Combining Blockchain and Artificial Intelligence – Literature Review and State of the Art

Conference Paper · November 2020

CITATIONS
22

READS
8,293

1 author:

Erik Karger
University of Duisburg-Essen
31 PUBLICATIONS **200** CITATIONS

SEE PROFILE

Combining Blockchain and Artificial Intelligence – Literature Review and State of the Art

Completed Research Paper

Erik Karger
University Duisburg-Essen
Universitätsstraße 9, 45141 Essen
erik.karger@icb.uni-due.de

Abstract

Artificial intelligence and blockchain are among the most popular technologies. Combine the two technologies also harbors manifold potentials. For instance, blockchain can help address specific AI-related difficulties such as the black box problem. Vice versa, AI offers opportunities to improve the blockchain's mining process, or smart contracts. Despite their relevance for companies, these combination solutions have so far received little attention. We undertake a systematic literature review to close this research gap and to provide a first comprehensive overview of this emerging field. We do so by providing a threefold categorization of the different options for connecting the blockchain and AI.

Keywords: blockchain, artificial intelligence, smart contracts, machine learning, deep learning

Introduction

Among the 21st century's various disruptive technologies, artificial intelligence (AI) and blockchain belong to those that stand out in terms of the attention and hype they have received (Salah et al. 2019). However, bringing together AI and blockchain is a combination of two completely different technologies. The blockchain is still a very young technology and research field. It was first described in the white paper *Bitcoin: A Peer-to-Peer Electronic Cash System* in 2008, although the term "blockchain" was not yet mentioned (Nakamoto 2008). In comparison, AI has been a well-researched area for several decades, beginning with the proposal of a first artificial neuron model (McCulloch and Pitts 1943) and Alan Turing's highly regarded essay *Computing Machinery and Intelligence* (1950). Until recently, researchers only studied blockchain and AI applications in isolation, focusing on their individual application in different vertical domains and businesses. Nevertheless, connecting AI and blockchain harbors a great deal of potential. Such a combination is rarely a question of developing completely new applications. Most of the academic work in this area investigates how one of the two technologies can support the other. For instance, the blockchain can enable an increase in the transparency of AI systems, which often have the character of a black box (Castelvecchi 2016). Against this background, the explainable artificial intelligence (XAI) research field has increasingly become an area of interest for the research community (Došilović et al. 2018). As an exemplary application, the blockchain can therefore provide new potentials for increasing transparency (Dillenberger et al. 2019; Sarpatwar et al. 2019). On the other hand, AI can help overcome some challenges with which that the blockchain, as a new technology, still struggles. Finally, there is a third category of use cases whose focus is not primarily on one technology supporting the other. Instead, AI and blockchain are used side by side and unfold their effect through their respective strengths. Examples include a platform for global employability (Keršič et al. 2020), or an approach that utilizes blockchain and automated machine learning to provide an automated customer service (Li et al. 2019).

To date, very little literature deals with blockchain's role in the AI context (Salah et al. 2019). As our review of the current literature shows, vice versa also holds true, namely for publications that deal with AI's impact on and benefits for blockchain. To this day, the literature lacks comprehensive reviews and studies on the possibilities that blockchain and AI can develop in cooperation. Initial ideas were already mentioned in 2014 and 2015 publications. As our literature review shows, since 2017 and 2018 an increase in research took place. Nevertheless, as Salah et al. (2019) mention, the research field on the possible combinations of AI and blockchain is still in its infancy. While Salah et al. conducted an extensive literature research on blockchain's role in the AI context (Salah et al. 2019), there is as yet, to the best of our knowledge, no study on blockchain and AI's combined potential synergies and their subsequent advantages and benefits. This is surprising, as this combination can be very useful and valuable for a lot of use-cases. An example is the blockchain's energy-intensive mining process, which can lead to enormous energy consumption (Fairley 2017), but AI holds the promise of possible improvements by forecasting the transaction confirmation time (Singh and Hafid 2020), or through a new consensus procedure (Chen et al. 2018). In turn, the blockchain can serve as a database to encourage more people to share personal data (e.g. Zyskind et al. 2015). This data can be highly valuable for companies as a data source for their AI systems. Given all the benefits for companies, combining AI and blockchain can be considered a very relevant topic for the IS field. We therefore endeavor to close the research gap by offering a current overview of the scientific work and approaches in this area. The aim of this work is to provide the latest state of research on the potential that combined AI and blockchain can have. Our aim also includes investigating open questions and possible future research directions. Our goal is therefore to find answers to the following research questions: How can blockchain and artificial intelligence be combined? What are the possible advantages of such a combination?

The rest of the paper is structured as follows: In section 2, we describe some of both AI and blockchain's foundations. Section 3 describes the research method used to conduct the systematic literature review. Section 4 is divided into three subsections corresponding to the respective possibilities of combining AI and blockchain. The publications found are presented here, and the current state of research described. Section 5, the final section, presents a discussion of and concluding remarks about this paper's results, as well as providing an outlook on future research.

Foundations

Blockchain

On closer inspection, blockchain is a combination of previously existing technologies. For instance, Diffie and Hellmann already formulated digital signature and public key cryptography ideas in 1976 (Diffie and Hellman 1976). Diffie and Hellmann were also the first to recognize the necessity of hash functions for digital signatures. The first works on hash functions' analysis and construction were published at the end of the 1970s by, for instance, Merkle (1979) and Rabin (1978) (Preneel 2010). Further developments later became part of the blockchain occurred in the 1990s. Haber and Stornetta (1991) recognized the problem of digital documents being easy to modify. On the basis of hash functions, they proposed two solutions for digital time-stamping documents so that they cannot be forged (Haber and Stornetta 1991). Satoshi Nakamoto combined the ideas for group signature schemes (Chaum and van Heyst 1991) and ring signature schemes (Rivest et al. 2001) with today's blockchain in 2008 (Nakamoto 2008). Currently , the blockchain has been widely adopted in various fields and is associated with high expectations (Salah et al. 2019). Some authors argue that the blockchain is the technology with the greatest potential to shape the next decade's business world. Tapscott and Tapscott believe that, in this respect, the blockchain is ahead of other technologies, such as AI, big data, and robotics (Tapscott and Tapscott 2016). According to Iansiti and Lakhani (2017), as well as Casey and Wong (2017), five basic principles underlie the blockchain technology:

- Distributed database: The whole database and its complete history are available for each blockchain party. No single party controls the data and information, and all the parties can verify the transactions without having to use an intermediary.
- Peer-to-peer transmission: The network peers can communicate with one another without a central node. This includes the storing and forwarding of information to all other peers.

- Transparency with pseudonymity: Transactions and their associated values are visible to everyone within a blockchain network. The single nodes on a blockchain have an alphanumeric address as a clear identifier. Transactions occur between these blockchain addresses.
- Irreversibility of records: Once a transaction is part of the blockchain, it cannot be altered or changed, because a transaction is linked to each transaction carried out beforehand. Various approaches and algorithms ensure transactions' permanence and correct order.
- Computational logic: The blockchain's computational logic makes it possible to program on the blockchain. Users can set up algorithms and rules that automatically trigger transactions between nodes.

The blockchain's name is derived from its technical structure, which can also be interpreted as a chain of blocks with each block connected to the previous blocks by a hash. Until recently, the blockchain was only used in connection with the *Bitcoin*, which is the best known project based on the blockchain (Abbatemarco et al. 2018). Recent research discusses the blockchain's potential for other application areas and industries. Examples are the blockchain's utilization in the context of smart cities (Xie et al. 2019), the internet of things (Christidis and Devetsikiotis 2016), and in the music industry (Baym et al. 2019). Smart contract is another often-mentioned term in connection with the blockchain. This refers to software that imitates contracts' behavior or logic, which allows companies to automate contracts' terms and conditions. A smart contract can refer to data fields contained in the blockchain (Tapscott und Tapscott, 2016). Such "contracts" or processes do not require any human interpretation or intervention, as a computer program executes them (Franco 2015). It should be noted that the blockchain is not a uniform technology. According to Tasca and Tessone (2019), thousands of blockchain-based projects are under development worldwide. Some of these projects propose completely new functionalities and architectures. Consequently, the previously mentioned authors stick to the terms "blockchains" and "blockchain technologies" (Tasca and Tessone 2019).

Artificial Intelligence

Although mankind has long tried to understand the functioning of intelligence, the term AI was first coined in 1956 (Russell and Norvig 2016). In recent years, there has been a reemergence of interest in the field of artificial intelligence among managers and academics (Brock and Wangenheim 2019). Currently, AI is a broad and thriving field with many practical applications and active research topics (Goodfellow et al. 2016). Machine learning (ML) technology powers many aspects of modern society: from web searches to content filtering on social networks, to recommendations on e-commerce websites, and it is increasingly present in consumer products, such as cameras and smartphones (LeCun et al. 2015). Deep learning is also among the current trending technologies. Owing to larger datasets and more powerful computers, deep learning has seen tremendous growth over the last years (Goodfellow et al. 2016). The architecture of deep learning comprises different modules arranged in multiple layers. Each of these layers can transform input data and is able to learn. Deep learning has improved the state of the art in several areas, such as speech recognition, visual object recognition, and object detection (LeCun et al. 2015). Swarm intelligence is another AI discipline concerned with intelligent multi-agent systems' design (Blum and Li 2008). This field of research is inspired by swarms from nature like ants or termites, which have formed a collective behavior. Nowadays, there is a wide range of possible practical applications of swarm systems. Examples include the transport of large and heavy objects by means of a swarm of mobile miniature robots (Chen et al. 2013), various applications of swarm robots in the agricultural sector (Emmi et al. 2014; Yaghoubi et al. 2013), and potential applications for entertainment purposes or toy robots (Alonso-Mora et al. 2014).

Research Method

According to Kitchenham and Charters, a systematic literature review (SLR) can be used to identify and evaluate "all available research relevant to a particular research question, or topic area, or phenomenon of interest" (Kitchenham and Charters 2007). One of this paper's declared objectives is to provide an as complete overview of the combination solutions as possible. A SLR was found to be a useful method to identify all relevant research and scientific work. In conducting the SLR, we followed Kitchenham and Charters's (2007) methodology. After precisely defining the research question, we identified the first

fundamental literature to derive relevant key terms for the search string. We subsequently tested the string in the used databases to guarantee its functionality. This resulted in the following string used for the search: *"("blockchain" OR "distributed ledger" OR ("blockchain" AND "smart contract")) AND ("intelligent" OR "intelligence" OR "artificial intelligence" OR "machine learning" OR "deep learning" OR "distributed intelligence" OR "neural network")*." We conducted searches with this string in the following databases:

- AIS Electronic Library (https://aisel.aisnet.org)
- EBSCO Host (https://search.ebscohost.com)
- Emerald Insight (https://www.emerald.com/insight/)
- Proquest (https://www.proquest.com/)
- Science Direct (https://www.sciencedirect.com/)
- SpringerLink (https://link.springer.com/)
- Web of Science (https://webofscience.com/)
- Wiley Online Library (https://onlinelibrary.wiley.com/)

We followed Mikalef et al. (2018) and Dybå and Dingsøyr's (2008) approaches to select the identified studies. After eliminating the duplicates, a total of 1,776 publications remained.

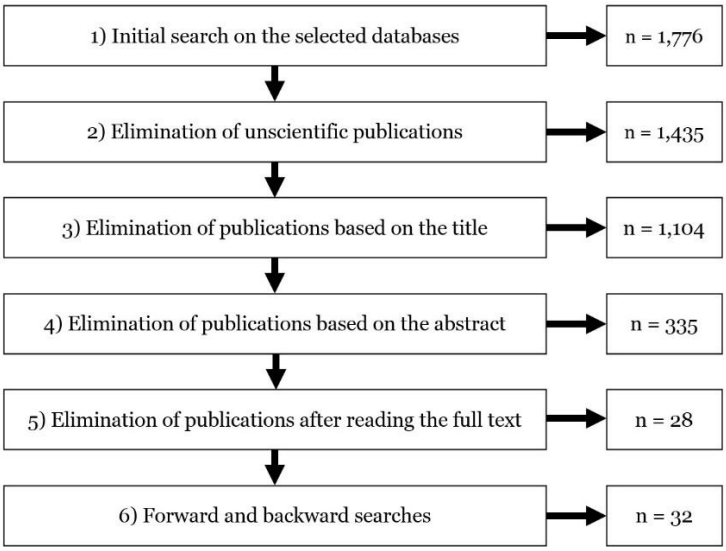

Figure 1. Illustration of the elimination criteria and the resulting number of publications

Figure 1 illustrates the different process steps to identify the relevant sources. The first step excluded all publications not published in a peer-reviewed journal or conference. We also excluded white papers, as they were often rather vague and lacked technical details. The white paper by SingularityNet (2019) was the only exception to this rule, because identified literature cited it. After this step, 1,435 articles remained. In the next step, we evaluated each study separately and in more detail. We removed more publications after reading the titles. This resulted in a total of 1,104 publications. These publications' abstracts were read to gain a first impression of the exact content. This led to another 769 papers being eliminated. A more detailed analysis of the remaining 335 articles' text was necessary in order to classify the content.

The reading of the 335 articles' abstracts and entire text led to a particularly large number of articles identified as unfitting for our study, which resulted in just 28 publications being found relevant. A major reason for this small number is that trend technologies, such as AI and blockchain, are often mentioned together. In most cases, however, these technologies are treated separately, while their combined potentials are only very rarely examined. We did additional backward and forward search searches based on the remaining publications. During this last step, we found four additional publications not included in

previous database search. This led to a total of 32 highly relevant articles and publications suitable for answering our previously defined research questions.

Findings

The identified combination applications can be divided into three main categories. The first category consists of use-cases and applications that use the blockchain to support or enhance existing AI applications. Consequently, and in line with previous research, we called this category *blockchain for AI*. In contrast, the second category (*AI for blockchain*) consists of use-cases where AI applications aim to improve the blockchain. This includes the mining process and smart contracts. Finally, the third category consists of applications and platforms that use AI and blockchain together without focusing on the one supporting or leveraging technology through the other one. We decided to call this third category *AI with blockchain*. As far as we know, no other research has as yet described this category.

Blockchain for AI

The first main category consists of use cases that aim to support AI methods and techniques by means of the blockchain. Work dealing with the potential of blockchain for AI has been found most frequently. These applications can be divided into the following subcategories:

- Blockchain-based data management
- Blockchain-based data marketplaces
- Blockchain-based AI architectures
- Blockchain-enhanced swarm systems
- Increase of transparency through the blockchain

The order of the categories in the list above and in the following is arbitrary and has no bearing on their priority.

Blockchain-based data management

The huge amount of available data is a driving factor behind the current AI revolution (Dinh and Thai 2018). Using the blockchain to store, manage, and share data has some advantages and potential gains for AI and ML systems. According to Salah et al., centralized data storage via clouds, data centers, and clusters is becoming a major bottleneck for highly secure and data-protection-relevant AI applications' development. Centralized data storage is very vulnerable in terms of data protection and security when it comes to personal and sensitive data about users, locations, activities, and health records (Salah et al. 2019). Furthermore, there are several ways to manipulate the training data and models of AI systems. The field of adversarial machine learning is concerned with creating algorithms that are more robust towards these security challenges. This is a topic of significant relevance, also addressed by the NIST, that published a first draft for the taxonomy and terminology of adversarial machine learning (Tabassi et al. 2019). Using the blockchain to obtain and store learning data for AI and ML systems holds the promise of opportunities to counteract the difficulties and dangers mentioned above. This means that data's secure storage and provision via the blockchain are a direct advantage for AI and ML systems. Possible gains are greater security, better quality of learning data, and increased motivation for data creators and owners to share their data.

Zyskind et al. (2015), who investigated the blockchain's potential to create a decentralized system for managing personal data, were responsible for an early approach. Their focus was on mobile applications, since these collect personal data without the user always being aware of it or being able to control it. These authors therefore presented a protocol in which a blockchain acts as an automated access control manager, eliminating the need for third-party control or trust. In contrast to *Bitcoin*, the transactions in this system are not of a financial nature, but are used to implement data-related instructions, such as storage, retrieval, and sharing. In this approach, the blockchain only serves as an instrument for access control, while the data are not stored on the blockchain (Zyskind et al. 2015). Xia et al. investigate the potential of a blockchain-based data exchange of healthcare data in cloud environments (Xia et al. 2017). The dissemination of medical data beyond individual institutions' protected cloud, poses a serious threat to patients' privacy. Xia et al. propose a blockchain-based data sharing framework that adequately

addresses the access control challenges associated with sensitive data stored in the cloud as a novel solution. In this approach, like the one described by Zyskind et al., the blockchain does not serve as a storage medium for the data, but its purpose is instead to enable access or to ensure that medical data can be provided more securely (Xia et al. 2017).

Shrestha and Vassileva (2018) present a blockchain-based model for collecting research data. This system should ensure the maintenance of complete and updated research data and a verifiable record of origin. All accesses to, the common use of, and the sharing of data should also be possible. This should not only lead to greater transparency for data owners, but also to protecting data against misuse. Users should also be given additional incentives, for example, digital tokens, to pass their data on to interested data seekers (Shrestha and Vassileva 2018). Yue et al. (2016) propose an app architecture based on the blockchain called *Healthcare Data Gateway*. The aim is to enable patients to easily and securely own, control, and share their data without compromising privacy. This might lead to new opportunities to improve healthcare systems' intelligence while keeping patient data private (Yue et al. 2016). Shafagh et al. (2017) focus on blockchain-based sharing and storage of data from the Internet of Things (IoT). In this approach, the blockchain is used as a control layer providing access to the storage. This control layer allows a secure and resilient access control management (Shafagh et al. 2017). With *FairAccess*, Ouaddah et al. (2017) propose a decentralized, pseudonymous, and data protection-oriented authorization management that uses blockchain technology to manage constrained devices' access control in the IoT context.

Blockchain-based data marketplaces

Another aspect in this context is the concept of electronic data marketplaces based on a blockchain. Subramanian (2017) proposes these decentralized marketplaces as a counter-draft to the company-controlled ones. In a decentralized marketplace, a network of nodes replaces the company responsible for the marketplace's proper functioning. This network is responsible for matching buyers and sellers, enabling transactions and for the infrastructure. The network of nodes therefore provides the same functionality independently and at the same time as a centralized marketplace would (Subramanian 2017). According to Subramanian, such decentralized marketplaces minimize transaction costs, as they do not require intermediaries, and buyers can pay sellers directly. Moreover, owing to the fast network validation, transactions occur immediately, and payment modalities do not delay them. There are also gains in security, as transaction details can be encrypted, network manipulation is extremely difficult and cost-intensive, and identities do not need to be revealed on the marketplace (Subramanian 2017). Özyılmaz, Doğan, and Yurdakul (2018) propose a blockchain-based marketplace for IoT data. Owing to their ever-increasing number and distribution, IoT devices are increasingly relevant as data generators. Such a decentralized IoT data platform, based on the blockchain, can offer all its participants various advantages. According to the mentioned authors, these advantages include not only economic gains, but also technical and user-related benefits. AI and ML providers are therefore given access to a huge data pool that was previously not available in this form. This increase in training and test data would lead to AI and ML systems' improved performance, which would ultimately also benefit companies or end-consumers (Özyılmaz et al. 2018).

Mamoshina et al. (2018) present the decentralized marketplace concept for personal health data based on a blockchain. With the help of such a decentralized marketplace, the authors envisage many opportunities for discovering drugs, developing biomarkers, and preventive health care. The authors also emphasize the challenges that data management faces in the health sector. The health sector is specifically challenged to ensure a high level of data protection and security. Data breaches in health storage systems can be particularly costly, since various policies threaten reputational damage and high penalties. Mamoshina et al.'s proposed marketplace is aimed at returning individuals' control of their personal data, including their medical records, to them. The marketplace does this by allowing users to upload their data directly into the system and allowing the use of these data once they have been purchased through the system. In addition, the marketplace ensures fair tracking of all the data use activities (Mamoshina et al. 2018).

Montes and Goertzel (2019) suggested another approach, the *SingularityNET* project. This is a platform for an open AI marketplace on which buyers and sellers can exchange AI services via a blockchain, and AI agents can trade with one another. The blockchain acts as a basis for a network-internal crypto currency. The latter tokens are the means of payment for or the medium for the exchange of AI services and for the internal coordination of AI agents (Montes and Goertzel 2019). Through smart contracts, the AI agents

will be able to request the performance of AI work, exchange data, and deliver the results (SingularityNet 2019). The various network nodes and participants work together to not only solve AI tasks, as explained below, but also to build large, decentralized data sets. *SingularityNet* allows data producers to set usage restrictions for their data and to receive percentage payments if they are used. Similarly, *SingularityNet* participants can track their contributions and their evolution, as well as gain financial benefits when the data sets and collaborative services grow. By decentralizing ownership and access to records, Montes and Goertzel see a great potential for *SingularityNet* regarding simplifying access to and the use of AI technology, especially for smaller companies. This would counteract the current trend of large technology giants hoarding very large data sets and smaller companies lacking access to data and the expertise to prepare these (Montes and Goertzel 2019).

Table 1. Overview of identified benefits of blockchain-based data management and data marketplaces

	Higher Security	Increased Privacy	Control about own data	Increased Transparency	Easier regulation
Zyskind et al. 2015	X		X		X
Xia et al. 2017	X	X	X		
Shrestha and Vassileva 2018	X	X	X	X	
Yue et al. 2016	X	X	X	X	X
Shafagh et al. 2017	X	X	X		
Ouaddah et al. 2017		X	X	X	
Subramanian 2017		X		X	
Özyılmaz et al. 2018	X	X			
Mamoshina et al. 2018	X	X	X	X	
Montes and Goertzel 2019			X		
Σ	7	8	8	5	2

In the current literature, blockchain-based data management and data marketplaces are the most investigated blockchain for AI applications. The benefits identified in the literature are manifold, with increased privacy (e.g., Xia et al. 2017), increased transparency (e.g., Shrestha and Vassileva 2018), and the possibility of returning data owners' control of their data to them, mentioned most often(Yue et al. 2016). According to some authors, blockchain's decentralized architecture will lead to greater security (Özyılmaz et al. 2018; Shafagh et al. 2017). Table 1 provides an overview of the most often mentioned advantages and benefits of blockchain-based data management and data marketplaces.

Blockchain-based AI architectures

DeepRing is an architecture that Akhil Goel et al. (2019) propose to protect deep neural networks by means of the blockchain. Individual blocks of convolutional neural networks (CNNs) are arranged randomly and contain information about the closest legitimate blocks. An advantage of this architecture is that *DeepRing* can register and detect all attacks on CNNs. Tampering at a certain point changes the respective block's hash value and that of all subsequent blocks, making changes or attacks visible and recognizable very quickly and easily. This increases the entire network's transparency, and that of individual blocks. The authors used experiments to show that blockchain's and deep neural networks' synergy can create tamper-proof models (Goel et al., 2019). Sgantzos and Grigg believe that a blockchain does not only serve as a basis for data, but as one for an entire artificial intelligence that works with its own data (Sgantzos and Grigg, 2019). These authors maintain that implementing a swarm of artificial intelligence agents (AIAs) would form a Church-Turing-Deutsch principle machine. According to the authors, this would impact different areas, such as the Internet of Things (IoT), financial markets, smart cities, and personalized medicine (Sgantzos and Grigg, 2019). In a previous publication, Sgantzos already showed that it is theoretically possible to implement certain cellular automata by means of a blockchain. Simulating a *Naturally Random Generated Mutational System* to allow a developed genetic algorithm to

evolve, should make such an implementation possible. Dedicated coins and tokens will make the interaction with such a system possible via the blockchain (Sgantzos, 2017).

In the same article, Montes and Goertzel also examine the advantages and gains that *SingularityNet* might bring to distributed AI (Montes and Goertzel 2019). In addition to merely exchanging data, AI agents should also be able to request AI work or provide results by means of smart contracts. The ability to quickly and dynamically connect or combine different AI systems or agents is also of central importance. In this way, it should be possible to react adequately to different requests to the network, which require different capabilities or AI systems. Agents should also be able to develop and train new and independent AI agents so that the network can be automatically coordinated and further developed. Similar to the exchange of data, this application will be paid for by means of a blockchain-based token. In the application that *SingularityNet* aims at, the blockchain for decentralized AI applications should provide the combined advantage of facilitating several agents' coordination with one another. Further, smart contracts help AI agents interact with one another, with external customers, and when requesting various tasks or data, as well as payment for them (Montes and Goertzel 2019). However, *SingularityNet* is currently not an executable platform and is still under development. Mariani et al. (2017) investigate different technologies' influence, including that of the blockchain, on tuple-based coordination systems. They argue that the blockchain technology's properties, such as its traceability and transparency, should further improve and refine tuple-based models' suitability. These authors see the possibility of managing interactions between the different involved agents by means of the blockchain and of creating interaction traces dynamically. It should also be possible to link interaction events by means of transactions and to provide a kind of accounting of the interactions' history within the system. This would make it possible to reliably determine who accessed what based on which previous events or facts, which would be a great advantage, for example, to later clarify responsibility for a particular event or action. The blockchain can also be used to monitor the interactions and coordinate the rules. A type of event correlation would be possible, since the blockchain ensures that distributed transactions are stored and visible in a very ordered and consistent way; that is, in the correct sequence (Mariani et al. 2017).

Blockchain-enhanced swarm systems

In the context of artificial swarm intelligence, using the blockchain holds the promise of certain advantages and possible improvements. The blockchain might help increase safety, support distributed decision making, and differentiate between individual robots' behavior. It was long assumed that swarm systems are robust, and that individual robots' failure has little effect on a swarm's overall collective behavior and security (Millard et al. 2013). Bjerknes and Winfield (2013) showed that the latter is not true, and that the overall system's reliability decreases with an increasing swarm size. Higgins et al. (2009) define various potential security gaps and dangers that can arise in the context of swarm systems. For example, security threats can emerge from insecure communication channels or from manipulated swarm members. According to Ferrer (2018), the blockchain can provide a reliable peer-to-peer communication channel for each agent in a swarm, therefore counteracting potential threats, vulnerabilities, and attacks. In the case of swarm robotics, public-key cryptography allows robots to share their public keys with other robots for communication purposes. Consequently, each robot in the network can send information to specific robot addresses by ensuring that only the robot with an appropriate private key can read the message (Ferrer 2018). The blockchain can also prevent third-party robots from decrypting information, even if they use the same communication channel. Similarly, a message's authorship can be clearly proven when robots use their own private key to encrypt messages (Ferrer 2018). Strobel et al. (2018) present a proposal in their article on how the blockchain can increase the safety of swarm systems. The authors developed a coordination mechanism that uses a blockchain for various purposes. Each robot keeps a separate copy of the blockchain and acts as a node and a miner in the blockchain network. The blockchain serves as a medium for exchanging knowledge, capturing voices, and applying decision strategies. The coordination functions are realized via a smart contract. This contract allows the swarm members to perform various functions and activities, including voting or making decisions. To trigger these functions' execution, the robots create signed transactions and send them to the network via the blockchain protocol. In their experiments, the authors showed that it is possible to identify and exclude malicious or byzantine robots from a swarm (Strobel et al. 2018).

Decision making algorithms are another crucial component in the field of swarm intelligence. They are used, for instance, for the dynamic allocation and execution of tasks (Das et al. 2011), or to control mobile

robots' collective movements (Navarro and Matía 2011). Nguyen et al. (2020) argue that swarm systems' decentralized nature makes them suitable to be combined with the blockchain. These authors propose a new, distributed collective decision algorithm for swarm robotics through which robots form a peer-to-peer network and perform various transactions using blockchain technology. The authors implemented various collective decision algorithms with and without blockchain participation to perform a benchmarking exercise. They subsequently carried out tests and compared the results with respect to various indicators, such as the consensus time and exit probability. Nguyen et al. showed that their proposed method surpasses other methods without a blockchain (Nguyen et al. 2020).

On the other hand, in the context of swarm robotics, Ferrer (2018) proposes using the blockchain as an instrument to facilitate decision making and consensus. Once a swarm member is faced with a situation that requires agreement, it can initiate a special transaction stored in the blockchain and which is therefore visible to all the other swarm members. Different addresses are linked to this transaction, each of which represents one of the available decision options. The other swarm members can now vote by sending a token, corresponding to the option that the specific swarm member selected, to the address. Agreements can thus be reached quickly, securely, and verifiably by means of, for example, the majority rule, since all robots can monitor the balance of the addresses involved in the voting process. According to Ferrer, the described method avoids a training and learning phase for new swarm robots, since all agreements and all related transactions are part of the blockchain. By downloading the ledger, new robots automatically obtain the history of all previous decisions and agreements, which enables an automatic synchronization with the rest of the swarm (Ferrer 2018). However, as the number of transactions increase, the blockchain also has an increasing amount of data to store. From a certain size onward, it becomes increasingly difficult to download or save the blockchain (Wagner 2014). This so-called "bloating" can become an issue if the blockchain is used in the swarm systems context. If large numbers of robots are used over a long period of time, they can extend the blockchain to such an extent that they can no longer keep a copy of the entire master book of transactions (Ferrer 2018).

Nishida et al. (2018) address this issue. These authors also see the continuously increasing blockchain as a challenge for its use in the swarm systems environment. They therefore propose an approach by which the blockchain's size and growth can be reduced. This proposal only comprises the storage of hash values in the blockchain, which are generated from the target data to be exchanged. The size of the transactions contained in the blockchain is therefore always the same and does not depend on the shared information's size. Tests that Nishida et al. carried out showed that the new method reduces the increase in the blockchain size by 73.0% (Nishida et al. 2018).

Increased transparency

According to Salah et al., AI systems' decisions that consumers or users find difficult to understand might lose their value (Salah et al. 2019). A clear audit trail might not only improve the data's and models' trustworthiness, but also provide a transparent way of tracking the process of how the AI system came to its decision (Corea 2019). Dillenberger et al. (2019) assume that the blockchain can increase trust in and the transparency of AI systems. The authors emphasize that with AI's increasing importance in everyday life and in critical business processes, trust in data, models, training processes, and results is of increasing importance. The blockchain can help track and illustrate a specific AI process at different granularity levels. The blockchain can also enable a fair evaluation of different stakeholders' contributions by capturing the involved parties' interactions and activities (Dillenberger et al. 2019). This approach is further elaborated in another publication, in which some of the same authors (Sarpatwar et al. 2019) present a generic blockchain library to create trust in distributed AI applications and processes. The library captures the entire distributed AI training process, including the data, intermediate and final models, processes and dependencies, participants, operations, and relevant metadata (Sarpatwar et al. 2019).

AI for blockchain

In the second main category, the roles of artificial intelligence and blockchain change. This category consists of scientific works dealing with the blockchain's support or enhancement through artificial intelligence methods. This topic has different names: Panetta (2019) calls the combination of the blockchain and other technologies, such as AI or the internet of things, *enhanced blockchain solutions*.

Garimella and Fingar (2018) use the term *Blockchain 4.0* when referring to intelligent blockchain applications. Our research established that this second category has to date received far less scientific attention than the first one. We divided the identified studies into two categories: the improvement of smart contracts by means of AI to make them more intelligent, and the improvement of the mining process.

Intelligent smart contracts

Artificial intelligence's possible potentials are specifically mentioned in terms of smart contracts. An AI system could, for example, function as a recommendation system during contract negotiations in supply chains (Almasoud et al. 2018). Based on archived smart contracts, the AI system could analyze how the parties negotiated in the past. This would allow the recommendation system to propose an appropriate language and clauses that would most likely lead to agreement between the different parties involved. Similarly, the AI can analyze past contracts to identify not yet considered factors in order to integrate them into future contracts (Almasoud et al. 2018). Additionally, in the smart contracts' context, an AI could be programmed to negotiate different conditions that could affect certain goods' price or quality. Furthermore, AI systems using supervised or unsupervised learning techniques or methods could determine the optimal time to trigger or perform a smart contract (Nguyen and Bailey 2018). For example, a purchase could be made at an optimal time in order to maximize a certain price-performance ratio. Such a smart contract would also react automatically to price or contract changes, and, based on this, dynamically change a service or a good's quality (Nguyen and Bailey 2018).

In addition, AI also has the potential to help in the event of contracts' failure. In this scenario, an AI system could help find alternative solutions dynamically and specifically tailored to the parties' needs (Nguyen and Bailey 2018). Omohundro (2014) believes that a combination with artificial intelligence methods would be required to make smart contracts operational in IoT environments. Conventional smart contracts are often sufficient with regard to processing purely digital transactions. However, as soon as an interaction with the real and physical world begins, more intelligence and real knowledge of decision making would probably be required. AI systems are needed to translate information from a variety of sensors into precise terms to which smart contracts can respond. Similarly, smart contracts that interact with the real world and lead to physical actions, such as the delivery of objects, should be linked to human or robotic agents (Omohundro 2014).

Improvement of the mining process

Singh and Hafid (2020) explore the possibility of using machine learning to predict the *Ethereum* blockchain's transaction confirmation time. As the number of transactions increases, the latter authors see the need for users to know if their transaction will be accepted and how long this is likely to take. They present three different models that can predict this confirmation time. These three models are each based on different machine learning methods: Naïve Bayes Classifiers, Random Forests, and Multi-Layer Perceptrons. Despite offering these approaches, the authors stress that this research field is still in its infancy and offers much potential for further research (Singh and Hafid 2020).

Chen et al. (2018) also criticize the immature consensus mechanisms currently used in blockchains. They suggest a completely new consensus mechanism as an alternative, which they call Proof of Artificial Intelligence (PoAI) (Chen et al. 2018). This new and energy-saving consensus protocol should help ensure a blockchain network's decentralization and security. All nodes of a blockchain network are sorted by a CNN, according to various criteria, such as computing power or security aspects, in a ranking list. Only the best nodes, which become part of a mining pool, can take over the mining. The relevant mining node is selected from this mining pool according to a rotation mechanism. This approach has some advantages, for example, competing for computing power is no longer necessary, which saves electricity and ensures fairness and decentralization. According to the mentioned authors, the results of the first experiments with this algorithm are promising (Chen et al. 2018).

Blockchain with AI

Contrary to previous literature, we believe that it is necessary to introduce a third category of use cases in order to provide a precise classification of the combination potentials. This third category does not focus

on either AI or blockchain's support or the enhancement by the other technology. Instead, AI and blockchain exist side by side and through their combination, create completely new applications. We therefore call this third category blockchain with AI.

Markopoulos et al. describe an approach using AI and blockchain in combination in the human resources management context (Markopoulos et al. 2020). This work's starting point is the *Democratic Teaming Model* (DTM) aimed at selecting project personnel democratically. However, this model depends on the many different skills of the team builder, who is the sole decision maker. Markopoulos et al. elaborate how both AI and blockchain hold a promise of potential gains for the DTM. By including expert systems, the organization can obtain recommendations on how teams should be composed. The expert system can use various types of employee data, such as their interests, experiences, or past activities. The blockchain can support this further by securing the data feed and transactions to optimize the analytical output. Besides expert systems, Markopoulos et al. see potentials for other AI technologies, such as machine learning, pattern recognition, or case-based reasoning (Markopoulos et al. 2020). Keršič et al. (2020) develop a platform for global employability based on AI and blockchain (Keršič et al. 2020). Their goal is to create a platform that allows an automatic search and recruitment process. Here, the blockchain is mainly used to ensure data integrity and to automate the business logic through smart contracts. In Keršič et al.'s approach, ML, as a part of AI, is used to analyze large amounts of data. ML can help find a suitable employee for a given task, which would avoid applicants and job offers' manual screening (Keršič et al. 2020). Arora et al. (2020) propose a combination of deep learning or AI and blockchain to make collaborative recommender systems safer. The goal of this approach is to make simple control of own data possible. The mentioned authors believe that the combination of these technologies would be very useful for those industries in which data privacy is important (Arora et al. 2020).

Ladia (2020) also addresses the issue of companies unable to share data with one another for privacy reasons. This is a huge disadvantage, because machine learning models benefit from additional training data. This author presents a blockchain-based implementation allowing the training of machine learning models without compromising privacy as a solution. In this approach, the blockchain handles the joint ownership and control of a *training machine*. This *training machine* acts as an independent, secure container that receives training data and untrained models as input. The *training machine* trains the respective model internally and returns the trained model as output. To ensure maximum safety, the data are not visible to any other party and are automatically deleted after the training process (Ladia 2020). Li et al. (2019) also present an approach based on blockchain and automated machine learning (AutoML) for an open and automated customer service. The starting point here is data collected by IoT devices during customer service. These data can be traded in an open, but secure, way with the blockchain. The blockchain can also be used to ensure that the data are not changed or manipulated. AutoML does the analysis to reduce dependency on human experts. These authors believe that their approach can particularly help small and medium-sized enterprises (SMEs). SMEs often do not have the necessary resources, since machine learning methods' development is often time-consuming as well as labor and knowledge intensive. AutoML in combination with the blockchain should allow this process to be automated to make it more accessible (Li et al. 2019).

Mylrea (2019) investigates how blockchain, AI, and machine learning together could form distributed autonomous energy organizations (DAEOs). Such a DAEO would serve as a basis of a distributed autonomous system for trading energy. This would have much potential, such as improving both the security and the speed, as well as reducing the need for third parties. Autonomous smart contracts could use autonomous agents to automatically exchange values or services. In this context, the blockchain can also function as a secure storage medium, through which the data is cryptographically signed and securely stored in a distributed ledger. This would allow the blockchain to be used, especially when the DAEO's AI requires sensitive data. Mylrea also takes a critical look at the blockchain, showing when it could make a meaningful contribution, but also when a conventional database would be more suitable. However, Mylrea concludes that a DAEO, equipped with AI and blockchain, would improve the electrical infrastructure's safety, efficiency, and resilience (Mylrea 2019).

Discussion and Conclusion

Both artificial intelligence and blockchain are technologies which harbor great potential for future usage. The same probably holds true regarding the solutions and applications in which blockchain and AI are

used in combination. Such combination solutions can be divided into three different groups: on the one hand, there are solutions in which the blockchain is used to support AI systems, or to address the associated difficulties (blockchain for AI). In contrast, applications in the AI for blockchain field are intended to help overcome blockchain-related issues with the help of AI and machine learning solutions. Besides these two categories, which the literature has already described, our paper introduces a third category, blockchain with AI. In the applications of this new category, blockchain and AI coexist. One technology's support of the other does not apply to applications in this third category. We considered it necessary to introduce this third category in order to have a comprehensive overview of all the blockchain and AI combination solutions. By providing an overview of the current scientific research and publications, our literature review contributes to the research on how blockchain and AI can be combined. The categorization of the papers that we identified in this regard is intended to be a first attempt to order and fully categorize the existing research. The existing studies only concentrate on individual areas, for example, the blockchain for AI (Salah et al. 2019). Our paper is, on the other hand, aimed at providing a complete overview of all the categories of possible combinations, which also include a description of the possible application potentials or gains, that can arise from an AI and blockchain combination. We believe that we succeeded in providing interested researchers with an initial overview of this emerging research field.

In view of future technological developments' unpredictability, this paper's results only represent the current state of the art in research. One could, however assume that the tripartitioning of the research field (blockchain for AI, AI for blockchain, blockchain and AI), which this paper describes for the first time, will continue to be a meaningful form of this field's structuring in the future. The categories of combination solutions compiled here, as well as their disadvantages and weaknesses, are also likely to retain their relevance and become the subject of future projects and research. However, the completeness of the applications and application categories described here cannot be guaranteed in the long term, since this study only investigates scientific publications and articles. Owing to technology's fast development, there might be use-cases in practice that research has not yet considered. Consequently, a closer investigation of the grey literature, white papers, and use-cases the practice might provide further insights. In addition, AI and blockchain's combination applications cannot be viewed in isolation. Instead, both AI and blockchain are continuously subject to new research results and developments. These new results and progress might have a direct influence on the combined applications field. It might, for instance become possible for each of the two technologies to address the other's disadvantages and weaknesses even further in the future. This would lead to the development of further applications in the areas of blockchain for AI and AI for blockchain. Furthermore, it is conceivable that some of AI and blockchain's currently existing disadvantages might be solved without the intervention of one of the two. This might make some combination solutions obsolete. It should be remembered that the combination of AI/ML and blockchain does not represent a combination of two clearly defined technologies. Instead, they should be understood as generic terms that cover many different techniques and methods. The latter creates a great deal of complexity and an enormous amount of potentially conceivable configurations and combinations, besides giving rise to a multitude of further research questions. These questions could be used to investigate the suitability of different AI and ML methods, as well as the different blockchain variants, for combination solutions. Salah et al. (2019) provide an initial list of future and open research questions. Completely new technologies, such as quantum computing, which could have a direct influence on the blockchain are also of interest (Kiktenko et al., 2018; Rodenburg and Pappas, 2017). We conclude that many interactions with other technologies and disciplines are possible. It is therefore likely that the research on combining AI and blockchain will undergo dynamic developments in the future.

Appendix – Full list of investigated publications

Table 2. Full list of investigated publications

ID	Author(s)	Year	Category	Application
01	Shrestha and Vassileva	2018	Blockchain for AI	Blockchain-based data management
02	Shafagh et al.	2017	Blockchain for AI	Blockchain-based data management
03	Ouaddah et al.	2017	Blockchain for AI	Blockchain-based data management
04	Xia et al.	2017	Blockchain for AI	Blockchain-based data management
05	Yue et al.	2016	Blockchain for AI	Blockchain-based data management
06	Zyskind et al.	2015	Blockchain for AI	Blockchain-based data management
07	Montes and Goertzel	2019	Blockchain for AI	Blockchain-based data marketplace
08	Mamoshina et al.	2018	Blockchain for AI	Blockchain-based data marketplace
09	Özyılmaz et al.	2018	Blockchain for AI	Blockchain-based data and AI marketplace
10	Mariani et al.	2017	Blockchain for AI	Blockchain-based decentralized intelligence
11	Nguyen et al.	2020	Blockchain for AI	Blockchain-based swarm system support
12	Ferrer	2018	Blockchain for AI	Blockchain-based swarm system support
13	Nishida et al.	2018	Blockchain for AI	Blockchain-based swarm system support
14	Goel et al.	2019	Blockchain for AI	Blockchain-based AI infrastructure
15	Sgantzos and Grigg	2019	Blockchain for AI	Blockchain-based AI infrastructure
16	Sgantzos	2017	Blockchain for AI	Blockchain-based AI infrastructure
17	Dillenberger et al.	2019	Blockchain for AI	Blockchain-based increase of transparency
18	Sarpatwar et al.	2019	Blockchain for AI	Blockchain-based increase of transparency
19	Almasoud et al.	2018	AI for blockchain	AI-supported smart contracts
20	Nguyen and Bailey	2018	AI for blockchain	AI-supported smart contracts
21	Omohundro	2014	AI for blockchain	AI-supported smart contracts
22	Singh and Hafid	2020	AI for blockchain	AI-enhanced mining process
23	Chen et al.	2018	AI for blockchain	AI-enhanced mining process
24	Markopoulos et al.	2020	Blockchain with AI	Parallel use of AI and blockchain
25	Keršič et al.	2020	Blockchain with AI	Parallel use of AI and blockchain
26	Arora et al.	2020	Blockchain with AI	Parallel use of AI and blockchain
27	Ladia	2020	Blockchain with AI	Parallel use of AI and blockchain
28	Li et al.	2019	Blockchain with AI	Parallel use of AI and blockchain
29	Mylrea	2019	Blockchain with AI	DAEO
30	Salah et al.	2019	Blockchain for AI	General discussion
31	Corea	2019	General discussion	General discussion
32	Dinh and Thai	2018	General discussion	General discussion

References

Abbatemarco, N., Rossi, L. M. de, and Salviotti, G. 2018. "An econometric model to estimate the value of a cryptocurrency network. The Bitcoin case," *Research Papers 164*.

Almasoud, A. S., Eljazzar, M. M., and Hussain, F. 2018. "Toward a Self-Learned Smart Contracts," in *15th International Conference on e-Business Engineering*: *ICEBE 2018: Proceedings,* Xi'an, China. 12. Oktober - 14. Oktober, Los Alamitos, California: IEEE Computer Society, Conference Publishing Services, pp. 269-273.

Alonso-Mora, J., Siegwart, R., and Beardsley, P. 2014. "Human - robot swarm interaction for entertainment," in *HRI'14*: *Proceedings of the 2014 ACM/IEEE International Conference on Human-Robot Interaction*, G. Sagerer, M. Imai, T. Belpaeme and A. Thomaz (eds.), Bielefeld, Germany. 3. März - 6. März, ACM Press, p. 98.

Arora, M., Chopra, A. B., and Dixit, V. S. 2020. "An Approach to Secure Collaborative Recommender System Using Artificial Intelligence, Deep Learning, and Blockchain," in *Intelligent communication, control and devices*: *Proceedings of ICICCD 2018*, S. Choudhury, R. Mishra, R. G. Mishra and A. Kumar (eds.), Singapore: Springer, pp. 483-495.

Baym, N., Swartz, L., and Alarcon, A. 2019. "Convening Technologies: Blockchain and the Music Industry," *International Journal of Communication* (13), pp. 402-421.

Bjerknes, J. D., and Winfield, A. F. T. 2013. "On Fault Tolerance and Scalability of Swarm Robotic Systems," in *Distributed Autonomous Robotic Systems*: *The 10th International Symposium*, A. Martinoli, F. Mondada, N. Correll, G. Mermoud, M. Egerstedt, M. A. Hsieh, L. E. Parker and K. Støy (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg; Imprint; Springer, pp. 431-444.

Blum, C., and Li, X. 2008. "Swarm Intelligence in Optimization," in *Swarm intelligence*: *Introduction and Applications*, C. Blum and D. Merkle (eds.), Berlin, Germany: Springer, pp. 43-86.

Brock, J. K.-U., and Wangenheim, F. von 2019. "Demystifying AI: What Digital Transformation Leaders Can Teach You about Realistic Artificial Intelligence," *California Management Review* (61:4), pp. 110-134 (doi: 10.1177/1536504219865226).

Casey, M. J., and Wong, P. 2017. *Global Supply Chains Are About to Get Better, Thanks to Blockchain*. https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain. Accessed 30 September 2019.

Castelvecchi, D. 2016. "Can we open the black box of AI?" *Nature* (538:7623), pp. 20-23.

Chaum, D., and van Heyst, E. 1991. "Group Signatures," in *Advances in cryptology - EUROCRYPT '91*: *Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, April 8 - 11, 1991 ; proceedings*, D. W. Davies (ed.), Berlin: Springer, pp. 257-265.

Chen, J., Duan, K., Zhang, R., Zeng, L., and Wang, W. 2018. "An AI Based Super Nodes Selection Algorithm in BlockChain Networks,"

Chen, J., Gauci, M., and Gross, R. 2013. "A strategy for transporting tall objects with a swarm of miniature mobile robots," in *2013 IEEE International Conference on Robotics and Automation (ICRA)*: *Proceedings,* Karlsruhe, Germany. 6. Mai - 10. Mai, IEEE, pp. 863-869.

Christidis, K., and Devetsikiotis, M. 2016. "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access* (4), pp. 2292-2303.

Corea, F. 2019. *Applied Artificial Intelligence: Where AI Can Be Used In Business*, Cham: Springer.

Das, G. P., McGinnity, T. M., Coleman, S. A., and Behera, L. 2011. "A fast distributed auction and consensus process using parallel task allocation and execution," in *2011 IEEE/RSJ International Conference on Intelligent Robots and Systems*, I. Staff (ed.), San Francisco, CA, USA. 25. September - 30. September, IEEE, pp. 4716-4721.

Diffie, W., and Hellman, M. 1976. "New directions in cryptography," *IEEE Transactions on Information Theory* (22:6), pp. 644-654.

Dillenberger, D. N., Novotny, P., Zhang, Q., Jayachandran, P., Gupta, H., Hans, S., Verma, D., Chakraborty, S., Thomas, J. J., Walli, M. M., Vaculin, R., and Sarpatwar, K. 2019. "Blockchain analytics and artificial intelligence," *IBM Journal of Research and Development* (63:2/3), 1-14.

Dinh, T. N., and Thai, M. T. 2018. "AI and Blockchain: A Disruptive Integration," *Computer* (51:9), pp. 48-53 (doi: 10.1109/MC.2018.3620971).

Došilović, F. K., Brčić, M., and Hlupić, N. 2018. "Explainable artificial intelligence: A survey," in *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*: *Proceedings,* Opatija, Kroatien. 21. Mai - 25. Mai, IEEE, pp. 210-215.

Dybå, T., and Dingsøyr, T. 2008. "Empirical studies of agile software development: A systematic review," *Information and Software Technology* (50:9-10), pp. 833-859 (doi: 10.1016/j.infsof.2008.01.006).
Emmi, L., Gonzalez-de-Soto, M., Pajares, G., and Gonzalez-de-Santos, P. 2014. "New trends in robotics for agriculture: integration and assessment of a real fleet of robots," *The Scientific World Journal* (2014).
Fairley, P. 2017. "Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous," *IEEE Spectrum* (54:10), pp. 36-59 (doi: 10.1109/MSPEC.2017.8048837).
Ferrer, E. C. 2018. "The Blockchain: A New Framework for Robotic Swarm Systems," in *Proceedings of the Future Technologies Conference (FTC) 2018*: *Volume 2*, K. Arai, R. Bhatia and S. Kapoor (eds.), Vancouver, BC, Canada. 15. November - 16. November, pp. 1037-1058.
Franco, P. 2015. *Understanding Bitcoin*: *Cryptography, Engineering and Economics*, Chichester, West Sussex: Wiley.
Garimella, K., and Fingar, P. 2018. *AI+Blockchain*: *A brief guide for gamechangers*, Tampa: Meghan-Kiffer Press.
Goel, Akhil, Agarwal, A., Vatsa, M., Singh, R., and Ratha, N. 2019. "DeepRing: Protecting Deep Neural Network with Blockchain," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops,* Long Beach, California. June 16-20.
Goodfellow, I., Bengio, Y., and Courville, A. 2016. *Deep learning*, Cambridge, Massachusetts, London, England: MIT Press.
Haber, S., and Stornetta, W. S. 1991. "How to time-stamp a digital document," *Journal of Cryptology* (3:2), pp. 99-111.
Higgins, F., Tomlinson, A., and Martin, K. M. 2009. "Survey on Security Challenges for Swarm Robotics," in *Proceedings, the Fifth International Conference on Autonomic and Autonomous Systems*, R. C. Calinescu (ed.), Valencia, Spain. 20. April - 25. April, Los Alamitos, Calif.: IEEE Computer Society, pp. 307-312.
Iansiti, M., and Lakhani, K. R. 2017. "The truth about blockchain," *Harvard Business Review* (95:1), pp. 118-127.
Keršič, V., Štukelj, P., Kamišalić, A., Karakatić, S., and Turkanović, M. 2020. "A Blockchain- and AI-based Platform for Global Employability," in *Blockchain and applications*: *International congress*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto and J. M. Corchado (eds.), Cham, Switzerland: Springer, pp. 161-168.
Kitchenham, B., and Charters, S. 2007. "Guidelines for performing Systematic Literature Reviews in Software Engineering: Version 2.3,"
Ladia, A. 2020. "Privacy Centric Collaborative Machine Learning Model Training via Blockchain," in *Blockchain and applications*: *International congress*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto and J. M. Corchado (eds.), Cham, Switzerland: Springer, pp. 62-70.
LeCun, Y., Bengio, Y., and Hinton, G. 2015. "Deep learning," *Nature* (521:7553), pp. 436-444.
Li, Z., Guo, H., Wang, W. M., Guan, Y., Barenji, A. V., Huang, G. Q., McFall, K. S., and Chen, X. 2019. "A Blockchain and AutoML Approach for Open and Automated Customer Service," *IEEE Transactions on Industrial Informatics* (15:6), pp. 3642-3651 (doi: 10.1109/TII.2019.2900987).
Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., Ogu, I. O., and Zhavoronkov, A. 2018. "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget* (9:5), pp. 5665-5690.
Mariani, S., Omicini, A., and Ciatto, G. 2017. "Novel Opportunities for Tuple-based Coordination: XPath, the Blockchain, and Stream Processing," in *18th Workshop "From Objects to Agents"*: *Proceedings of the 18th Workshop "From Objects to Agents"*, P. de Meo, M. N. Postorino and D. Rosaci (eds.), Scilla, Italien. 15. Juni - 16. Juni, pp. 61-64.
Markopoulos, E., Kirane, I. S., Balaj, D., and Vanharanta, H. 2020. "Artificial Intelligence and Blockchain Technology Adaptation for Human Resources Democratic Ergonomization on Team Management," in *Human Systems Engineering and Design II*, T. Ahram, W. Karwowski, S. Pickl and R. Taiar (eds.), Cham: Springer International Publishing, pp. 445-455.
McCulloch, W. S., and Pitts, W. 1943. "A logical calculus of the ideas immanent in nervous activity," *The Bulletin of Mathematical Biophysics* (5:4), pp. 115-133 (doi: 10.1007/BF02478259).
Merkle, R. C. 1979. *Secrecy, authentication, and public key systems*: *Doctoral Dissertation*, Standford, CA, USA.

Mikalef, P., Pappas, I. O., Krogstie, J., and Giannakos, M. 2018. "Big Data Analytics Capabilities: A Systematic Literature Review and Research Agenda," *Information Systems and e-Business Management* (16:3), pp. 547-578 (doi: 10.1007/s10257-017-0362-y).

Millard, A. G., Timmis, J., and Winfield, A. F. T. 2013. "Towards Exogenous Fault Detection in Swarm Robotic Systems," in *Towards autonomous robotic systems*: *14th Annual Conference, TAROS 2013 Oxford, UK, August 28–30, 2013 Revised Selected Papers*, A. Natraj, S. Cameron, C. Melhuish and M. Witkowski (eds.), Oxford, Großbritannien. 28. August - 30. August, Cham: Springer, pp. 429-430.

Montes, G. A., and Goertzel, B. 2019. "Distributed, decentralized, and democratized artificial intelligence," *Technological forecasting and social change* (141), pp. 354-358.

Mylrea, M. 2019. "Chapter 12 - Distributed Autonomous Energy Organizations: Next-Generation Blockchain Applications for Energy Infrastructure," in *Artificial intelligence for the Internet of everything*, W. Lawless, R. Mittu, D. Sofge, I. S. Moskowitz and S. Russell (eds.), London, United Kingdom, San Diego, CA: Academic Press, an imprint of Elsevier, pp. 217-239.

Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Accessed 24 October 2019.

Navarro, I., and Matía, F. 2011. "A framework for the collective movement of mobile robots based on distributed decisions," *Robotics and Autonomous Systems* (59:10), pp. 685-697.

Nguyen, H., and Bailey, S. 2018. "Use of Artificial Intelligence for Smart Contracts and Blockchains," *FinTechLaw Report: E-Banking, Payments and Commerce in the Mobile World* (20:2), pp. 1-7.

Nguyen, T. T., Hatua, A., and Sung, A. H. 2020. "Blockchain Approach to Solve Collective Decision Making Problems for Swarm Robotics," in *Blockchain and applications*: *International congress*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto and J. M. Corchado (eds.), Cham, Switzerland: Springer, pp. 118-125.

Nishida, Y., Kaneko, K., Sharma, S., and Sakurai, K. 2018. "Suppressing Chain Size of Blockchain-Based Information Sharing for Swarm Robotic Systems," in *2018 Sixth International Symposium on Computing and Networking Workshops*: *Proceedings,* Takayama, Japan. 27. November - 30. November, Los Alamitos, CA: IEEE Computer Society, Conference Publishing Services, pp. 524-528.

Omohundro, S. 2014. "Cryptocurrencies, smart contracts, and artificial intelligence," *AI Matters* (1:2), pp. 19-21.

Ouaddah, A., Elkalam, A. A., and Ouahman, A. A. 2017. "Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, Á. Rocha, M. Serrhini and C. Felgueiras (eds.), Cham: Springer International Publishing; Imprint; Springer, pp. 523-533.

Özyılmaz, K. R., Doğan, M., and Yurdakul, A. 2018. "IDMoB: IoT Data Marketplace on Blockchain," in *2018 Crypto Valley Conference on Blockchain Technology*: *Proceedings,* Zug. 20. Juni - 22. Juni, Los Alamitos, California, Washington, Tokyo: Conference Publishing Services, IEEE Computer Society, pp. 11-19.

Panetta, K. 2019. *The CIO's Guide to Blockchain*. https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/. Accessed 26 August 2020.

Preneel, B. 2010. "The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition," in *Topics in cryptology*: *The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010*. *Proceedings*, J. Pieprzyk (ed.), Berlin: Springer, pp. 1-14.

Rabin, M. O. 1978. "Digitalized Signatures," in *Foundations of secure computation*, R. A. DeMillo (ed.), New York: Academic Press, pp. 155-166.

Russell, S. J., and Norvig, P. 2016. *Artificial intelligence*: *A modern approach*, Boston, Columbus, Indianapolis: Pearson.

Salah, K., Rehman, M. H. U., Nizamuddin, N., and Al-Fuqaha, A. 2019. "Blockchain for AI: Review and Open Research Challenges," *IEEE Access* (7), pp. 10127-10149.

Sarpatwar, K., Vaculin, R., Min, H., Su, G., Heath, T., Ganapavarapu, G., and Dillenberger, D. 2019. "Towards Enabling Trusted Artificial Intelligence via Blockchain," in *Policy-Based Autonomic Data Governance*, S. Calo, E. Bertino and D. Verma (eds.), SPRINGER NATURE, pp. 137-153.

Shafagh, H., Burkhalter, L., Hithnawi, A., and Duquennoy, S. 2017. "Towards Blockchain-based Auditable Storage and Sharing of IoT Data," in *Proceedings of the 2017 on Cloud Computing Security Workshop*, B. Thuraisingham (ed.), Dallas, Texas, USA. 3. November, New York, NY: ACM, pp. 45-50.

Shrestha, A. K., and Vassileva, J. 2018. "Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners," in *BLOCKCHAIN - ICBC 2018*: *First international conference*, S. Chen, H. Wang and L.-J. Zhang (eds.), Seattle, WA, USA. 25. Juni - 30. Juni, Springer, pp. 259-266.

Singh, H. J., and Hafid, A. S. 2020. "Prediction of Transaction Confirmation Time in Ethereum Blockchain Using Machine Learning," in *Blockchain and applications*: *International congress*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto and J. M. Corchado (eds.), Cham, Switzerland: Springer, pp. 126-133.

SingularityNet 2019. *White Paper 2.0*: *SingularityNET - A Decentralized, Open Market and Network for AIs*. https://public.singularitynet.io/whitepaper.pdf. Accessed 18 October 2019.

Strobel, V., Ferrer, E. C., and Dorigo, M. 2018. "Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario scenario," in *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, E. Andre, S. Koenig, M. Dastani and G. Sukthankar (eds.), Stockholm, Schweden. 10. Juli - 15. Juli, 3237383: International Foundation for Autonomous Agents and Multiagent Systems, pp. 541-549.

Subramanian, H. 2017. "Decentralized blockchain-based electronic marketplaces," *Communications of the ACM* (61:1), pp. 78-84.

Tabassi, E., Burns, K. J., Hadjimichael, M., Molina-Markham, A. D., and Sexton, J. T. 2019. *A Taxonomy and Terminology of Adversarial Machine Learning*: *Draft NISTIR 8269*. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8269-draft.pdf. Accessed 2 September 2020.

Tapscott, D., and Tapscott, A. 2016. *The Impact of the Blockchain Goes Beyond Financial Services*. https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services. Accessed 26 October 2019.

Tasca, P., and Tessone, C. J. 2019. "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification," *Ledger* (4), pp. 1-39.

Turing, A. M. 1950. "Computing Machinery and Intelligenc," *Mind* (LIX:236), pp. 433-460.

Wagner, A. 2014. *Ensuring Network Scalibility: How to Fight Blockchain Bloat*. https://bitcoinmagazine.com/articles/how-to-ensure-network-scalibility-fighting-blockchain-bloat-1415304056. Accessed 23 September 2019.

Xia, Q., Sifah, E., Smahi, A., Amofa, S., and Zhang, X. 2017. "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," *Information* (8:2), pp. 44-59.

Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., and Liu, Y. 2019. "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," *IEEE Communications Surveys & Tutorials* (21:3), pp. 2794-2830 (doi: 10.1109/COMST.2019.2899617).

Yaghoubi, S., Akbarzadeh, N. A., Bazargani, S. S., Bazargani, S. S., and Bamizan, M. 2013. "Autonomous Robots for Agricultural Tasks and Farm ssignment and Future Trends in Agro Robots," *International Journal of Mechanical & Mechatronics Engineering* (13:3).

Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. 2016. "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *Journal of medical systems* (40:10), p. 218.

Zyskind, G., Nathan, O., and Pentland, A. 'S.' 2015. "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *2015 IEEE Security and Privacy Workshops (SPW),* San Jose, CA, USA. 21. Mai - 22. Mai, Piscataway, NJ: IEEE, pp. 180-184.