TEE	Trusted Execution Environment
XAI	Explainable AI
NFT	Non-fungible Token
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
DEX	Decentralized Exchange
IoT	Internet of Things

II. RESEARCH METHODOLOGY

In order to gain a comprehensive overview of all applicable research in the sectors of AI and DLT convergence, it was important to establish a framework on how these sources would be gathered. A majority portion of this research was systematically identified and gathered from the following range of credible journals and conferences:

- IEEE Xplore
- AIS Electronic Library
- Springer Link
- Springer Open
- ArXiv (e-Print archive)
- MDPI
- SSRN (Social Science Research Network)
- Royal Society Publishing
- Science Direct

In addition to this, a portion of research was cited from several less formal sources. This is due to the fact that the topics discussed in this paper, namely DLT and AI are both rapidly developing technologies and in order give the most updated state of research in these fields, it was important to consult additional sources such as blog posts (i.e. Business Insider, VICE), video and written lecture pieces (i.e. MIT and IBM) and media releases (i.e. Deloitte and Bank of England). These together with ArXiv's preprints are released faster than published works, allowing for the latest research to be gathered in these rapidly developing fields. It is imperative to mention that all of these sources were analyzed for their credibility by assessing each author, company or research body's contributions. In addition, more than one source per section was analyzed in order to give a comprehensive understanding of each section in the literature review.

The search terms used consisted of an array of single and/or combined phrases located in either the title and/or body of the piece. The following was used within the researchers search term:

- 'DLT' OR 'Distributed Ledger Technology' as the main research terms with 'Blockchain Technology' OR 'DAG' OR 'Hologram' being used as advanced search terms.

  An estimated total of 15600 research sources were identified for these search terms.
- 'AI' OR 'Artificial Intelligence' as the main research terms with 'Narrow AI' OR 'Weak AI' OR 'Artificial General Intelligence' OR 'Strong AI' OR 'Machine Learning' OR 'Neural Networks' OR 'Deep Learning' OR 'Reactive Machine' OR 'Smart Information Systems' being used as advanced search terms.

  An estimated total of 1 240 000 research sources were identified for these search terms.

These search terms were then combined in order to identify sources of AIs convergence with DLT and DLTs convergence with AI. An estimated total of 4 680 research sources were identified based on the combination of search terms. This however did not specifically display different sources linked to AIs enhancement of DLT and then DLTs enhancement of AI. Therefore, this population was further disseminated into two categories, an AI for DLT stack and a DLT for AI stack. This was achieved by breaking each stack into several major subsections which are investigated in the literature review section of this paper. It should be further noted that research prior to 2008 has been excluded due to the fact that blockchain technology, the most popular DLT, was first introduced through the whitepaper release of the cryptocurrency Bitcoin by its creator Satoshi Nakamoto in 2009 [2]. Research was conducted from the 14th of January 2021 to the 11th of March 2022.

Finally, several of the topics presented in this paper are influenced by [14]. However, additional recent topics focusing on the convergence of DLT and AI has been included. These topics include the following:

- Parachains
- Decentralized Neural Networks
- Non-fungibe Tokens
- Decentralized Finance
- Decentralized Exchanges
- Decentralized Autonomous Organizations
- Blockchain Oracles
- Internet of Things
- 5G Technology

III. BACKGROUND

The Merriam-Webster dictionary describes the term Convergence as "the merging of distinct technologies, industries, or devices into a unified whole". The concept of technology convergence was first coined in 1990 and has grown into the emergence of integrated fields such as nanotechnology, bioinformatics, and computational linguistics. In this section, the background of AI and DLT will be explored in order to establish a clear understanding of each concept before further investigating their convergence.

A. DLT

DLT is an umbrella term for multi-stakeholder and cross party systems that process data in a decentralized manner within trustless environments [15]. DLT is divided into two main categories, private and public.

1) PRIVATE DLT

A private DLT strictly requires nodes to have permission to join a network, these types of DLTs make use of a distributed rather than a decentralized architecture. Furthermore, they are less transparent in their nature due to the hierarchy of role-based access where validators are manually appointed rather than a consensus protocol being followed [16]. Examples of private DLTs include Hyperledger Fabric [17] and Quorum [18].

2) PUBLIC DLT

A public DLT, also known as a permissionless DLT, is open to any user in the network, allowing them to join the network as a node. Consensus protocols are followed, allowing users in the network to view and validate data transactions. Public DLTs are also both decentralized and distributed and examples include cryptocurrencies such as Bitcoin and Ethereum built on blockchain technology [16]. There are 3 main public DLTs the researchers want to highlight.

a: BLOCKCHAIN TECHNOLOGY

Blockchain technology is the most known DLT, garnering a lot of attention since the introduction of the cryptocurrency Bitcoin [2]. Blockchain technology can be described as a distributed consensus model that is unchangeable, containing a shared digital ledger made up of a chain of blocks that sequentially records tangible and intangible data transactions [19]. Data transactions are recorded on the blockchain by being verified by a majority of the miners (an agent that holds a full node) on the network [20]. Each block contains the following four elements [21]:

- A set of transactions.
- A hash taken from the previous mined block - this indicates that each block will be produced in a chronological fashion because the current block can identify where it came from.
- A header for each block containing its hash value.
- A merkle hash tree.

The Bitcoin blockchain for example, uses a ''proof-of-work'' consensus protocol in order to confirm and process transactions. This entails miners of the network having to solve mathematical puzzles by hashing a set of transactions in the block. This therefore generates new blocks to the blockchain. It is imperative to note that the Bitcoin blockchain uses a SHA256 (Secure Hash Algorithm 256-bit) cryptographic hash function to do this [22].

b: DIRECTED ACYCLIC GRAPH (DAG)

In mathematics, the concept of DAG is a graph that moves in one direction without connecting the other edges. Therefore, it makes it impossible to transverse the whole graph starting at one edge. A DAG DLT uses this logic by only allowing nodes and transactions to move in specific directions [23]. Each transaction is connected to at least one other in the following manner:

- Transactions are directed by earlier transactions connecting to later transactions.
- Transactions are acyclic meaning a specific transaction cannot loop back and connect to itself.
- Transactions are connected in a mesh type of fashion, representing nodes linked to each other in a graph network.

An example of a DAG DLT is IOTA's Tangle [24].

c: HOLOCHAIN

An agent-focused rather than data-focused architecture. It opts to not use any consensus algorithm and instead gives each agent their own forking system, thus increasing scalability of the network [25]. This DLT is relatively new and still requires further research and investigation.

3) RECENT BLOCKCHAIN TECHNOLOGY ADDITIONS

Research into blockchain technology has increased over the years and has moved from building individual blockchains to focusing on the scalability and interoperability between blockchains. This section will explore sidechains and parachains as recent additions to potentially achieving these goals. Furthermore, other protocol developments such as smart contracts, non-fungible tokens, decentralized autonomous organizations, decentralised finance, decentralized exchanges and blockchain oracles have been included.

a: SIDECHAINS

A sidechain is a completely separate secondary blockchain, connected to a parent/main blockchain by means of a two-way peg which allows for the interchangeability of digital assets at a pre-agreed rate between the main blockchain and its sidechain(s). It should be noted that side chains can have a completely different consensus protocol to the main blockchain [26]. Furthermore, sidechains aim to take a computational load off of main blockchains, increasing scalability and flexibility [27].

b: PARACHAINS

Parachains (short for parallelizable chains) are application specific data structures that are validated by validators in a relay chain. Parachains make use of the security provided by relay chains and due to their parallel nature, parachains are able to process transactions in a scalable, secure manner and perform highly distributed computations completely independently, reducing the overall stress placed on the root relay chain [28]. This means that if there are five parachains, then all can be executed in parallel without the fear of collision and all can use the same source of security. There are also highly specific parachains developed for distinct purposes [29]. These include, but are not limited to, Encrypted Consortium Chains, Privacy Chains and Smart Contract Chains. Polkadot is a blockchain for scalable decentralized computation and interoperability and makes use of parachains to accomplish this [30]. The Polkadot blockchain is a ''level 0'' solution that uses a relay chain at its centre and surrounds it with parachains that connect automatically. Furthermore, non-parachains such as Bitcoin and Ethereum require a bridge to connect to the Polkadot ecosystem [31].

c: SMART CONTRACTS

A smart contract is an agreement between two entities that is initiated by a piece of code stored on a blockchain that will automatically execute once a set of attributes have been met. Smart contracts are currently used for various purposes including, but not limited to, financial trades, credit authorizations and crowdfunding agreements (ICOs) [32]. The codes of smart contracts are replicated across nodes on a blockchain and therefore benefit from the security, privacy and immutability that blockchain technology provides [33]. The biggest smart contract provider is Ethereum but, various other platforms exist such as Cardano and NEO [34].

d: NON-FUNGIBLE TOKENS (NFTs)

An NFT or Non-fungible token represents a unique and non-interchangeable digital asset that is stored on a blockchain.

Data stored in an NFT is digitally secured and verified using the cryptographic functions related to blockchain technology [35]. Current real-world use cases for NFTs include digital artworks, digital collectables and event ticketing.

e: DECENTRALIZED AUTONOMOUS ORGANIZATION

A Decentralized Autonomous Organization (DAO) is an organization designed with a programmed set of open-source coded rules and governed by a community of users. The aim of a DAO is to reduce the risk of human error or manipulation regarding the management of data and finances by making decisions based on an automated set of rules and through the majority decision taken by a community of users [36].

f: DECENTRALIZED FINANCE

Decentralized Finance (DeFi) is a relatively new concept that aims to provide financial products, services and instruments using distributed ledgers and smart contracts instead of through traditional avenues such as brokerages or banks [37].

g: DECENTRALIZED EXCHANGES

A decentralized exchange (DEX) is a cryptocurrency exchange where peer-to-peer transactions are enabled through the use of self-executing code agreements residing in underlying smart contracts. Therefore, there is no requirement for an intermediary party to facilitate the buying and selling of assets as is with traditional exchanges [38].

h: BLOCKCHAIN ORACLES

Blockchain oracles are third-party services that allow blockchain-based smart contracts which exist on-chain to access off-chain data. An example of data gathered, evaluated and verified by a blockchain oracle could be temperature measured by a sensor (hardware oracle) or cryptocurrency price information gained from a 3rd party exchange (software oracle) [39].

B. AI

A 1950 paper by [1] introduced the development of The Turing test. This imaginary simulation aimed to test whether or not a machine had the capability to think and perform in the same manner as a human being. This was potentially one of the first concepts of AI. AI is described in many different ways, due to this being a literature review paper, several definitions of AI have been identified. The following detail the most applicable at the discretion of the researchers:

- The Merriam Webster dictionary - " a branch of computer science with the simulation of intelligent behaviour in computers".
- AI: A Modern Approach - "The study of agents that receive percepts from the environment and perform actions. " [3].
- Patrick Winston, the Ford professor of AI and computer science at MIT - "Algorithms enabled by constraints, exposed by representations that support models targeted at loops that tie thinking, perception and action together. " [40].

While many publications and articles created their own definition of AI in the preamble of their works, it is determined that many of these definitions provide a broad abstract understanding of AI. These definitions are vague and can misrepresent exactly which type of AI is being discussed. It is therefore important to establish an overview of the technologies, models and methods that fall within AI. In article by the authors of [41], a 2-dimensional model is presented which aims to assess the maturity of AI based on its intelligence capabilities. This is shown with the x-axis representing an AIs ability to address aspects of uncertainty and the y-axis representing the ability to adapt and solve various problems. Based on this model, 5 AI maturity levels are presented.

1) REACTIVE MACHINES

Reactive machines refer to the oldest version of AI created. The capability of this type of AI is limited to its reaction to various stimuli and is not built with memory-based functionality, thus restricting its ability to learn from past activity and data [42]. An example of a reactive machine is IBM's Deep Blue (chess computer) built in 1997 [43].

2) SMART INFORMATION SYSTEMS

Smart Information systems make use of AI, specifically machine learning and deep neural networks, to analyze big data and create smart technologies that are currently used in various industries from robotics in the assembly of automobiles to the development of entire smart homes and cities [44].

3) ARTIFICIAL GENERAL INTELLIGENCE

AGI often referred to as "strong AI" and is currently a hypothetical form of AI [45]. AGI describes an intelligent entity that can interpret and understand data in the same manner as the human brain. It aims to do this through the development of a universally accepted algorithm that can be used to learn and act in any environment [46]. AGI is currently an idea and presents the concept of AI-based robotics, which differs from the focus of this research paper which will be on the use of AI software in convergence with DLT. The researchers will focus on the further improvement of AI decision making using past and current data sets, rather than on artificially intelligent robotics and its interpretive analysis of data to come to a decision [47].

4) SELF-AWARE AI

The concept of a self-aware AI is very similar to that of AGI. The only difference is that a self-aware AI would develop the ability to both understand and evoke emotion, beliefs and desires of its own [48]. As mentioned above, this version of AI is currently hypothetical and therefore will not form part of the focus of this paper.

5) NARROW AI

Narrow AI aims to use a set of rules to analyze large quantities of data in order to develop forecasts regarding a specific task at hand [49]. IBM, for example, uses narrow AI in the development and operation of their supercomputer Watson [50]. However, narrow AIs specific focus on a single domain adds a limitation to its ability, due to the logic behind its computational analysis not being easily transferable to another task. Therefore, narrow AI cannot compute dynamically across domains as humans do [51], [52].

Machine Learning is the application of algorithms in systems that give them the ability to autonomously learn, develop and enhance from experience rather than being specifically programmed [53]. ML models aim to use initial data samples as a foundation and to continually analyse and learn by identifying patterns in the data. Eventually, the model would be able to learn autonomously by itself without any external help [54]. There are 3 main machine learning algorithms the researchers want to highlight.

a: SUPERVISED MACHINE LEARNING

Supervised machine learning is a set of algorithms that use known labeled sets of input data (x) to produce a known output (Y) in an accurate manner [55]. The algorithm/s continually make predictions of the outcome and are repetitively adjusted until the correct output is generated [56].

$$Y = f(x) \tag{1}$$

Supervised machine learning can be classified into two types of issues, a classification issue and a regression problem. A classification issue is when the outcome data should be assigned into a specific category (such as a decision tree where the outcome could be ‘blue’ or ‘green’) [55]. A regression problem on the other hand, aims to interpret the connection between the dependent and independent data sets (such as using linear regression to determine housing prices) [57].

b: UNSUPERVISED MACHINE LEARNING

Alternative to supervised learning, this set of machine learning algorithms aim to analyse unlabeled sets of data by determining unknown patterns through learning about the similarities and differences in the data [58]. An example would be facial recognition. Common methods used within unsupervised learning are clustering and association rules [59].

c: REINFORCEMENT LEARNING

Reinforcement learning aims to develop and train an ML model in a trial-and-error fashion so that it can reach the correct conclusion and make the right decisions in a complex situation. The model would be rewarded for a right decision and penalised for a wrong decision, thus allowing the system to learn from its own mistakes [60]. This approach differs from supervised learning as the AI is given no idea of what the correct outcome should be [61].

IV. REVIEW OF DLT FOR AI

The first part of this literature review aims to explore how DLT could be used to enhance AI. Based on the researchers analysis of the current state of research in this field, the following main subsections have been identified.

A. DLT-BASED AI DATA PRIVACY

The battle between privacy and personalization has become a leading talking point. Major technology companies such as Facebook, YouTube and more recently TikTok aim to use centralized AI-based data collection and analysis techniques to curate content for their users. Netflix, for example, recommends videos to a user by analyzing not only the specific users viewing patterns, but also the viewing patterns of other users on the platform [62]. This presents a risk of imposing on a users’ privacy. Facebook, for example, encountered a massive scandal in 2018 when data analytics firm Cambridge Analytica had improperly gained data from over 87 million Facebook users [63]; AI-enhanced DLT could be a potential solution to this problem. An article by the authors of [12] proposes the example of a social network where an AI collects and analyses user’s data in a decentralized manner from the user’s device. Data is then personalized and returned back to the user in a closed loop. The development of such a platform could lead to users having both control over their data and allow them to find comfort in knowing their privacy is protected while at the same time receiving the benefits of automatic data customization. An article by the authors of [64] explore how such data sharing platforms would be designed and built.

1) DECENTRALIZED FEDERATED AI

Federated learning, also known as collaborative learning, aims to train a machine learning model using only the data stored on a local device. Once the data has been gathered and analyzed, the resulting output (not the data itself but, rather what the ML model has learnt) is sent to a master client. The master client will then group the output from a multitude of different devices and form a new model, without ever removing data off each local device [65]. This approach differs from traditional models where multiple different data sets are uploaded to a central point and analyzed. The evolutionary next step in the development of Federated AI would be to deploy it on a DLT. DLT-based federated learning would have nodes/aggregated nodes participating in a decentralized network and responsible for training AI-based ML models [9]. Due to the nature of DLT, various benefits would become prevalent. These include reducing the risk of privacy exploitation by limiting the ability for initial data inputted into the ML model to be shared. Furthermore, an article by the authors of [66] present an AI marketplace built on the blockchain where users can purchase ML models and sellers can use their local computational capacity to further enhance the model’s data quality. The authors identified a 15 percent reduction in the cost of execution.

However, an article by the authors of [67] explores the disadvantage present in federated AI's when compared to traditional machine learning models. It is determined that the introduction of DLT brings with it a limited performance overhead of up to 15 percent for federated learning models. This, however, does present an opportunity for future research, which will be discussed at a later stage. In [68], the authors explore the use of a DLT-based federated learning model in the healthcare sector. In this article, the authors present a potential privacy preserving solution to patient data. The use of federated learning models deployed via smart contracts on the Ethereum blockchain system allows data to be accurately and securely logged and input data never being released.

2) TRUSTED EXECUTION ENVIRONMENTS

Trusted Execution Environments (TEEs) are situated in an isolated compartment of the main processor of a central processing unit, but outside the normal operating systems in which data can be stored confidentially and transferred securely between or from applications running within the TEE [69]. Based on the nature of TEEs, it only shares data with third party applications that meet all criteria points which are established to maintain its trustworthy nature. Current real-world use cases for TEEs include smart phones. The TEE presented in this use case is a separate processing environment that exists apart from the rich execution environment (RSS) containing its own memory and storage. The TEE is used to perform sensitive operations and store sensitive data.

In some cases of DLT, there is data that is hypersensitive and requires the highest level of privacy. A solution to this is the use of trusted execution environments. An article by the authors of [70] explores DLT-based off-chain payment channels setup in TEEs to secure transactions between parties. Furthermore, development into the use of TEEs in permissioned DLTs is found in articles by the authors of [71], [72] and [73]. A further look into LucidiTEE by VISA explains how analytics take place in each secured part of the TEE without retaining any input or output data, thus enforcing history-based policies (the current rules surrounding data is dependent on the prior use of that data) [71]. In a similar fashion to DLT-based federated AI, a potential negative in the use of TEEs is that the extent of the trustworthiness of the TEE is at the mercy of the hardware manufacturer.

3) DIFFERENTIAL PRIVACY

The best way to describe this is to use an example where differential privacy has been utilized. In October 2006, Netflix created a competition open to the public whereby they challenged any person/group to develop a system that could outperform the accuracy of their collaborative filtering program using a dataset of movie ratings. This dataset held no personal identifying data, but it resulted in participants recovering over 99 percent of personal data by using auxiliary data points from IMDB [74]. Differential privacy aims to incorporate randomly generated noise into algorithms to lessen the risk of privacy issues by malicious third parties. Therefore, data becomes fuzzy and imprecise, making it more difficult to breach [75].

In an article by the authors of [76], the use of differential privacy in DLT (specifically blockchain technology) is explored to achieve further privacy enhancements. They experimented using differential privacy to achieve secure self-controlled private data sharing on the blockchain. This article was presented using a prototype built on the Quorom network (an Ethereum blockchain smart contract platform). This however, is still a prototype that uses an experimental approach and gains experimental results. Therefore, further research is still required.

B. EXPLAINABLE AI

As the sophistication of AI increases so does the level of trust required. The decision making of AIs has rapidly transitioned from virtual assistants (examples include Apple's Siri and Amazon's Alexa) to complicated aggregated machine learning models that make life and death decisions (examples include self-driving cars and healthcare systems).

A further issue known as the black box dilemma which deals with the fact that we have minimal insight into how AI's make the decisions they do [77]. Due to the complex nature of machine learning algorithms, it is often not understood exactly how and why AI systems make the decisions they do, specifically in the development and use of deep neural networks. Explainable AI (XAI) proposes a potential solution to solve the black box dilemma of AI systems. Researchers aim to use a set of tools and frameworks to understand the predictions generated by AI models. Further to this, XAI can provide reasoning for decisions made and whether the decision is justifiably positive or negative by implementing continual feedback taking into account new datasets and thus revisiting the value of the decision made.

There are several articles that explore the use of DLT in explainable AI systems. These range from the incorporation of federated learning models [9], [67] and trusted execution environments [78] but, there are two sources the researchers would like to highlight. In an article by the authors of [12], the need for an immutable audit trail to track the flow of data patterns that AI systems use to make the decisions is explored. DLT offers a potential solution in tracking AI data and offering interested parties a detailed audit trail to track each decision made by an AI system. In an article by the authors of [79],the development of AGI (Artificial General Intelligence) progression using DLT encryption, specifically smart contracts, as a more efficient alternative to human-based monitoring is investigated. A drawback in this article is that AI data pattern control systems need to be developed and tested in a transparent, non-hackable simulation. The field of DLT-based explainable AI poses one of the best fields for future research. The advantages of achieving the comprehensive levels of trust with AI systems through the use of DLT and, finally opening the black box by identifying the 'why' behind decisions made could be a massive step forward in the evolution of practical use cases such as self driving cars.

C. SMART CONTRACT-BASED ARTIFICIAL INTELLIGENCE

In an article by the authors of [9] and [80], the use of smart contracts as a platform to ensure computational integrity on which machine learning models can be situated is investigated. This entails placing artificial intelligent systems onto DLT (specifically blockchains) using smart contracts and decentralized applications. Users would be able to deploy AI systems on smart contracts and have them self-execute once a predefined set of conditions have been met. This is further explored by the authors of [81] in their article. The authors explore the use of smart contract-based AIs to transport pieces of software which would be free from bugs and loopholes, a current issue experienced in the development of blockchain by a multitude of different participants. In the article by the authors of [82], the use of Ethereum smart contracts together with AI systems to provide visibility on decisions taken by an AI (in this case it refers to the development of Deepfake video content) is explored, therefore making digital content credibly traceable. There have been further articles that look at establishing smart contract-based economies in sectors such as electric vehicles [83] and identity management systems [84].

As a build on the current state of research, ML models placed on off-chain smart contracts can be better implemented in TEEs, based on the fact that TEEs can supply high levels of computational power through the use of GPUs while still preserving the anonymity of personal data. This is supported in articles by the authors of [85] and [86] with them further investigating the ability for smart contract executions to be scaled off-chain while simultaneously maintaining high levels of data integrity. However, a potential drawback is that the solution can easily be implemented in Ethereum smart contracts, but not in other blockchains and/or DLTs without modification to the original scripting system.

D. DATA MARKETS AND STAKING-BASED DATA SHARING

The operating effectiveness and accuracy of ML models and AI systems is based heavily on the amount of data that is inputted. The generation of high-quality comprehensive data sets require the ability for highly skilled actors to identify and describe information correctly [87]. This data, when fed into ML models generates non-partisan outcomes and allows the AI systems to make the most accurate decisions possible. Companies, such as Google and Facebook, benefit from the combination of both high-level AI developments and the ability to feed those AI systems with large quantities of data. The issue here is that a few large entities are in control of large sets of personal data, which they make revenue from (i.e. Facebook Ads) and their methods behind how they process this data is unknown. Therefore, the development of DLT-based data marketplaces poses a potential solution.

In an article by the authors of [11], the development of staking-based protocols for data access and monetization is described. Their whitepaper refers to the development of DLT-based (using Ethereum ERC20 wallets) data marketplaces where publishing and consuming data is tokenized. Furthermore, providers are rewarded for their data based proportionally on the amount of token liquidity staked. By creating both staking requirements and associated tokenized rewards for data, it therefore leads to more users participating in the system. Thus, high-quality private data can be obtained in a decentralized manner, allowing all parties involved to gain from the process. Individual users can monetize their private data and smaller players in the field of AI system development could gain more high-quality data. A potential drawback to this is that data is only gained if the individual users trust in the system is enough to warrant providing their personal data.

E. PARACHAINS

In January 2021, Ocean Protocol, a decentralized data exchange protocol came together with Polkadot, a multi-chain technology in order to give Polkadot users the ability to transfer data on the Ocean Protocol marketplace. This was achieved through Moonbeam, an Ethereum compatible smart contract parachain on the Polkadot platform [88]. Ocean Protocol's compute-to-data framework aims to increase the advantages of using private data (i.e. for research and business purposes) while reducing the risk of privacy exploitation by never directly sharing data, but rather granting specific access to it. Data is never moved away from the ownership of the entity/individual while still allowing third party developers/researchers to use the data to further improve AI models [11]. However, until now this has only been possible on the Ocean Protocol platform. The introduction of Moonbeam and specifically the parachain-based framework of the Polkadot network makes it possible for interoperability between users and data on both networks to occur [89]. The ultimate aim for Ocean Protocol is to become the underlying data layer for multiple blockchains [89]. This ability for parachains to be deployed and connected could potentially mean that full interoperability across blockchain networks is achieved. This could make the transfer of data across networks possible, and when specifically focusing on data used for AI models, it could mean quicker and easier access to high quality datasets. However, the development and use of parachains is fairly new and further research and development into the viability of this solution is required.

F. DECENTRALIZED NEURAL NETWORKS

In an article by the authors of [90], an AI platform called DeepBrain Chain is presented. Through the use of blockchain technology it aims to lower the cost of processing power in addition to using smart contracts to ensure the privacy, security and ownership of data as well as the transparency of developed AI algorithms.

Furthermore, in an article by the authors of [91], a privacy preserving decentralized learning of randomized neural networks is presented. The article identified that decentralized learning of randomized neural networks resulted in a similar performance to a centralized approach where full training data is available at a single node. However, it should be noted that there is a need for further testing of more randomized-based neural networks.

G. INTERNET OF THINGS

In an article by the authors of [92], the use of blockchain technology is presented as a potential solution to reducing high energy consumption caused by Internet of Things technology. In an article by the authors of [93], architectures for blockchain technology integrated Internet of Things is presented. The article explores the incentives and use cases for such an integration to occur and presents an architecture titled BIIT 1.0 as a potential solution.

An alternative framework is presented in an article by the authors of [94]. In order to address security, scalability and latency issues related to Internet of Things, a blockchain-based distributed cloud architecture with a software defined networking (SDN) is presented. This enables the distribution of fog nodes at the edge of the network. An evaluation was conducted against other existing models and resulted in an overall improvement in performance and a reduction in delay and response time.

H. 5G TECHNOLOGY

In an article by the authors of [95], 5G technology is explored and further developed through the use of both AI and blockchain technology. Currently, 5G makes use of various complex digital technologies such as Multiple Input Multiple Output which runs over higher radio frequencies. The introduction of AI can assist in simplifying these complex processes but it raises a security and privacy concern. The article presents the case of integrating blockchain technology to secure AI-enabled 5G cellular networks. Furthermore, the authors present a simulated case study using blockchain technology for AI-enabled 5G which resulted in a 20 percent decrease in energy consumption at the RAN level.

V. REVIEW OF AI FOR DLT

The second part of this literature review aims to explore how AI could be used to enhance DLT. Based on the researchers analysis of the current state of research in this field, the following main subsections have been identified.

A. AI-BASED CONSENSUS ALGORITHMS

Since the release of Bitcoins whitepaper by Satoshi Nakamoto [2] in 2008 and the emergence of its underlying driver blockchain technology, there have been multiple different consensus algorithms released with each proposing a solution to DLT drawbacks and weaknesses [96]. Several articles in current literature explore the use of AI-based consensus algorithms to solve the enormous amount of computational energy that is lost to the Proof-of-Work (PoW) consensus. The following indicates the two AI-based consensus algorithms the researchers want to highlight from current literature.

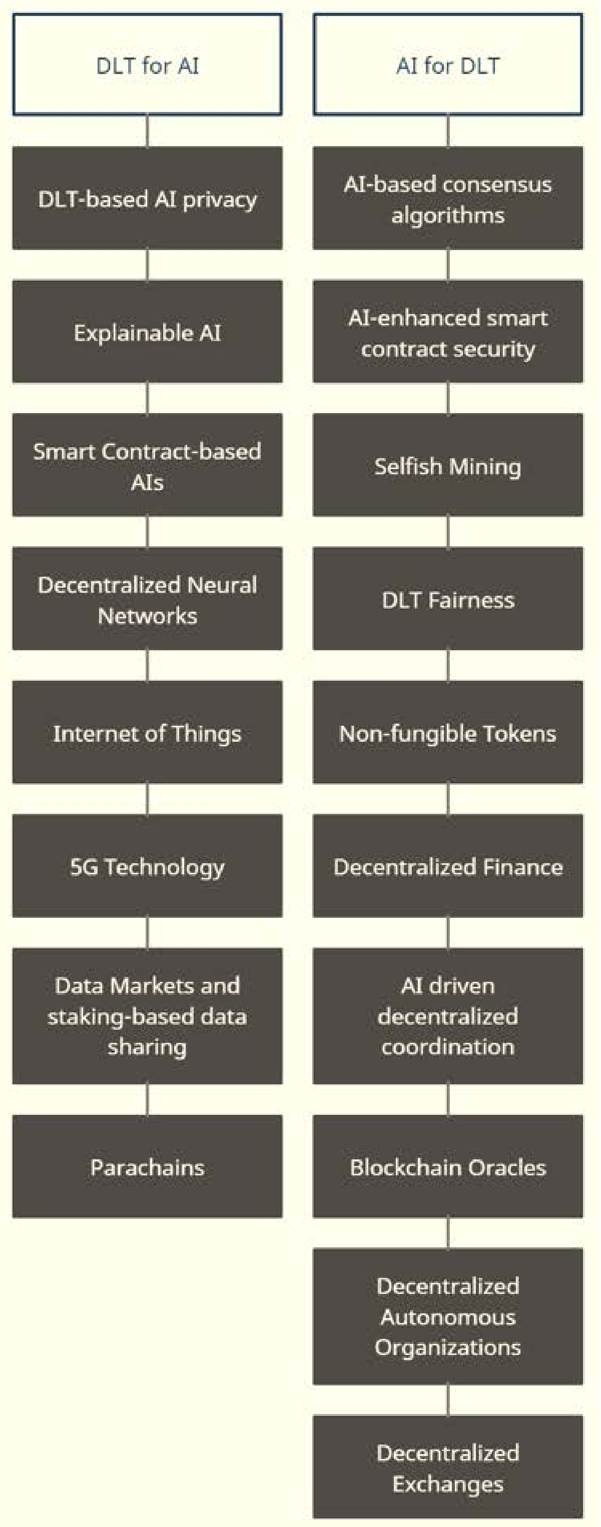


FIGURE 1. Overview of current research topics.

1) PROOF-OF-DEEP LEARNING

In an article by the authors of [10], Proof-of-Deep Learning is a proof-of-concept design that harnesses and recycles blockchain computational energy and re-invests it back into the execution of deep learning models is investigated. This is achieved through the establishment that a valid proof for a new block would only be produced if a deep learning model is generated. However, a potential drawback is that malicious requesters and miners are able to generalize the model requester. In addition, this approach is still conceptual and therefore requires further research to be performed using a realistic pattern of block submission and more deep learning data sets.

2) PROOF-OF-KERNEL WORK

In an article by the authors of [97], the Poof-of-Kernel Work (PoKW) consensus algorithm where only a reduced number of nodes participate in solving Proof-of-Work computational puzzles in such a way that malicious third parties cannot stage an attack due to the reduced strike area is investigated. The use of AI in making their consensus approach adaptive to various systems is shown through a use case. A pilot project collaboration by XAIN and Porsche was run focusing on improving blockchain-powered hybrid Porsche vehicles through reinforcement learning and PoKW. The results increased efficiency and security in communication between vehicle machine networks. Furthermore, it allowed for substantial reductions in energy consumption and democratized networks including mobile low-power devices such as in engine control units (ECUs) in connected vehicles.

B. ARTIFICIAL INTELLIGENCE-ENHANCED SMART CONTRACT SECURITY

The articles in this subsection explore how AI is used to further improve smart contract security.

1) THE USE OF NEURAL NETWORKS

In an article by the authors of [98], neural networks are used as a method to analyse the operational code gained from smart contracts and therefore classify the particular sector a smart contract exists is explored. In [99], the authors take a different approach, running long short-term memory (LSTM) neural network architectures on various different smart contract operational code. A specific article by the authors of [14] highlights an article by the authors of [100] and their method to detect honeypot smart contracts. However, before this article can be explored, it is important to explain what a smart contract honeypot transaction is. A honeypot is a malicious smart contract that is used to deceive, usually novice users of their funds by luring them in with a free, withdrawable amount stored in a smart contract. However, once the user interacts with the smart contracts, the funds are not released and the processing fees used to initiate the withdrawal are taken [100].

In an article by the authors of [100], the case of using data analysis techniques to detect smart contract transaction behaviour is presented. They achieve this by collecting aspects of smart contract data such as flow of funds, source code length and other features used in the detection of honeypot smart contracts. This is then aggregated into a training model and executed. This would allow for the detection of new honeypots based on already known techniques. In an article by the authors of [100], the analysis of contract bytecode and transaction behaviour in order to identify honeypots is explored. They do this by separating instances of movements in funds between the contract creator, the contract and the transaction sender. Furthermore, transaction attributes that contain vital information for the detection of honeypots are identified. This approach allowed for both the identification of new honeypots based on already known techniques as well as the identification of unknown honeypot techniques by sequentially removing one technique from the training set. However, a potential drawback is the inability to identify contracts or accounts with larger transaction histories and place it into categories that do not involve honeypots.

Based on further analysis of long short-term memory (LSTM) neural networks,an article by the authors of [101] investigate its use in smart contract security and conclude that its use, together with convolutional neural networks positively assist in the encryption of passwords on current systems such that malicious attacks (i.e. DDOS, MITM) are significantly reduced.

2) THE USE OF GAME THEORY

In an article by the authors of [102], they develop, implement and experiment with a framework of a heavy-duty smart contract using game theory which aims to use a select number of processors to carry out the processing of heavy-duty tasks. The use of game theory allows for efficiency in both computational power and security of the smart contract.

C. SELFISH MINING

The concept of selfish mining was first introduced in an article by the authors of [103] in 2013. In this paper, the authors explain that contrary to popular belief, miners or pools of miners can exploit the Bitcoin network and create a centralized ecosystem. This is done by miners who intentionally hold off on publishing mined blocks. Based on this, honest miners are forced to process data on obsolete chains, therefore increasing the selfish miners portion of the mining revenue. This issue has been discussed in depth since an article by the authors of [103] was published. In terms of the use of AI, there are several articles that provide a solution to selfish mining. In an article by the authors of [104], they explore the use of a multi-functional reinforcement learning model to solve complex selfish mining formulated based on the discrete-time stochastic control process called Markov Decision Process (MDP). Based on an experiment carried out by the authors, it was determined that the model could function without prior knowledge of the variables regarding the selfish mining MDP model. In an article by the authors of [105], they focus on the detection of selfish mining. They present a trial-and-error approach to expose selfish mining attacks that use the Proof-of-Work (PoW) consensus algorithm. This is achieved through a data analysis approach to identify the size of transaction confirmations and the production of blocks to the network in order to identify situations when selfish mining is occurring.

D. AI-DRIVEN DECENTRALIZED COORDINATION

AI has the ability to be the talking point between a multitude of different devices based on different technologies. It can enhance the communication between technologies, removing any need for a centralized point of communication and further securing the transfer of data between these devices. In an article by the authors of [106], they refer to this concept by presenting the case of how blockchain technology can be used in conjunction with robotic swarms. In an article by the authors of [107], they explore the use of blockchain technology as a dynamic method to analyze reputation as a unit of measure. The researchers demonstrate this through the use of a data analysis approach to further improve federated learning functions. Furthermore, an article by the authors of [108] propose the use of self-identifying TEE-based confidentiality in smart contracts. This article is specifically targeted in this section due to the fact that a practical prototype system had been developed and tested in order for the authors to arrive at their conclusion.

It is important to explore the use of AI and DLT in the development of The Internet of Things (IOT) as the industry is growing rapidly and there is a lot of promise in the development of specific technologies being able to speak to each other [109]. The Internet of Things refers to physical devices that are connected via the Internet, all collecting and analyzing data in order to produce a real-time result [109]. An example of IOT can range from a single light bulb controlled from a mobile application all the way to full potential smart cities where entire regions are equipped to control aspects such as lighting, traffic, waste management and parking by analyzing the data collected from various sensors, cameras, platforms and other sources [110]. In an article by the authors of [111], a DLT-based AI-enhanced IOT architecture that aims to remove centralized data analysis, security and privacy risks as well allow for larger and more efficient training data for AIs is presented. This is achieved through a DLT-based AI architecture that during their qualitative analysis, indicates higher levels of precision and security while lowering levels of energy waste when compared to other forms of technology (eg: fog computing). As mentioned before, the researchers once again commend the authors in taking a practical approach to the investigation of AI and DLT as an effective and efficient coordination mechanism. A further article by the authors of [112], they investigate the use of DLT and AI in ensuring the security and privacy of communications in the IOT space. They propose a traffic monitoring solution used to remove the collision of data patterns and ensure energy efficiency. In articles by the authors of [113] and [13], they investigate how the convergence of AI and DLT could potentially lead to developments in real world use cases such as smart cities, healthcare, self-driving vehicles, precision farming, and, banking and finance. IOTA launched Tangle in 2016, a directed acyclic graph DLT used to store transaction data securely and provide a scalable decentralized marketplace for Internet of Things device data [114]. However, the drawbacks include the need for persistent storage needs (via permanodes) [115].

E. DLT FAIRNESS

In an article by the authors of [12], the use of AI as a mediator for humans using a DLT of some form is described. AI has the ability to take actions and execute decisions that resolve any issues and track those decisions and their outcomes on chain. The use of AI as a mediator for example, the way humans communicate digitally has been explored. In an article by the authors of [116], the use of AI in the development of "smart" text messages is described. AI would have the ability to identify that a potential conflict may occur based on its analysis of word structure and conversational context and in return propose something to say to the writer. In the realm of AI as a mediator brings a slew of different potential positives such as the ability to communicate better. However, it also brings rise to potential challenges such as user conversation privacy. The more interesting alternative dispute resolution that AI is being used for is that of the arbitrator, specifically in the DLT space. AI could be a better alternative to humans in the arbitration process by being more unbiased, consistent and completely information driven [117]. However, a potential drawback here is that the learning model only operates for pre-programmed voting setups, which results in it being limited in its implementation.

Regarding smart contract fairness, the authors of [118] propose an article that aims to use a machine learning-based voting system that allows participants to vote on several smart contract attributes. Once the votes have been counted, the majority decision is followed, thus directing the overall behaviour of the smart contract. Furthermore, a point to highlight is the ML models analysis of participants' voting history in order to assist them in making future decisions. This is imperative as it helps to make quick decisions in unexpected situations.

F. NON-FUNGIBLE TOKENS

Non-fungible Tokens are a relatively new technology that is using AI to enhance its functionality, product offering and security. In an article by the authors of [119], an AI tool developed by online art community and gallery DeviantArt is investigated. The AI tool presented aims to detect infringements of digital artwork NFTs that do not belong to the original artist. This is achieved by using image recognition machine learning to scan public blockchains and online NFT marketplaces for the same or similar artwork images. Once identified, the tool will alert the artist of the infringement and request that they submit a Digital Millennium Copyright act (DMCA) takedown request to have the NFT removed. It should be noted that there is a need for further research and user acceptance testing to investigate the validity of the solution presented.

Furthermore, an article by the authors of [120] describe Fetch. ai's approach to developing NFTs using AI and machine learning. The tool called Colearn pAInt aims to create a collection of NFTs using AI and machine learning by combining the collective art of up to 100 users. In addition, users who purchase these NFTs will own the underlying AI algorithm and will be entitled to a portion of the proceeds of any artworks produced by the algorithm.

G. DECENTRALIZED FINANCE

In an article by the authors of [121], BlockBank, an AI-enhanced DeFi platform, is presented. The application aims to enhance the trades made by the users through the guidance of an AI-powered bot that analyses real-time trading and social media activity to make informed trading strategy predictions.

Furthermore, in an article by the authors of [122], an AI-powered DeFi cryptocurrency portfolio management platform is presented. Users of the platform make use of Dynamic Asset Sets (DynaSet) where AI is utilized to dynamically balance and manage a portfolio of cryptocurrency utility tokens. The AI algorithm manages the ratio of the DynaSet via trustless smart contracts, executing trades on Uniswap, a noncustodial decentralized exchange.

H. DECENTRALIZED EXCHANGES

In an article by the authors of [123], a permissionless Solana-based decentralized exchange (DEX) tool is presented where AI is implemented together with underlying smart contracts and blockchain-based data oracles to assist users in their trading activities. The tool "Soldex" makes use of a neural network algorithm that gathers and analyzes asset prices and movements to present users with an array of various trading strategies.

I. DECENTRALIZED AUTONOMOUS ORGANIZATION

An AI-enhanced Decentralized Autonomous Organization (DAO) is presented in an article by the authors of [124]. Through the use of adaptive ML and feedback loops, the DAO presented aims to automate all human-based administrative functionalities and have AI autonomously execute decisions based on the data it is given. An interesting use case presented focuses on marketing strategies that are developed, evaluated and maintained by an AI functionality. An AI algorithm would generate and place advertisements, evaluate its return on investment (ROI) and adjust the overall marketing strategy accordingly using feedback loops thus not requiring the need for human interaction.

J. BLOCKCHAIN ORACLES

The trustworthiness of external data is currently a problem associated with blockchain oracles with the validity of information residing with the party inputting the data [125]. In article by the authors of [126], an AI-based blockchain oracle is presented to solve this problem. Through the use of decentralized narrow AI, smart contract decision making would be transparent and immutable based on the interpretation and validation of external data. Furthermore, several other AI functionalities could be used in various use cases, such as image recognition being used to validate insurance claims.

VI. COMPARISON AND DISCUSSION

The above two sections presented a systematic analysis and review of the current state of research on the convergence of DLT and AI. The current state of research on their convergence is largely limited to scientific research. In addition, the strengths, weaknesses, and overall characteristics of the two technologies differ substantially. One of the aims of AI is to extract, interpret, and analyze large quantities of data. This is currently performed using centralized servers which poses a risk for abusive hacking and exploitation. The design of DLT on the other hand provides a consensus-based decentralized ledger that enhances the security of digital data. However, it does not provide for the deep analysis of data like AI does. Therefore, the theoretical integration of both technologies would harness each other's strengths and provide the capabilities to solve their weaknesses. AI could potentially enhance DLT performance and governance, while DLT could provide improved data security, privacy and increase the overall performance of the AI in question.

By reviewing current literature, in terms of the impact of AI for DLT, there are subsections with varying levels of real world use case practicality. Investigation into alternative consensus algorithms (i.e. Proof-of-Deep Learning and Proof-of-Kernel Work) show this. Proof-of-Kernel Work is explored through a practical real world use case by improving blockchain-powered hybrid Porsche vehicles. On the other hand, Proof-of-Deep Learning is a conceptual idea and requires fundamental research in order to create a foundation for practical implementation. Furthermore, a review of research indicates security and governance advantages over smart contract data, specifically in Ethereum smart contracts. Furthermore, a focus is placed on IOTAs Tangle, an alternative to blockchain DLTs and its advantage of scalability in the development of a data marketplace for IOT devices. However, further research is required as this DLT poses a risk of persistent storage needs due to permanodes. Therefore, either further research into how to navigate past this disadvantage is needed or a focus needs to be placed on alternative DLT solutions. Finally, the use of AI in NFTs is explored with a practical solution developed to assist in identifying digital artwork NFT infringements.

TABLE 2. Review of DLT for AI.

Category	Findings	DLT Used	Strength	Drawback
Decentralized Federated AI [65], [9], [67], [68]	Using nodes/aggregated nodes participating in a decentralized network and responsible for training AI-based ML models [9], [67].	Blockchain	Reducing the risk of privacy exploitation.	Limited performance overhead of up to 15 percent for federated learning models.
Trusted Execution Environments [69], [70], [71], [72], [73]	DLT-based off-chain payment channels setup in TEEs to secure transactions between parties [70], [72].	Blockchain (Hyperledger Fabric)	Data security and privacy.	Extent of the trustworthiness of the TEE is at the mercy of the hardware manufacturer.
Differential Privacy [75], [74], [76]	Aims to incorporate randomly generated noise into algorithms to lessen the risk of privacy issues by malicious third parties [76].	Blockchain (Quorom)	Self-controlled private data sharing.	Does not focus on query-related data sharing.
Explainable AI [77], [9], [67], [78], [12], [79]	The development of AGI (Artificial General Intelligence) progression using DLT encryption, specifically smart contracts, as a more efficient alternative to human-based monitoring.	Blockchain (via Smart Contracts)	Audit trail of component usage stored via DLT.	AI data pattern control systems need to be developed and tested in a transparent, non-hackable simulation.
Smart contract-based AIs [9], [80], [81], [82], [83], [84], [85], [86]	The use of smart contract-based AIs to transport pieces of software which would be free from bugs and loopholes.	Blockchain (via Smart Contracts)	It can be scaled off-chain while simultaneously maintaining high levels of data integrity.	Can be implemented in Ethereum smart contracts, but not in other blockchains and/or DLTs without modification to the original scripting system.
Data markets and staking-based data sharing [87], [11]	The development of DLT-based (using Ethereum ERC20 wallets) data marketplaces where publishing and consuming data is tokenized.	Blockchain (via Smart Contracts)	Individual users can monetize their private data and smaller players in the field of AI system development could gain more high-quality and quantities of data.	Data is only gained if the individual users trust in the system is enough to warrant providing their personal data.
Parachains [88], [11], [89]	The use of parachain networks to transfer data across blockchain networks. This could be used to easily transfer data into AI models situated on various blockchains.	Parachains (Blockchain Technology	Data privacy, blockchain interoperability.	The need for further research into the development of parachains and bridging to other blockchain technologies/DLTs is required.
Decentralized Neural Networks [91], [90]	The use of blockchain technology to lower the cost of processing AI algorithms and improve performance.	Blockchain Technology	AI processing costs,increased performance and blockchain interoperability.	The need for further testing around more randomized-based neural networks.
Internet of Things [127], [92], [93], [94], [128]	The use of blockchain technology to increase overall improvement, ensure security and privacy and reduce delay, response time and latency of IoT networks.	Blockchain Technology	Increased performance, security and privacy while reducing delay, response time and latency.	The need for further testing of blockchain technology within larger IoT networks.
5G Technology [95]	The use of blockchain technology in conjunction with AI to simplify traditional 5G network processes and improve efficiency.	Blockchain Technology	20 percent decrease in energy consumption at the RAN level.	As 5G technology is relatively new, there is a need for further testing of blockchain technology within 5G networks.

However, further research into the viability and effectiveness of this solution is required.

As in the case of DLTs impact in AI, the advantages mentioned in all subsections are highly centered around AI data security and privacy, in addition to giving power to the individual over how their data is utilized when incorporated into AI models. The section is divided into areas where current research is not mature enough to warrant practicality and user acceptance while other areas are further advanced. Trusted Execution Environments, for example, is a topic that incorporates a technology already well established and used (i.e. in cellphones). Furthermore, research focuses on real world use case applications developed and tested by large, well known entities (i.e. LucidiTEE by Visa). This TEE-based blockchain system is developed and tested for transferring hypersensitive data across a multitude of different parties. This development is an addition to the overall potential possibility of real-world implementation and adoption. However, in saying this there are other fields where fundamental research is still required. Explainable AI, for example is a complex topic that requires thorough research and analysis. Furthermore, DLT-based solutions are currently altogether (i.e.Development of AGI progression using DLT encryption). Regarding parachains, a practical use case is presented in the research but is limited in that the concept of parachains is fairly new and further research is required into understanding the viability of the solution. This thinking can be used across the entire literature review as the testing via a use case may have been completed but the practicality of a fully fledged and mass adopted solution requires additional research to be completed.

As a whole, both the use of DLT in AI and AI for DLT are exciting fields that present a good case for future research. The individual technologies of AI and DLT are useful alone and research in this field indicates that they could be useful when converged together. Future research topics are explored in the next section.

VII. APPLICATIONS AND USE CASES

In this section, current applications and use cases spanning various industries will be discussed.

A. HEALTHCARE

In an article by the authors of [129], the impact of blockchain technology on the healthcare industry is explored and discussed. Blockchain technology offers various benefits such as decentralized storage, security, privacy as well as being tamper-proof. However, the healthcare industry requires strict control over the authenticating and record sharing of patient data. Therefore, a subset of researchers from academia and industry have focused on developing applications and architectures to cater for the healthcare industry.

In an article by the authors of [130], a blockchain-based record storage and sharing application called Medicalchain is presented. The application allows patients to share their medical records with specific healthcare professionals. Furthermore, any interactions of this data is recorded in an immutable and transparent manner on Medicalchain's private ledger. Medicalchain is not just a single application but also a blockchain ecosystem that allows developers to build upon it. Developers can create smart contracts that when executed, analyze patient data and output an opinion such as which diet is best to follow. Medicalchain has been officially launched and is currently in use in several hospitals in the United Kingdom.

In an article by the authors of [131], a use case for a medical drug supply chain is presented. The current medical drug supply chain suffers from various complex and inefficient processes and the risk of counterfeit products is still a major concern. Due to the nature of blockchain technology and its ability to keep an immutable and transparent record of data and information, its application to the medical drug supply chain industry is highly applicable. The solution is currently theoretical and the need for a practical blockchain framework with a transaction verifying process is presented.

The applications and use cases presented above satisfy various requirements specific to the healthcare industry. However, there are still several risks that need to be addressed, such as mining attacks. In addition, there are several requirements specific to the healthcare industry that are not yet explored through the blockchain technology applications presented.

B. 5G TECHNOLOGY

In an article by the authors of [95], a comprehensive intelligence and secure data analytic framework is presented for 5G technology that incorporates a convergence of blockchain technology and AI. The framework, named "Block5GIntell" is successfully compared to other traditional alternatives with a resulting energy consumption reduction of 20 percent at the RAN level.

Furthermore, in an article by the authors of [132], a healthcare centered context-aware blockchain-based model is presented with the aim of encrypting data among various nodes within the architecture of a 5G network. The proposed model was evaluated against various evaluation metrics and outperformed in comparison to alternative solutions.

C. INTERNET OF THINGS

In an article by the authors of [127], a blockchain-based smart home gateway architecture is presented with the aim of preventing data forgery. Currently, the connections between Internet of Things devices are maintained centrally, thus presenting various security vulnerabilities. The solution presented uses blockchain technology in the gateway layer between device and the cloud layer to ensure data integrity and security. Based on the evaluation performed, the implemented solution outperformed other existing methods. Smart cities are also impacted from the development of the Internet of Things.

An article by the authors of [128] present a comprehensive literature review of the various security issues affecting the integration of blockchain technology into smart cities. Multiple solutions are explored with a specific focus on the development of blockchain-AI based intelligent transportation systems. In article by the authors of [133], a blockchain-based real-time ride-sharing service is presented as a potential use case. The application aims to achieve accurate matching by representing the ride share area as multiple overlapping grids so users can find and share the same rides. Furthermore, privacy is maintained through the encrypting of offers and requests. Through an evaluation performed, the application requires low communication and computation overheads.

D. SUPPLY CHAIN

In an article by the authors of [134], a blockchain-based circular economy model is presented. This model follows

TABLE 3. Review of AI for DLT.

Category	Findings	DLT Used	Strength	Drawback
AI-based consensus algorithms [2], [96], [10], [97]	A proof-of-concept design that harnesses and recycles blockchain computational energy and re-invests it back into the execution of deep learning models.	Blockchain	Saving computational energy.	Malicious requesters and miners are able to generalize the model requestor.
AI-enhanced smart contract security [98], [99], [14], [100], [101], [102]	Using AI data analysis techniques to detect smart contract transaction behaviour.	Blockchain (via Smart Contracts)	The detection of honeypots and other malicious agents based on known and unknown techniques.	Inability to identify contracts or accounts with larger transactions and place it into categories that do not involve honeypots.
Selfish mining [103], [104], [105]	The use of a multi-functional reinforcement learning model to solve complex selfish mining formulated based on the discrete-time stochastic control process called Markov Decision Process (MDP).	Blockchain	Identify the size of transaction confirmations and the production of blocks to the network in order to identify situations when selfish mining is occurring.	Detection of selfish mining through a trial-and-error approach using the proof-of-work (PoW) consensus algorithm can lead to computational energy wastage.
AI-driven decentralized coordination [106], [107], [108], [109], [110], [111], [112], [113], [13], [114], [115]	Store transaction data securely and provide a scalable decentralized marketplace for Internet of Things device data.	DAG (IOTA - Tangle)	Scalability.	The need for persistent storage needs (via permanodes).
DLT Fairness [12], [116], [117], [118]	Using a machine learning-based voting system that allows participants to vote on several smart contract attributes that directs the overall behaviour of the smart contract.	Blockchain (via Smart Contracts)	Governance over smart contract data.	Learning model only operates for pre-programmed voting setups, which results in it being limited in its implementation.
Non-fungible Tokens [119], [120]	Using AI to detect infringements of digital artwork NFTs.	Blockchain (via NFTs)	Governance over NFT data.	There is a need for further research and user acceptance testing to investigate the validity of the solution.
Decentralized Finance [121], [122]	Development of an AI-powered bot that analyses real-time trading and social media activity to make informed trading strategy predictions.	Blockchain (via Smart Contracts)	AI-based trading advice.	There is a need for further research and user acceptance testing to investigate the validity of the solution.
Decentralized Exchanges [123]	AI is implemented together with underlying smart contracts and blokchain-based data oracles to assist users in their trading activities.	Blockchain (via Smart Contracts)	AI-based trading advice.	There is a need for further research and user acceptance testing to investigate the validity of the solution.
Decentralized Autonomous Organization [124]	DAO utilizing adaptive ML and feedback loops to automate administrative functionalities and perform autonomous decision making.	Blockchain (via Smart Contracts)	AI-based execution of administrative functionalities and decision making.	There is a need for further research and user acceptance testing to investigate the validity of the solution.
Blockchain Oracles [125], [126]	Using decentralized narrow AI to make smart contract decision making transparent and immutable based on validation of external data.	Blockchain (via Smart Contracts)	Solving problem associated with validating off-chain blockchain data.	There is a need for further research to investigate the validity of the solution in solving the blockchain oracle problem presented.

the process flow of make, use and recycle which replaces the current take, make and dispose supply chain model. Through the use of blockchain technology, products can be traced from their production origin to their sale or recycling. Furthermore, customers purchasing these products have full access to the products history therefore knowing its origin and whether or not the product was recycled.

In an article by the authors of [135], supply chain management within the medical industry is explored through the use of AI-enhanced medical drone application in Ghana's healthcare supply chain. Results from this study found that sustainable development goals were achieved such as a reduction in carbon emissions. In addition, socio-economic advantages were identified such as a reduction of mortality rates, thus leading to improved social and economic livelihood for citizens.

VIII. RESEARCH GAPS AND FUTURE DIRECTION

In this section, the strengths, weaknesses and trends in each subsection of the literature review are explored and as a result, future research topics are presented.

A. DLT FOR AI

1) EXPLAINABLE AI

DLT offers a solution to the AI black box problem by providing a transparent and secure ledger on which AI metadata, stemming from various training models, could sit. Furthermore, DLT can be used to host XAI applications in both an on-chain and off-chain situation. This addition to current XAI models could allow for increased levels of security and reliability of the AI going forward. Based on current research, basic AI models are being deployed on a distributed ledger of some kind, however in order for larger, more complex AI models to be placed on DLT, further research and development is required. A potential solution, as proposed by the authors of [78] investigates the use of trusted execution environments to analyse complex private data in an effective and efficient manner. A demonstration is shown using a sample of patient healthcare data but the idea of using trusted hardware (in this case TEEs) to execute machine learning models via DLT is a future research topic.

2) DATA MARKETS AND STAKING-BASED DATA SHARING

There are many advantages in tokenizing data on a DLT-based marketplace so that it can be traded securely and efficiently. In addition, it also creates an economic incentive for individuals to share their data, thus generating more diverse data sets for AI models to consume [9]. There are many articles discussing various technical solutions in this field [136], [114] and [137]. However, the topic of how to best build tokenized marketplaces and economies remains as a research topic to be investigated. Furthermore, an article by the authors of [138] mention the potential disadvantage of incentivizing individuals to share their data. They present a case that individuals could be economically motivated to share their data and therefore, not make informed decisions as to what they are really sharing and with what entity. This further builds onto the previous future research in how tokenized data marketplaces could be built [138]. Finally, there exists a future research question relating to the tokenizing of AI assets (i.e. training data, algorithms and models). There exists research in articles by the authors of [139] but further development into how to execute this process more effectively and efficiently, with the most upside and the least risks to personal data needs to be further researched.

3) DECENTRALIZED FEDERATED AI

Articles by the authors of [14] and [12] mention the use of DLT to organise federated AI models so that no input data is shared among participants and instead, nodes are the actors within the federated environment. The use of DLT-based federated AI models could potentially ensure privacy and security of data, however further research is still required in order for this concept to be executed in real-world use cases. As mentioned in the literature review section of this paper, there exists limitations in this field. An article by the authors of [67] explores the disadvantage DLT presents with regards to federated AI's in comparison to traditional machine learning models. It is determined that the introduction of DLT brings with it a limited performance overhead of up to 15 percent for federated learning models. Future research is therefore required in order to identify ways in which performance overhead can be reduced for real-world use cases. In addition to the technical future research topic proposed, there exists a need for non-technical future research to be investigated. It is currently unclear whether the potential guarantees of increased privacy and security from DLT-based federated learning models will encourage individuals to become more willing to share their data with AI models. Furthermore, as discussed in the previous section, a tokenized economy with data incentives will still have to be efficiently and effectively developed in order for data to be gathered for DLT-based federated learning models.

B. AI FOR DLT

1) DLT FAIRNESS

The use of AI-based DLT protocol security and smart contract security has been researched in the literature review section of this paper. However, a future research topic presents itself with a focus on AIs capabilities to govern DLT protocols and smart contracts. The current development of the reliability and explainability of AI is not sufficient to justify that it will operate as expected when brought together with DLT [140]. Therefore, further research is required into the reliability, trustworthiness, security and overall operations and explainability of AI before it can be used to govern DLT protocols and smart contracts.

2) AI-BASED CONSENSUS ALGORITHMS

The article by the authors of [10] present the 'Proof-of-Deep Learning' consensus algorithm which aims to recycle blockchain energy and have miners execute deep learning training tasks instead of processing hash calculations. The design presented holds a lot of potential but is still a novel idea in its early stages of development and is without any real world use case implementation. As mentioned in the article, the model requester could become universal to multiple malicious requesters who may conspire with miners.

Therefore, more focus needs to be placed on identifying patterns of realistic block submissions and investigating more deep learning training sets. This presents a future research opportunity to further develop the Proof-of-Deep Learning consensus algorithm.

3) AI-DRIVEN DECENTRALIZED COORDINATION

Articles in the literature review section of this paper investigate how the convergence of AI and DLT can lead to potential improvements in privacy and security while simultaneously lowering energy consumption and waste. However, the majority of these articles are concepts and have not been implemented into real world use cases. Furthermore, regarding challenges relating to IOT such as security, privacy and scalability need to be further investigated and explored in order for complete practical solutions to be developed and implemented [111].

4) SELFISH MINING

In an article by the authors of [104], they propose a potential solution to solving the Markov Decision Process (MDP) problem using multi-functional reinforcement learning models. However, per the article, future research is required in order for this solution to be completely developed. A focus on incorporating more DLT (in this case the Bitcoin blockchain) features such as stale block rate. Furthermore, a focus needs to be placed on increasing the speed of convergence of the mining algorithm proposed in order to make it as economical as possible. This could potentially be achieved through a focus on deep reinforcement learning models.

5) NON-FUNGIBLE TOKENS

In article by the authors of [119], an AI tool is presented with the goal of assisting in the detection of infringements in digital artwork NFTs. This is achieved through the use of image recognition machine learning to scan public blockchains and online NFT marketplaces for the same or similar artwork images. Due to this solution being relatively new, further research into its viability and effectiveness is required. In addition, the use of AI can be leveraged and combined with other technologies, such as verifiable credentials, to assist in the validation and ownership of underlying data assets within NFTs.

IX. CONCLUSION

In this paper, the researchers investigated the current state of literature as presented by the authors of [14], in addition to identifying new research streams within the convergence of DLT and AI. Furthermore, several future research topics on the convergence of DLT and AI are also presented. Both technologies are currently trending and their convergence offers realistic benefits in various sectors. In addition, progressive developments indicate a new wave of opportunity may exist to be taken advantage of in this sector. The literature review section was divided into two parts, each making AI or DLT the dependent and independent variable. In terms of the advantages AI can bring to DLT, the researchers analysis highlighted literature regarding developments of innovative AI-based consensus protocols, ways to further enhance smart contract security and device coordination, potential solutions to malicious mining, ensuring fairness exists in the DLT space and the identification of fraudulent digital assets. On the other hand, DLT could aid AI by providing potential solutions to explainable AI, developments of AI data markets and presenting various solutions to ensure AI data privacy and scalability. In order to develop a future research agenda, the researchers aimed to use the literature review as a foundation and selected key sub sections believed to be filled with opportunity. The results indicated that both theoretical and practical advances in the convergence of AI and DLT exist, with specific focus placed on the subsections of explainable AI, data markets, decentralized federated AI, DLT fairness, AI consensus algorithms, DLT-based device coordination and NFTs. The researchers believe this paper provided an understanding and meaningful insights into the convergence of DLT and AI. Together with a focus on developments in this emerging field, it helps to add to the body of knowledge and analysis that currently exists.

REFERENCES

[1] A. M. Turing, “Computing machinery and intelligence,” in *Parsing the Turing Test*. Dordrecht, The Netherlands: Springer, 2009, pp. 23–65.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Bitcoin Foundation, Boston, MA, USA, Tech. Rep. 1, 2009.

[3] S. Russell and P. Norvig, “Artificial intelligence: A modern approach,” Prentice-Hall, Upper Saddle River, NJ, USA, Tech. Rep. 4, 2002.

[4] G. Lugano, “Virtual assistants and self-driving cars,” in *Proc. 15th Int. Conf. ITS Telecommun. (ITST)*, May 2017, pp. 1–5.

[5] S. Paliwal, V. Bharti, and A. K. Mishra, “AI chatbots: Transforming the digital world,” in *Recent Trends and Advances in Artificial Intelligence and Internet of Things*. Cham, Switzerland: Springer, 2020, pp. 455–482.

[6] T. R. Weiss. *IDC: AI Spending Expected to Double Globally to 110b by 2024*. Enterprise AI. Accessed: Dec. 15, 2021. [Online]. Available: https://www.enterpriseai.news/2020/08/28/idc-ai-spending-expected-to-double-globally-to-110b-by-2024/

[7] P. G.-P. E. Benos and R. Garratt. (Aug. 1, 2017). *Staff Working Paper no. 670, the Economics of Distributed Ledger Technology for Securities Settlement*. Bank of England. [Online]. Available: https://www.bankofengland.co.U.K./-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf

[8] World Economic Forum. *Deep Shift Technology Tipping Points and Societal Impact*. Accessed: Dec. 15, 2021. [Online]. Available: https://www.weforum.org/reports/deep-shift-technology-tipping-points-and-societal-impact

[9] S. Thiebes, S. Lins, and A. Sunyaev, “Trustworthy artificial intelligence,” *Electron. Markets*, vol. 31, pp. 1–18, Oct. 2020.

[10] C. Chenli, B. Li, Y. Shi, and T. Jung, “Energy-recycling blockchain with proof-of-deep-learning,” in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 19–23.

[11] *Ocean Protocol: Tools for the Web3 Data Economy*, Ocean Protocol Found., Singapore, 2020.

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

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

[14] K. D. Pandl, S. Thiebes, M. Schmidt-Kraepelin, and A. Sunyaev, “On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda,” *IEEE Access*, vol. 8, pp. 57075–57095, 2020.

[15] M. Rauchs, A. Glidden, B. Gordon, G. C. Pieters, M. Recanatini, F. Rostand, K. Vagneur, and B. Z. Zhang, "Distributed ledger technology systems: A conceptual framework," SSRN, New York, NY, USA, Tech. Rep. 1, 2018.

[16] H. Natarajan, S. K. Krause, and H. L. Gradstein, "Distributed ledger technology (DLT) and blockchain. world bank group," Fintech Note, Washington, DC, USA, Tech. Rep. 1, 2017.

[17] *Hyperledger Fabric*. Accessed: Dec. 15, 2021. [Online]. Available: https://www.hyperledger.org/use/fabric

[18] *Consensys Quorum*. Accessed: Dec. 15, 2021. [Online]. Available: https://consensys.net/quorum/

[19] *What is Blockchain Technology?*. IBM. Accessed: Dec. 15, 20201. [Online]. Available: https://www.ibm.com/za-en/topics/what-is-blockchain

[20] S. Wilkinson and J. Lowry, "Metadisk a blockchain-based decentralized file storage application," Semantic Scholar, Washington, DC, USA, Tech. Rep. 1, 2014.

[21] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," in *Proc. 12th Student Conf. Managerial Sci. Technol.*, 2015, pp. 1–8.

[22] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annu. Int. Conf. theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2015, pp. 281–310.

[23] A. Saad and S. Y. Park, "Decentralized directed acyclic graph based DLT network," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 158–163.

[24] S. Popov and Q. Lu, "IOTA: Feeless and free," IEEE Blockchain Tech. Briefs, New York, NY, USA, Tech. Rep. 1, 2019.

[25] E. Harris-Braun, N. Luck, and A. Brock. (2018). *Holochain. Scalable Agent-Centric Distributed Computing*. DRAFT (ALPHA 1)-2/15/2018. [Online]. Available: https://whitepaperdatabase. com/wp-content/uploads/2018/08/holochain-HOT-whitepaper.pdf

[26] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K.-R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102471.

[27] B. N. Musungate, B. Candan, U. C. Cabuk, and G. Dalkilic, "Sidechains: Highlights and challenges," in *Proc. Innov. Intell. Syst. Appl. Conf. (ASYU)*, Oct. 2019, pp. 1–5.

[28] D. Ramos and G. Zanko, "An analysis of polkadot as an initiative for inter-communication between multiple blockchains," MobileyourLife, Bogotá, Colombia, Tech. Rep. 1, 2020.

[29] R. Habermeier. *What is a Parachain?*. Acala Network. Accessed: Dec. 15, 2021. [Online]. Available: https://acala.discourse.group/t/what-is-a-parachain/46

[30] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," Polkadot, Cham, Switzerland, White Paper 1, 2016.

[31] A. S. B. Laboon and F. Shirazi, "Blockchain interoperability (part 3): Polkadot," Seba Bank, Cham, Switerland, Tech. Rep. 1, 2021.

[32] L. M. *What is a Smart Contract and how Does it Work?*. Bitdegree. Accessed: Jan. 18, 2022. [Online]. Available: https://www.bitdegree.org/crypto/tutorials/what-is-a-smart-contract

[33] S. D. Levi and A. B. Lipton, "An introduction to smart contracts and their potential and inherent limitations," in *Harvard Law School Forum Corporate Governance & Financial Regulation*. Boston, MA, USA: Harvard, 2018.

[34] J. Liebkind. *4 Blockchain Contenders in Competition With Ethereum*. Investopedia. [Online]. Available: https://www.investopedia.com/news/4-blockchain-contenders-competition-ethereum/

[35] K. B. Muthe, K. Sharma, and K. E. N. Sri, "A blockchain based decentralized computing and NFT infrastructure for game networks," in *Proc. 2nd Int. Conf. Blockchain Comput. Appl. (BCCA)*, Nov. 2020, pp. 73–77.

[36] L. Liu, S. Zhou, H. Huang, and Z. Zheng, "From technology to society: An overview of blockchain-based DAO," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 204–215, 2021.

[37] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner, and B. Schlosser, "DeFi-ning DeFi: Challenges pathway," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2021, pp. 181–184.

[38] Coinbase. *What is a DEX*. Accessed: Jan. 18, 2022. [Online]. Available: https://www.coinbase.com/learn/crypto-basics/what-is-a-dex

[39] Binance. *Blockchain Oracles Explained*. Accessed: Jan. 18, 2022. [Online]. Available: https://academy.binance.com/en/articles/blockchain-oracles-explained

[40] P. Winston. *What is Artificial Intelligence?*. Builtin. Accessed: Jan. 18, 2022. [Online]. Available: https://builtin.com/artificial-intelligence

[41] D. Abele and S. D'Onofrio, *Artificial Intelligence—The Big Picture*. Wiesbaden, Germany: Springer, 2020, pp. 31–65.

[42] N. J. Nilsson and N. J. Nilsson, *Artificial Intelligence: A New Synthesis*. San Mateo, CA, USA: Morgan Kaufmann, 1998.

[43] *Deep Blue*. Accessed: Jan. 18, 2022. [Online]. Available: https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/

[44] E. Ismagilova, L. Hughes, Y. K. Dwivedi, and K. R. Raman, "Smart cities: Advances in research—An information systems perspective," *Int. J. Inf. Manage.*, vol. 47, pp. 88–100, Aug. 2019.

[45] H. Hodson. (Mar. 1, 2019). *Deepmind and Google: The Battle to Control Artificial Intelligence*. The Economist. [Online]. Available: https://www.economist.com/1843/2019/03/01/deepmind-and-google-the-battle-to-control-artificial-intelligence

[46] S. Russell and P. Norvig, "AI a modern approach," *Learning*, vol. 2, no. 3, p. 4, 2005.

[47] A. Jaswal. *How AI can Change the Face of Web Development?*. Signity. Accessed: Jan. 18, 2022. [Online]. Available: https://www.signitysolutions.com/blog/ai-change-web-development/

[48] R. Chatila, E. Renaudo, M. Andries, R.-O. Chavez-Garcia, P. Luce-Vayrac, R. Gottstein, R. Alami, A. Clodic, S. Devin, B. Girard, and M. Khamassi, "Toward self-aware robots," *Frontiers Robot. AI*, vol. 5, p. 88, Aug. 2018.

[49] W. Naudé and N. Dimitri, "The race for an artificial general intelligence: Implications for public policy," *AI Soc.*, vol. 35, no. 2, pp. 367–379, Jun. 2020.

[50] IBM. *IBM Watson is AI for Smarter Business*. Accessed: Jan. 18, 2022. [Online]. Available: https://www.ibm.com/watson

[51] J. Page, M. Bain, and F. Mukhlish, "The risks of low level narrow artificial intelligence," in *Proc. IEEE Int. Conf. Intell. Saf. Robot. (ISR)*, Aug. 2018, pp. 1–6.

[52] Y. LeCun, Y. Bengio, and G. E. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, Dec. 2015.

[53] Expert.AI. *What is Machine Learning? a Definition*. Accessed: Jan. 18, 2022. [Online]. Available: https://www.expert.ai/blog/machine-learning-definition/

[54] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, Jul. 2015.

[55] (Aug. 19, 2020). IBM Cloud Learn Hub. *Supervised Learning*. [Online]. Available: https://www.ibm.com/cloud/learn/supervised-learning

[56] F. Osisanwo, J. Akinsola, O. Awodele, J. Hinmikaiye, O. Olakanmi, and J. Akinjobi, "Supervised machine learning algorithms: Classification and comparison," *Int. J. Comput. Trends Technol.*, vol. 48, no. 3, pp. 128–138, Jun. 2017.

[57] R. Gandhi. (May 27, 2018). *Introduction to Machine Learning Algorithms: Linear Regression*. Towards Data Science. [Online]. Available: https://towardsdatascience.com/introduction-to-machine-learning-algorithms-linear-regression-14c4e325882a

[58] A. Kassambara, *Practical Guide to Cluster Analysis in R: Unsupervised Machine Learning*, vol. 1. New York, NY, USA: STHDA, 2017.

[59] (Sep. 21, 2020). IBM Cloud Learn Hub. *Unsupervised Learning*. [Online]. Available: https://www.ibm.com/cloud/learn/unsupervised-learning

[60] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 2018.

[61] K. B. B. Osinski. *What is Reinforcement Learning? The Complete Guide*. (Jul. 5, 2018). [Online]. Available: https://deepsense.ai/what-is-reinforcement-learning-the-complete-guide/

[62] Netflix. *How Netflix's Recommendations System Works*. Accessed: Jan. 18, 2022. [Online]. Available: https://help.netflix.com/en/node/100639

[63] A. Ma. *Everyone is Talking About Cambridge Analytica, the Trump-Linked Data Firm That Harvested 50 Million Facebook Profiles—Here's What's Going on*. Business Insider. (Mar. 19, 2018). [Online]. Available: https://www.businessinsider.co.za/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3?r=U.S.&I% R=T

[64] *Basic Attention Token (BAT)*, Brave Softw., San Fransisco, CA, USA, 2021.

[65] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," 2019, *arXiv:1902.01046*.

[66] L. D. Nguyen, S. R. Pandey, S. Beatriz, A. Broering, and P. Popovski, "A marketplace for trading AI models based on blockchain and incentives for IoT data," 2021, *arXiv:2112.02870*.

[67] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen, and E. Ilie-Zudor, "Chained anomaly detection models for federated learning: An intrusion detection case study," *Appl. Sci.*, vol. 8, no. 12, p. 2663, 2018.

[68] J. Passerat-Palmbach, T. Farnan, R. Miller, M. S. Gross, H. L. Flannery, and B. Gleim, "A blockchain-orchestrated federated learning architecture for healthcare consortia," 2019, *arXiv:1910.12603*.

[69] J.-E. Ekberg, K. Kostiainen, and N. Asokan, "The untapped potential of trusted execution environments on mobile devices," *IEEE Secur. Privacy*, vol. 12, no. 4, pp. 29–37, Jul. 2014.

[70] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, "Teechain: A secure payment network with asynchronous blockchain access," in *Proc. 27th ACM Symp. Operating Syst. Princ.*, 2019, pp. 63–79.

[71] R. Sinha, S. Gaddam, and R. Kumaresan, "Luciditee: A tee-blockchain system for policy-compliant multiparty computation with fairness," Semantic Scholar, Washington, DC, USA, Tech. Rep. 2019/178, 2020.

[72] M. Brandenburger, C. Cachin, R. Kapitza, and A. Sorniotti, "Blockchain and trusted computing: Problems, pitfalls, and a solution for hyperledger fabric," 2018, *arXiv:1805.08541*.

[73] (Oct. 16, 2019). Hyperledger. *Introducing Hyperledger Avalon*. [Online]. Available: https://www.hyperledger.org/blog/2019/10/03/introducing-hyperledger-avalon

[74] J. Bennett and S. Lanning, "The Netflix prize," in *Proc. KDD Cup Workshop*, 2007, p. 35.

[75] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[76] X. Dong, B. Guo, Y. Shen, X. Duan, Y. Shen, and H. Zhang, "A self-controllable and balanced data sharing model," *IEEE Access*, vol. 7, pp. 103275–103290, 2019.

[77] A. Rai, "Explainable AI: From black box to glass box," *J. Acad. Marketing Sci.*, vol. 48, no. 1, pp. 137–141, Jan. 2020.

[78] N. Hynes, D. Dao, D. Yan, R. Cheng, and D. Song, "A demonstration of sterling: A privacy-preserving data marketplace," in *Proc. VLDB Endowment*, vol. 11, no. 12, pp. 2086–2089, Aug. 2018, doi: 10.14778/3229863.3236266.

[79] K. W. Carlson, "Safe artificial general intelligence via distributed ledger technology," *Big Data Cognit. Comput.*, vol. 3, no. 3, p. 40, Jul. 2019.

[80] J. Eberhardt and J. Heiss, "Off-chaining models and approaches to off-chain computations," in *Proc. 2nd Workshop Scalable Resilient Infrastructures Distrib. Ledgers*, 2018, pp. 7–12.

[81] B. Xing and T. Marwala, "The synergy of blockchain and artificial intelligence," SSRN, New York, NY, USA, Tech. Rep. 1, 2018.

[82] H. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, pp. 41596–41606, 2019.

[83] A. Sarkar and S. K. Ray, "Smart contract-based electric vehicle charging: A practice-based economy of things application," Pacific Asia Conf. Inf. Syst., Dubai, United Arab Emirates, Tech. Rep. 72, 2020.

[84] J. A. Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network," *Appl. Sci.*, vol. 9, no. 15, p. 2953, Jul. 2019.

[85] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, "Sprites and state channels: Payment networks that go faster than lightning," in *Proc. Int. Conf. Financial Cryptography Data Secur.* Paris, France: Springer, 2019, pp. 508–526.

[86] J. Teutsch and C. Reitwießner, "A scalable verification solution for blockchains," 2019, *arXiv:1908.04756*.

[87] W. Pang. (Nov. 17, 2019). *How to ensure data quality for AI*. Inside Big Data. [Online]. Available: https://insidebigdata.com/2019/11/17/how-to-ensure-data-quality-for-ai/

[88] M. Docs. *Cross-Chain Integration Plans*. Moonbeam. Accessed: Feb. 3, 2022. [Online]. Available: https://docs.moonbeam.network/learn/xchain-plans/

[89] V. Chawla. *Moonbeam Will Link Ocean Protocol and Polkadot*. Crypto Briefing. Accessed: Feb. 3, 2022. [Online]. Available: https://cryptobriefing.com/moonbeam-will-link-ocean-protocol-and-polkadot/

[90] D. Chain. *Deepbrain Chain Whitepaper*. Accessed: Feb. 3, 2022. [Online]. Available: https://www.deepbrainchain.org/assets/pdf/DeepBrainChainWhitepaper

[91] X. Liang, A. M. Javid, M. Skoglund, and S. Chatterjee, "Decentralized learning of randomization-based neural networks with centralized equivalence," *Appl. Soft Comput.*, vol. 115, Jan. 2022, Art. no. 108030. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1568494621009522

[92] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain technology toward green IoT: Opportunities and challenges," *IEEE Netw.*, vol. 34, no. 4, pp. 263–269, Jul. 2020.

[93] S. R. Niya, E. Schiller, and B. Stiller, *Architectures for Blockchain-IoT Integration*. Hoboken, NJ, USA: Wiley, 2021, pp. 321–344, ch. 13, doi: 10.1002/9781119675525.ch13.

[94] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.

[95] A. E. Azzaoui, S. K. Singh, Y. Pan, and J. H. Park, "Block5GIntell: Blockchain for AI-enabled 5G networks," *IEEE Access*, vol. 8, pp. 145918–145935, 2020.

[96] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: Mechanism, design and applications," *Sci. China Inf. Sci.*, vol. 64, no. 2, pp. 1–15, Feb. 2021.

[97] L.-N. Lundbæk, D. Janes Beutel, M. Huth, S. Jackson, L. Kirk, and R. Steiner, "Proof of kernel work: A democratic low-energy consensus for distributed access-control protocols," *Roy. Soc. Open Sci.*, vol. 5, no. 8, Aug. 2018, Art. no. 180422.

[98] W. J.-W. Tann, X. J. Han, S. S. Gupta, and Y.-S. Ong, "Towards safer smart contracts: A sequence learning approach to detecting security threats," 2018, *arXiv:1811.06632*.

[99] Y. Kim, D. Pak, and J. Lee, "ScanAT: Identification of bytecode-only smart contracts with multiple attribute tags," *IEEE Access*, vol. 7, pp. 98669–98683, 2019.

[100] R. Camino, C. F. Torres, M. Baden, and R. State, "A data science approach for detecting honeypots in ethereum," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–9.

[101] S. T. Abdulrazzaq, F. S. Omar, and M. A. Mustafa, "Decentralized security and data integrity of blockchain using deep learning techniques," *Periodicals Eng. Natural Sci. (PEN)*, vol. 8, no. 3, pp. 1911–1923, 2020.

[102] P. Liu and W. Zhang, "Game theoretic approach for secure and efficient heavy-duty smart contracts," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2020, pp. 1–9.

[103] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. Int. Conf. Financial Cryptography Data Secur.* New York, NY, USA: Springer, 2014, pp. 436–454.

[104] T. Wang, S. C. Liew, and S. Zhang, "When blockchain meets AI: Optimal mining strategy achieved by machine learning," 2019, *arXiv:1911.12942*.

[105] V. Chicarino, C. Albuquerque, E. Jesus, and A. Rocha, "On the detection of selfish mining and stalker attacks in blockchain networks," *Ann. Telecommun.*, vol. 75, no. 3, pp. 1–10, 2020.

[106] E. C. Ferrer, *The Blockchain: A New Framework For Robotic Swarm Systems*, vol. 1. Cham, Switzerland: Springer, 2018.

[107] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 72–80, Feb. 2020.

[108] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. and Song, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Jun. 2019, pp. 185–200.

[109] *Transformational Technologies: Today*, Oracle, Austin, TX, USA, 2018.

[110] C. Reichert. *Las Vegas Announces Smart City Plans With Cisco*. ZDNet. Accessed: Feb. 3, 2022. [Online]. Available: https://www.zdnet.com/article/las-vegas-announces-smart-city-plans-with-cisco/

[111] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

[112] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018.

[113] 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.

[114] K. R. Ozyilmaz, M. Dogan, and A. Yurdakul, "IDMoB: IoT data marketplace on blockchain," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 11–19.

[115] N. Yuva and I. Kırbas, "Directed acyclic graph based on crypto currency application example: Iota," in *Proc. Int. Conf. Data Sci. Appl.*, Porto, Portugal, 2018, pp. 26–28.

[116] J. Hohenstein and M. Jung, "AI as a moral crumple zone: The effects of AI-mediated communication on attribution and trust," *Comput. Hum. Behav.*, vol. 106, May 2020, Art. no. 106190.

[117] H. Eidenmüller. (Jun. 20, 2020). *What is an Arbitration? Artificial Intelligence and the Vanishing Human Arbitrator*. University of Oxford. [Online]. Available: https://www.law.ox.ac.U.K./business-law-blog/blog/2020/06/what-arbitration-artificial-intelligence-and-vanishing-human

[118] S. Liu, F. Mohsin, L. Xia, and O. Seneviratne, "Strengthening smart contracts to handle unexpected situations," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPCON)*, Apr. 2019, pp. 182–187.

[119] E. Genc. *Deviantart is now Using AI to Spot People Selling Stolen Art as NFTs*. Accessed: Feb. 3, 2022. [Online]. Available: https://www.vice.com/en/article/v7enyb/deviantart-is-now-using-ai-to-spot-people-selling-stolen-art-as-nfts

[120] S. Cooling, "Fetch.AI launches first NFT machine learning platform for AI-generated art," Medium, San Fransisco, CA, USA, Tech. Rep. 1, 2021.

[121] BlockBank. *Blockbank: Lightpaper*. Accessed: Feb. 3, 2022. [Online]. Available: https://blockbank.ai/pdf/lightpaper

[122] SingularityDAO. *Singularitydao: Platform Whitepaper*. Accessed: Feb. 3, 2022. [Online]. Available: https://www.singularitydao.ai/file/2021/04/Platform-Whitepaper-3.pdf

[123] S. D. Exchange. *Solana Decentralized Exchange: Whitepaper*. Accessed: Feb. 3, 2022. [Online]. Available: https://soldexai.gitbook.io/soldex-whitepaper/

[124] A. Gonfalonieri. *Why Building an AI Decentralized Autonomous Organization (AI DAO)*. Accessed: Feb. 3, 2022. [Online]. Available: https://towardsdatascience.com/why-building-an-ai-decentralized-autonomous-organization-ai-dao-85d018700e1a

[125] Chainlink. *What is the Blockchain Oracle Problem?*. Accessed: Feb. 3, 2022. [Online]. Available: https://blog.chain.link/what-is-the-blockchain-oracle-problem/

[126] Caraviggio. *AI Oracles on Blockchain*. Accessed: Feb. 3, 2022. [Online]. Available: https://www.lesswrong.com/posts/p9CSjcCoLqFptogjW/ai-oracles-on-blockchain-1

[127] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Hum.-centric Comput. Inf. Sci.*, vol. 10, no. 1, Dec. 2020.

[128] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustain. Cities Soc.*, vol. 63, Dec. 2020, Art. no. 102364. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210670720305850

[129] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519300864

[130] G. Capece and F. Lorenzi, "Blockchain and healthcare: Opportunities and prospects for the EHR," *Sustainability*, vol. 12, no. 22, p. 9693, Nov. 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/22/9693

[131] M. Sahoo, S. S. Singhar, and S. Sahoo, *A Blockchain Based Model to Eliminate Drug Counterfeiting*. Singapore: Springer, 2020, pp. 213–222.

[132] P. N. Srinivasu, A. K. Bhoi, S. R. Nayak, M. R. Bhutta, and M. Woźniak, "Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network," *Electronics*, vol. 10, no. 12, p. 1437, Jun. 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/12/1437

[133] M. M. Badr, M. Baza, S. Abdelfattah, M. Mahmoud, and W. Alasmary, "Blockchain-based ride-sharing system with accurate matching and privacy-preservation," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2021, pp. 1–8.

[134] R. Casado-Vara, J. Prieto, F. De la Prieta, and J. M. Corchado, "How blockchain improves the supply chain: Case study alimentary supply chain," *Proc. Comput. Sci.*, vol. 134, pp. 393–398, Aug. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187705091831158X

[135] I. S. Damoah, A. Ayakwah, and I. Tingbani, "Artificial intelligence (AI)-enhanced medical drones in the healthcare supply chain (HSC) for sustainability development: A case study," *J. Cleaner Prod.*, vol. 328, Dec. 2021, Art. no. 129598. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0959652621037768

[136] H. I. Ozercan, A. M. Ileri, E. Ayday, and C. Alkan, "Realizing the potential of blockchain technologies in genomics," *Genome Res.*, vol. 28, no. 9, pp. 1255–1263, Sep. 2018.

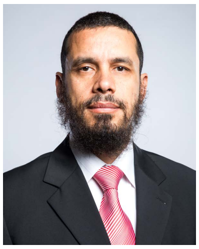
[137] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, pp. 102331–102344, 2019.

[138] S. Thiebes, M. Schlesner, B. Brors, and A. Sunyaev, "Distributed ledger technology in genomics: A call for Europe," *Eur. J. Hum. Genet.*, vol. 28, no. 2, pp. 139–140, Feb. 2020.

[139] M. Kim and J. Chung, "Sustainable growth and token economy design: The case of steemit," *Sustainability*, vol. 11, no. 1, p. 167, Dec. 2018.

[140] H. Bae, J. Jang, D. Jung, H. Jang, H. Ha, H. Lee, and S. Yoon, "Security and privacy issues in deep learning," 2018, *arXiv:1807.11655*.

JAGGER S. BELLAGARDA received the B.Com. degree (Hons.) in informatics from the University of Pretoria, in 2018, where he is currently pursuing the M.Sc. degree in applied science. He has published in the cryptocurrency space with his academic paper titled "The potential effect off-chain instant payments will have on cryptocurrency scalability issues-The Lightning Network" being included at the International Conference on Information Resources Management in Auckland, New Zealand, in May 2019. His research interests include blockchain technology, cryptocurrency, digital identity, and artificial intelligence.



ADNAN M. ABU-MAHFOUZ (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in computer engineering from the University of Pretoria. He is currently a Chief Researcher and the Centre Manager of the Emerging Digital Technologies for 4IR (EDT4IR) Research Centre, Council for Scientific and Industrial Research (CSIR), an Extraordinary Professor with the University of Pretoria, a Professor Extraordinaire with the Tshwane University of Technology, and a Visiting Professor with the University of Johannesburg. His research interests include wireless sensor and actuator networks, low power wide area networks, software defined wireless sensor networks, cognitive radios, network security, network management, and sensor/actuator node development. He is the Section Editor-in-Chief of the *Journal of Sensor and Actuator Networks* and an Associate Editor of IEEE ACCESS, IEEE INTERNET OF THINGS, and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS. He is a member of many IEEE Technical Communities.