Journal of Network and Computer Applications 225 (2024) 103858

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review article

AI-enhanced blockchain technology: A review of advancements and opportunities

Dalila Ressi [a,b,*], Riccardo Romanello [b], Carla Piazza [b], Sabina Rossi [a]

[a] Department of Environmental Sciences, Informatics and Statistics, Ca' Foscari University of Venice, Italy
[b] Department of Mathematics, Informatics, and Physics, University of Udine, Italy

ARTICLE INFO

Keywords:
Blockchain
Artificial intelligence
Machine learning

ABSTRACT

Blockchain technology has rapidly gained popularity, permeating various fields due to its inherent features of security, transparency, and decentralization. Blockchain-based applications, spanning from financial transactions to supply chain management, have revolutionized numerous industries. Concurrently, Artificial Intelligence (AI) techniques have emerged as a powerful tool for efficiently solving complex problems. The integration of AI into blockchain applications has shown promise in addressing key challenges such as security, consensus, scalability, and interoperability. While existing literature offers several surveys on the intersection of AI and blockchain, our work takes a distinct perspective by focusing on how AI solutions can enhance and optimize blockchain technology and its applications. Our goal is to provide a comprehensive literature overview of the methods that have been employed to improve blockchain technology through AI, encompassing machine learning, deep learning, natural language processing and reinforcement learning.

Our contribution highlights AI's potential to enhance blockchain, improving efficiency, security, and reliability of blockchain-based applications. By exploring AI's role in consensus, smart contracts, and data privacy, it advances theory and practical applications, fostering innovation across sectors for a more secure and efficient digital future.

1. Introduction

In recent years, the field of *Artificial Intelligence (AI)* has undergone a profound transformation, leaving a significant impact on both academia and industry. *Machine Learning (ML)* algorithms, and particularly *Deep Learning (DL)* models, have shown exceptional performance across a wide range of tasks, given the availability of sufficient data. Consequently, these techniques have been extensively implemented in most everyday technologies.

Simultaneously, another topic that has gained immense popularity is *Blockchain Technology* (*BC* or *BCT*) — a type of *Distributed Ledger Technology* (*DLT*). Decentralization, transparency, and immutability are among the many advantages coming from using this technology for consistent data storage. As a consequence, blockchain has emerged as a game-changing innovation with numerous applications across diverse domains.

The integration of AI and blockchain has garnered significant attention in recent years, with researchers exploring various ways to combine these two fields. The versatility of AI methods, coupled with the widespread adoption of blockchain, has given rise to a new area of interest. Incorporating AI into blockchain-based applications can yield numerous benefits, consisting of enhanced security, optimization, and efficiency. As a result, there has been an exponential growth in the number of works integrating these two technologies, driven by the potential synergies and advantages they offer when combined.

The purpose of blockchain is to securely store a substantial amount of data that is visible to everyone, making it an ideal provider for the vast volumes of data typically required to train deep learning models. This provides significant advantages to the community of AI developers, who can leverage the blockchain to share locally collected data (Kim et al., 2019). Furthermore, blockchain plays a pivotal role in addressing the explainability challenge that neural networks often face. By enabling shared data and models, blockchain ensures transparency and fairness of the training process. In addition, it fosters collaboration among the community, allowing for the collective design of better solutions, rather than relying solely on individual developers (Kim et al., 2019; Nguyen et al., 2021). This collaborative approach leverages the collective intelligence of the community, leading to more robust and comprehensive outcomes.

* Corresponding author at: Department of Mathematics, Informatics, and Physics, University of Udine, Italy.
E-mail addresses: dalila.ressi@unive.it (D. Ressi), riccardo.romanello@uniud.it (R. Romanello), carla.piazza@uniud.it (C. Piazza), sabina.rossi@unive.it (S. Rossi).

https://doi.org/10.1016/j.jnca.2024.103858
Received 4 May 2023; Received in revised form 16 November 2023; Accepted 28 February 2024
Available online 1 March 2024

Acronyms

BC	Blockchain
BCT	Blockchain Technology
DLT	Distributed Ledger Technology
PoW	Proof of Work
PoS	Proof of Stake
NFT	Non Fungible Tokens
DAO	Decentralized Autonomous Organization
ETH	Ethereum, also referred to its coin
ETC	Ethereum Classic
AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
XAI	Explainable Artificial Intelligence
NN	Neural Networks
DNN	Deep Neural Network
CNN	Convolutional Neural Network
LSTM	Long Short Term Memory
GANs	Generative Adversarial Networks
SVM	Support Vector Machine
NLP	Natural Language Processing
SL	Supervised Learning
UL	Unsupervised Learning
RL	Reinforcement Learning
IoT	Internet of Things
IIoT	Industrial Internet of Things
IoV	Internet of Vehicles
EHR	Electronic Health Records
VANETs	Vehicular Ad hoc Networks
SCF	Supply Chain Finance
DDoS	Distributed Denial of Service
Tx	Transaction
DeFi	Decentralized Finance

The ability of intelligent algorithms to extract meaningful patterns from large data sets makes the use of AI to analyze and study data saved in the blockchain a seamless integration of these two cutting-edge technologies. Including AI in the development of blockchain-based applications can bring many benefits. For example, reinforcement learning, and especially deep reinforcement learning (DRL), has been extensively applied in the context of blockchain-based Internet of Things (IoT) networks and Industrial IoT (IIoT). It has been utilized to automate business processes in various industry sectors and provide dynamic, optimized, and self-adjusting security policies (Outchakoucht et al., 2017). Moreover, machine learning techniques have found applications in enhancing the security of public blockchains. For instance, supervised methods have been largely adopted for various tasks, such as entity classification in Bitcoin, by identifying address aggregates (Tubino et al., 2022), predicting illicit transactions using ensembles (Alarab et al., 2020), discriminating exchange nodes from miners with decision trees (Michalski et al., 2020), and detecting fraudulent accounts on Ethereum blockchain Ostapowicz and Żbikowski (2020). Additionally, neural networks are commonly employed for cryptocurrency price prediction (Khedr et al., 2021), often treated as a classification task (Jay et al., 2020; Patel et al., 2020; Pintelas et al., 2020). Clustering methods like trimmed k-means and expectation minimization have also been effective in detecting fraudulent transactions associated with money laundering, ransomware attacks, and other suspicious activities (Monamo et al., 2016; Baek et al., 2019; Zhi et al., 2022). Furthermore, these techniques can even be utilized in defining a consensus protocol (Reddy and Sharma, 2020), showcasing the versatility and potential of machine learning in the realm of blockchain technology. Clustering methods also offer a valuable approach for gaining system insight (Awan and Cortesi, 2017), and can even be employed to identify entities within a network (Backstrom et al., 2007). As a result, they can be utilized to overcome the limitations of anonymity provided by certain systems.

Contributions. In this survey, we thoroughly analyze existing works to provide readers with insights on how machine learning and AI, in general, have been utilized in conjunction with blockchain technology and for which specific purposes. Our focus is on how AI can directly enhance blockchain-based applications by interacting with the underlying protocols, rather than solely performing evaluations on the data stored in the blockchain. Despite numerous studies that attempt to categorize and characterize existing literature on the subject, we have observed that many of them fall short in adequately addressing at least one of the following key aspects:

- *Integration and Subcategorization*: Many studies do not clearly specify how the integration of artificial intelligence (AI) and blockchain technologies is achieved, and how existing papers are classified into relevant subcategories. This lack of clarity makes it difficult to understand the nuances of how AI and blockchain are combined and utilized in different contexts.
- *AI's Impact on Blockchain*: Some studies do not focus sufficiently on how AI can specifically enhance blockchain technology or its applications. This includes exploring the potential benefits, challenges, and limitations of incorporating AI into blockchain systems. Such insights are crucial for understanding the implications of this integration and its potential impact on various industries and domains.
- *Comprehensive Overview of Recent Works*: Several studies lack a broad overview of the latest research and developments in the field of AI and blockchain. This includes a thorough analysis of the current state of the art, recent trends, and emerging approaches. Without a comprehensive understanding of the latest research, it becomes challenging to provide an up-to-date and insightful analysis of the topic.
- *Open Research Problems and Future Research Areas*: Many studies do not adequately address the open research problems in the field of AI and blockchain, nor do they outline potential research areas that have not been explored yet. Identifying research gaps and proposing future research directions is essential for advancing the field and driving innovation.

In conclusion, there is a need for studies to better address these critical aspects to provide a more comprehensive and insightful analysis of the integration of AI and blockchain technologies and its potential impact on various domains. While our work may not contribute significantly to the existing research or offer an in-depth examination of blockchain, we aim to illuminate the possibilities arising from the synergy between blockchain technology and AI.

Our research delves into cutting-edge advancements in integrating intelligent algorithms and neural networks into blockchain applications, aiming to uncover the latest findings in this field. We also conduct a comprehensive review of the diverse application areas where these two technologies have been synergistically combined, irrespective of the specific mode of integration. By doing so, we seek to elucidate the advantages and benefits that arise from leveraging the combined power of intelligent algorithms, neural networks, and blockchain technology.

While our approach is not exhaustive, our work still differs from other studies as we specifically focus on solutions that utilize intelligent algorithms to improve the behavior of blockchain protocols or workflows.

This work, focusing on how AI can enhance blockchain technology, plays a pivotal role in unraveling this potential synergy. As AI continues to advance, its capabilities in data analysis, pattern recognition, and automation are poised to address some of the fundamental

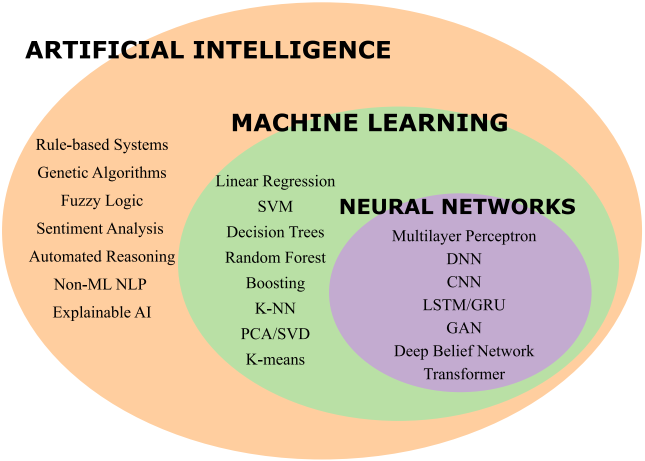


Fig. 1. Classification of some of the most popular AI techniques.

challenges faced by blockchain systems, such as scalability, security, and efficiency. By exploring how AI can be harnessed to optimize consensus mechanisms, enhance smart contract execution, and bolster data privacy within blockchain networks, our survey does not only contribute to the theoretical understanding of this dynamic interplay but it also paves the way for practical implementations that could revolutionize sectors ranging from finance and supply chain to healthcare and beyond. In an era characterized by rapid technological evolution, this work underscores the importance of harnessing synergies between two cutting-edge domains, ultimately driving the innovation needed to shape a more secure, transparent, and efficient digital future.

Structure of the paper. In Section 2 we introduce the fundamental concepts of artificial intelligence and blockchain. In Section 3 we compare our work with other existing reviews and surveys, which are categorized by different metrics. In Section 4 we discuss significant projects that utilize AI and blockchain in various application areas, even if they are not classified as “AI for blockchain”.

The focal point of our review is presented in Section 5, where we explore various potential methods for leveraging AI to enhance blockchain technology. Section 6 provides our insight into the specific problems that AI has effectively mitigated, as well as those that remain unresolved. Our final thoughts and conclusion are presented in Section 7.

2. Background

The purpose of this section is to provide a comprehensive background for a better understanding of the concepts of artificial intelligence and blockchain. Concerning artificial intelligence, we categorize and list the most prevalent AI techniques and explain what kind of task they can be used for. Additionally, we elaborate on two of the primary issues surrounding AI models, namely, data scarcity and explainability. Although this topic falls outside the scope of the present work, we briefly discuss how blockchain technology can aid in addressing these problems. For the blockchain background, we provide a comprehensive explanation of its intrinsic mechanisms, including consensus algorithms, miners/validators, smart contracts, and the distinction between private and public blockchains. We dedicate Section 5 to extensively discuss how AI methods have been integrated into blockchain technology, and how they can be used to improve blockchain security, performance, and efficiency.

2.1. Artificial intelligence

Artificial intelligence and machine learning are often referred to as if they were the same concept, but even if the terms are often considered interchangeable, they are not. Artificial Intelligence encompasses the overarching concept of creating systems that can imitate or replicate human behavior. Even if we are still not able to emulate the emotional sphere of the human brain, we have become incredibly proficient in teaching machines to solve a wide range of tasks, to the point that sometimes they are able to accomplish them better than humans. Machine learning instead refers to the collection of algorithms that are usually implemented to learn such tasks. Even if non-ML methods such as fuzzy logic (Mittal et al., 2020), sentiment analysis (Birjali et al., 2021), and automated reasoning (Davis and Marcus, 2016) have recently regained interest, most of the popularity of AI and ML comes from *Neural Networks (NN)* and *Deep Learning (DL)*. A common way to categorize AI methods is shown in Fig. 1.

Among artificial intelligence techniques, neural networks take a place of honor, both for their adaptability and the superior performance they can achieve on difficult tasks. Neural networks are a subset of machine learning algorithms that are inspired by the structure and function of the human brain. They are capable of solving complex problems in a variety of fields, such as image recognition, speech recognition, natural language processing, and robotics.

A neural network consists of interconnected layers of neurons, or nodes, that are capable of processing input data, learning from it, and producing output data. The most basic type of neural network is a feedforward neural network, which consists of a single input layer, one or more hidden layers, and a single output layer. The connections, or *weights*, in this type of architecture are present only between the nodes of two adjacent layers. These models are often used for tasks such as classification and regression.

Neural networks can be considered as mapping functions that take different types of inputs and are trained to return an output as close as possible to the desired one. The weights of the connections between neurons are adjusted during training to minimize the difference between the predicted output and the actual output. The activation function introduces non-linearity into the network, allowing it to model complex relationships between the input and output data. The number of layers and neurons a network is composed of highly impacts the complexity of the function it can model. For this reason, *Deep Neural Networks (DNNs)* contain a large number of layers and can learn from complex data. Other than the number of layers (the depth of the network) and the number of neurons in each layer (the width of the network), there are many other hyperparameters, that typically control the learning process. Examples of hyperparameters are the activation function, the learning rate, the decay, the number of epochs, the type of the layers and the sequence in which layers are organized.

The main advantage of using a neural model to solve a specific task comes from the capability of the network to learn the best parameters configuration by itself. Even if a good amount of knowledge is required to pick an appropriate architecture and hyperparameter configuration, it still involves limited human interaction with respect to other machine learning algorithms.

Architectures

Even if one of the first and simplest architectures is the traditional feedforward fully connected neural network, often simply referred to as ANN, many other types of architectures have been proposed in the last ten years. For example, another common architecture is called Convolutional Neural Network (CNN). It is characterized by the presence of convolutional layers, that allow extracting high-level features to solve image recognition tasks such as image classification, object detection, segmentation and scene understanding. The first CNN is AlexNet (Krizhevsky et al., 2012), proposed in 2012, and it is the reason why Neural Networks started to gain popularity. Indeed, Alexnet is the first neural network able to achieve results noticeably better than any other solution ever proposed before it. Thanks to its success, a multitude of different architectures have been proposed since then. For example, Recurrent Neural Networks (RNNs) differ from feedforward neural networks as they allow some feedback connections. RNNs are capable of processing sequences of variable length and can model temporal dependencies between inputs. They are used for sequence prediction tasks such as speech recognition and language modeling. Long short-term memory (LSTM) and Gated Recurrent Unit (GRU) networks are special types of RNNs that can remember information from previous inputs. They are largely exploited in *Natural Language Processing (NLP)* (Otter et al., 2020), not only for speech recognition but also for sentiment analysis, question answering (Soares and Parreiras, 2020), and language translation (Dabre et al., 2020). Another architecture widely used for NLP is called Transformer (Vaswani et al., 2017), where the authors introduced "attention" blocks to address some of the issues related to RNNs and deep networks in general, e.g., the vanishing gradient problem.

Types of Tasks

Typically, machine learning helps solve tasks that can be divided into three groups. The first class of problems is *Supervised Learning (SL)*. It concerns classification and regression problems, where a set of labeled data is used to learn the mapping between input data and the desired output. This example-based learning allows to classify new instances with extremely high accuracy, but the results are deeply limited by the need to have a large labeled dataset, free from mislabeled or dubious observations. The labeling and acquisition processes are usually long and expensive, and sometimes not even possible. Machine learning methods typically used for supervised learning are decision trees, ensembles such as bagging, boosting and Random Forest (RF), k-nearest neighbor (k-NN), linear/logistic regression, Support Vector Machine (SVM) and many different types of artificial neural networks. The evaluation metrics most used to assess the goodness of a model are Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE) for regression problems, and accuracy and F1-score for classification ones.

When data are unlabeled, *Unsupervised Learning (UL)* provides methods to detect groups of data with inherent strong similarity. The most common unsupervised algorithms are clustering methods such as hierarchical clustering, k-means and Density-Based Spatial Clustering of Applications with Noise (DBSCAN), but also methods for anomaly detection such as local outlier factor and isolation forest, and approaches for learning latent variable models, e.g., Expectation-Maximization (EM) algorithm, Principal Component Analysis (PCA) and Singular Value Decomposition (SVD) fall in this category. Neural networks commonly used for unsupervised tasks are Hopfield, Boltzmann, Restricted Boltzmann Machine (RBM), Autoencoder and Variational Autoencoder (VAE). A very particular network related to unsupervised learning is the Generative Adversarial Network (GAN). It is composed of two neural networks, where the first tries to "generate" realistic inputs that have to "fool" the other network, which has to discriminate between real and fake ones. Another type of generative network is Deep Belief Network (DBN) which is considered a more computationally efficient version of feedforward neural networks and can be used for image recognition, video sequences, motion capture data and NLP. Evaluating unsupervised methods might be challenging, and usually requires visualization techniques or testing. Some of the metrics used are the reconstruction error, log-likelihood, silhouette score and adjusted rand index.

The last type of problem tackled by machine learning falls under *Reinforcement Learning (RL)*, where an agent learns to make decisions through trial and error interactions with an environment. The agent receives feedback in the form of rewards or punishments for each action it takes, and aims to maximize its cumulative reward over time. Reinforcement methods are divided into model-based and model-free. In model-based RL a model of the environment is explicitly learned and used to make decisions. Model-free approaches instead learn policy directly from experience through trial-and-error interactions with the environment. Q-learning, SARSA, Monte Carlo, Temporal Difference (TD) learning, and Deep Reinforcement Learning (DRL) are all model-free methods. Reinforcement learning is closely related to other forms of machine learning, as it involves training a model to make decisions based on data. However, in reinforcement learning, the training data is generated by the agent's own actions in the environment rather than being provided by a human expert.

Limitations

Evaluating the performance of these methods can be challenging due to the complexity of the interaction between the agent and the environment. The choice of evaluation metric for reinforcement learning methods depends on the specific problem and goals of the agent. Typically, the performance of the algorithm is evaluated based on the cumulative reward received by the agent over multiple rounds, as well as the success rate in achieving certain tasks or goals. However, there may be other metrics that are relevant for specific reinforcement learning problems.

Two common drawbacks of machine learning methods and in particular of deep learning techniques are the scarcity of data and the unexplainability of their decision-making process.

Machine learning algorithms and deep neural networks require large amounts of data with good variability to be able to extract meaningful patterns while being able to maintain a good level of generalization. In many real-world situations, data acquisition can be constrained by physical, temporal, or financial limitations, which means that obtaining sufficient data is often not feasible. To mitigate such scenarios a large variety of solutions has been proposed:

- Generative Adversarial Networks (GANs) (Creswell et al., 2018) to artificially craft new observations (Kazeminia et al., 2020; Wang et al., 2018);
- Transfer Learning (Zhuang et al., 2020b) solutions that adopt a pre-trained network and fine-tune the weights with the available data. Sometimes this technique is adopted by using even only one or just a few instances (One-shot learning), or even only by providing descriptive attributes (Zero-shot learning) (Shorten and Khoshgoftaar, 2019);
- Data augmentation techniques such as in Gasparetto et al. (2018), Salamon and Bello (2017), Andriyanov and Andriyanov (2020) to boost the variability and quantity of observations.

The other most controversial characteristic of deep learning, and neural networks in general, is their unexplainable nature, as they are non-transparent and their predictions are not traceable by humans. Networks are often referred to as black boxes (Buhrmester et al., 2021) where it is extremely difficult to understand how the learning takes place or what the high-level features represent, due to their multi-layer nonlinear structure. For this reason, Explainable AI (XAI) has gained popularity recently. XAI is a set of methods and strategies to enhance the transparency, interpretability, and explainability of AI models. In particular, in the field of deep learning, techniques, such as Layerwise relevance propagation (LRP), can help understand which features and pixels for a particular input vector contribute the most to a neural network's output (Bach et al., 2015). Another possible benefit of these methods is that they can also be used to determine which parts of the network are used less, on average, and to remove them (Balemans et al., 2020). These kinds of pruning techniques are very common when using network compression, which still suffers from the same faults that XAI is trying to mitigate. As deep learning models grow in complexity, the difficulty of understanding what is happening inside the black box increases at the same pace. The unsolved problem of finding the global minima in a multidimensional non-linear cost function, and proving the optimality of the model, leads inevitably to solutions that work efficiently on the practical side, but that cannot be demonstrated to be the best ones. Even if some techniques try to formally reduce the networks' dimensions in an exact way (Castellano et al., 1997; Neill, 2020; Ressi et al., 2023, 2022), the solutions that work the best are still heavily dependent on approximations.

2.2. Blockchain technology

A *Blockchain (BC)* or *Blockchain Technology (BCT)* is a type of *Distributed Ledger Technology (DLT)* where digital data are stored into blocks. Each block is connected to the previous one, exactly as in a chain, and a new block can be added only to the end of the chain. The cryptographic algorithms that are at the base of the blockchain allow it to own some very appealing properties, the most important one being that it is impossible to change the content of a block without breaking the chain. The reason is that each block contains a hash to the previous one, which means that if any changes are made to the content of one block, it would require modifying not only that block but also all the subsequent blocks in the chain.

The popularity of blockchain-based applications and cryptocurrencies originates from the difficulty of performing a double-spending attack, contrary to what usually happens when using other distributed system protocols for data exchange. This is possible thanks to the *consensus algorithm*, where the nodes belonging to the system continuously verify the data and agree on which node can add the next block.

The purpose of most consensus protocols is to solve the Byzantine General's Problem (Lamport et al., 2019), overcoming the problem of reaching an agreement in a publicly accessible network with possible unreliable links (Lai and Chuen, 2018). Even if double-spending and other attacks (e.g., Sybil attack) are technically still possible, most of the time a malicious entity would need to control at least around 51% of the nodes in the network to have a chance of succeeding in an attack. There are also other mechanisms commonly exploited by most blockchains that can mitigate these problems, for example, possible forks of the chain are usually easily managed as nodes are encouraged to always pick the longest valid chain.

The ideas at the base of blockchain technology go back to at least the 1970s (Wong, 1986; Merkle, 1979; Kanare, 1985), but they have all been put together in the Bitcoin protocol proposed by Nakamoto in 2008 (Nakamoto, 2008). Although cryptocurrencies are built on blockchain technology, it is crucial to understand that they are distinct entities. A cryptocurrency is a digital currency typically implemented on a decentralized network. Most cryptocurrencies are based on distributed ledger technology, e.g., blockchain, where the whole history of a coin is clear and everybody can see each other transactions. Anonymity is guaranteed as each entity is represented by an address, while the security part is endorsed by the cryptographic algorithms used both to sign the single transactions and to chain the blocks to each other. The popularity of cryptocurrencies stems from the protocol's security and the pseudo-anonymity it provides. In this type of blockchain, honesty is generally ensured by two factors. Firstly, the block publisher is rewarded with a certain amount of coins or tokens, incentivizing participants to uphold the integrity of the blockchain. Secondly, the nodes and entities involved in transactions hold a stake in the form of crypto coins, which inherently motivates them to behave honestly. Any attempt to compromise the system, such as a double-spending attack, would erode trust in the cryptocurrency, leading to a significant decrease in its value. Thus, the value of a cryptographic coin is directly tied to the level of trust that investors place in its underlying protocol (Marella et al., 2020).

Consensus

Consensus algorithms are crucial protocols that govern how participant nodes in a blockchain network reach an agreement on the publisher of the next block and the overall state of the blockchain. A wide range of blockchain-based systems and consensus algorithms are available (Bouraga, 2021), and the number continues to grow every day (some of them are shown in Table 1).

The first consensus algorithm proposed is *Proof of Work* or *PoW* as in Bitcoin. In PoW nodes, called *miners*, compete to publish the next block. Miners have to invest their computational power into the task of finding, or *mining*, a random number called *nonce*. The nonce N has to be an integer value such that hashing the block data together with N results in a sufficiently small number. The hash function has to be collision resistant, meaning that it has to be computationally infeasible to find a collision—two different strings that hash to the same value. Multiple possible nonces exist for a specific block, but the only possible way to find one of these values is by trying plenty of numbers randomly. The computational capability of a machine directly impacts the number of possible values it can test at the same time, which is the reason why miners patronized the graphics card market during the last years. A Graphic Processing Unit (GPU) allows one to try multiple random values at the same time, parallelizing the work needed to find one of the precious nonces.

The economic benefits of being a miner come from both the reward achieved by mining a block (e.g., finding a suitable nonce for a specific block), and the eventual *transaction fees* of the same block. For this reason, it is not uncommon for miners to join a *mining pool* instead, where a group of nodes cooperates in finding the nonce and if one of them is successful they fairly split the reward.

Smart contracts

Even if Bitcoin is known as the first cryptocurrency, the next most valuable and popular one is Ethereum. Ethereum blockchain was launched in July 2015 by Vitalik Buterin and his team, which put particular attention to the development of smart contracts functionalities (Buterin et al., 2014). Ethereum protocol always used Proof of Work as consensus algorithm, but in September 2022 there was a major upgrade, also known as "the merge", to switch to Proof of Stake (PoS). Since then, Ethereum abandoned the term "miners", which are now instead called *validators*. The role of validators is to check the transactions inside the next block and to vote on their authenticity. The integrity of the validators is endorsed by economic interests, as they need to possess at least 32 Ether, or ETH, (worth about 45000 dollars, on March 2023) to participate in the voting. The algorithm used to select the next publisher simply picks one of the validators, while the probability of a validator being chosen is directly dependent on the amount of Ether they possess.

One of the most promising features of blockchain-based applications is the possibility of including *smart contracts*. A smart contract is a program or a piece of code designed to execute various operations based on its content. Among its functions, it can transfer coins or tokens to one of the parties involved. This mechanism has huge potential, as it completely bypasses the need of having a third party to guarantee many types of service, while also avoiding any bureaucratic procedures involved in signing a physical contract. Smart contracts can be implemented in blockchain for various applications: from insurance refunds to financial transactions, from corporate operations to the traceability of goods, and the protection of intellectual property (Hu et al., 2021; Lin et al., 2022). They are also used by Decentralized Autonomous Organizations (DAO) (Wang et al., 2019), real estate transactions (Ullah and Al-Turjman, 2021; Karamitsos et al., 2018), decentralized finance (Chen and Bellavitis, 2020), and in the legal industry (Waltl et al., 2019). Fig. 2 shows a simplified version of how smart contracts work. Smart contracts can be used to tokenize a wide range of assets, such as physical assets like real estate or personal property, digital assets like digital art or in-game purchases, and even contractual assets like insurance policies or other agreements. This tokenization process is typically achieved using Non-Fungible Tokens (NFTs), which provide a unique identification for each asset on the blockchain. Smart contracts have the potential to serve as a management framework for both private and public records, including personal records like wills, conveyances, medical data, education certificates, and employment records, as well as public records like land titles, vehicle registrations, passports, and building permits (Treleaven et al., 2017).

Smart contracts can also interact with external devices or sensors, that communicate data relevant to the execution of the program. The

Table 1
Some of the most common consensus protocols (Zhang and Lee, 2020; Bouraga, 2021).

Protocol name	Description	Cons	Type
PoW (Proof of Work)	Consensus protocol adopted by Bitcoin and Ethereum, where node selection depends on a computational power competition to solve a cryptographic puzzle (e.g., find the nonce)	The difficulty of finding the nonce involves an enormous energy consumption while achieving very low TSP (Transaction throughput per second)	Public
PoS (Proof of Stake)	Energy-saving consensus protocol where node selection depends on the held stake, rather than the computational power. Nodes still need to find the nonce, but it is a one-time computation that uses as key the amount of stake they own	Lower energy consumption than PoW, but only stakeholders can get the block reward	Public
DPoS (Delegated Proof of Stake)	A variant of PoS where stakeholders vote delegates as possible block creators. DPoS is a more cost-effective and efficient protocol when compared to PoW and PoS mechanisms.	It still suffers from the problem of having stakeholders controlling the liquidity	Public
PBFT (Practical Byzantine Fault Tolerance)	A five phases protocol (request, pre-prepare, prepare, commit, and reply) with low algorithm complexity that guarantees nodes maintain a common state and take consistent action in each round of consensus	Low fault tolerance and limited scalability (PBFT is suitable for a high performance network with a small number of nodes)	Private
Ripple	Open source payment protocol where the validating nodes in the list of trusted nodes called UNL (Unique Node List) communicate with each other and agree to record a transaction in the ledger only when 80% of the nodes received that transaction	Very low fault tolerance: only up to 20% of nodes in the entire network can have Byzantine Problem to not affect the correct result of consensus	Private

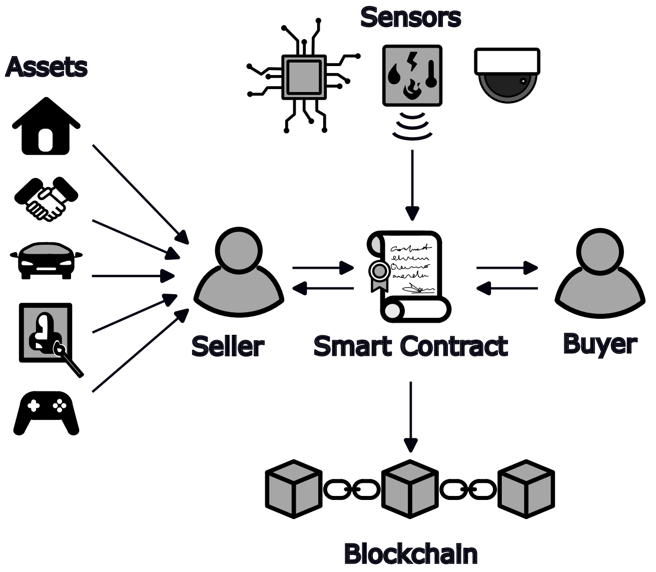


Fig. 2. Smart contracts mechanics.

trustless, transparent, digital contract is stored in a blockchain, avoiding the interaction of third parties such as banks, lawyers, and notaries. When the conditions in the program are met, the change of status must be registered in the blockchain, eventually paying a transaction fee (Zou et al., 2019).

Smart contracts are exposed to numerous vulnerabilities due to their non-standard software life cycles, especially because of the difficulty of updating the software shared by the nodes in the blockchain to solve inconsistencies or bugs (Destefanis et al., 2018). Other possible problems are their vulnerability to miscellaneous attacks, privacy leakage, and low processing rates due to the need to execute the code (Hu et al., 2021). A noteworthy event happened in July 2016, the Ethereum blockchain had a hard fork to reverse a hack that exploited smart contracts to remove roughly 50 million ETH from a DAO. To reverse the operation a new chain was created, still referred to with the Ethereum (ETH) denomination. At that time, some nodes rejected the decision to hard fork and kept mining on the old chain, since then renamed Ethereum Classic (ETC).

Public vs. Private

Public blockchains are famous for being decentralized, secure, and accessible to anybody, but the transparency of the ledger is sometimes a not desirable aspect for certain applications. For this reason, private blockchains, or mixed solutions (see Table 2), are usually adopted by companies, governance, or healthcare, to exploit the advantages offered by blockchain technology, while at the same time avoiding any leak of personal or sensitive data. Such systems, though, are usually centralized and they require nodes to be authenticated to enter the network, which compensates for the lower level of the overall security of the blockchain itself due to the lack of a consensus protocol.

The popularity of private blockchains is the result of the wild interest shown in cryptocurrencies during the last few years. Even if it is controversial to consider the private version of this technology still a type of blockchain, especially due to the absence of a consensus algorithm, it is undeniable how blockchain has become a widespread and largely adopted technology by both public and private entities.

3. Related surveys

There are compelling justifications for integrating and leveraging the synergies between blockchain and machine learning in a single application. Both technologies are inherently associated with processing substantial volumes of data. While blockchain is inherently designed to securely register and provide access to data, machine learning excels in analyzing data and producing precise results, particularly when working with large datasets. However, it is worth noting that machine learning models can lack transparency, not only during the training process but also during the data acquisition step. This limitation can be addressed by combining the two technologies, as they can complement each other's flaws. By utilizing the secure and transparent nature of blockchain for data registration and access, and leveraging the powerful data analysis capabilities of machine learning, the resulting application can provide enhanced accuracy and reliability while maintaining transparency and security throughout the data lifecycle. This integration can unlock new opportunities for applications that require both large-scale data analysis and transparent data handling, mitigating the limitations of each technology and creating a more robust solution.

In order to provide a comprehensive and exhaustive overview of the existing research on the topic, we begin by examining relevant published surveys and reviews. We have gathered surveys, reviews, and papers from reputable sources such as IEEE Xplore Digital Library, ACM,

Table 2
Different types of blockchain.

Type of blockchain	Anonymous	Permissioned	Incentive	Efficiency	Examples
Public	Yes	No	Mandatory	Low	Bitcoin, Ethereum
Consortium	No	Partially	Optional	Medium	Tendermint, Multichain
Private	No	Yes	Optional	High	Hyperledger, Corda

Springer, Scopus, and Google Scholar, using the strings: “blockchain” AND (“machine learning” OR “AI” OR “artificial intelligence” OR “deep learning”) AND (“survey” OR “review” OR “overview”). From this collection we further selected only the most important and recent ones, considering only those published later than 2018.

As there are already numerous applications employing both AI and blockchain technologies, our focus is on exploring their mutual benefits. Unlike other surveys, we adopt a unique approach to examining the literature from the perspective of how these two fields have been combined and for what purpose. In doing so, we classify applications, frameworks, and solutions that use both blockchain and AI into three categories:

1. Applications using both blockchain and AI algorithms independently;
2. Applications that leverage blockchain to enhance AI;
3. Applications that employ AI to enhance blockchain.

During our research, we have observed that a significant portion of applications leverage the combined potential of blockchain and artificial intelligence. However, in many cases, the utilization of blockchain is limited to serving as a distributed data storage solution, with a certain level of AI applied to the data stored therein. While these types of applications may still be classified as utilizing both AI and blockchain, it can be argued that in such cases, the two technologies are not truly leveraging each other’s potential for mutual benefit. (Further details on such applications can be found in Section 4.)

An alternative approach consists of utilizing blockchain, and more in general DLT, for training machine learning models. This technique, commonly known as federated or collaborative learning, involves a distributed system of entities working collectively to solve a specific machine learning task (Nguyen et al., 2021; Lu et al., 2019). There are many other ways blockchain can help AI, for example, by improving transparency and fairness, providing data sharing and integrity, and overall speeding up the development of AI algorithms (Wang et al., 2021a; Salah et al., 2019).

Conversely, AI can also be employed to enhance blockchain technology. We have observed a wide range of potential applications falling under this category. However, unlike most existing surveys that provide a general overview of works combining blockchain and AI, our focus is on how AI can improve the blockchain protocol itself or enhance the security, reliability, and efficiency of applications implementing this paradigm.

During our research, we identified a large number of existing surveys aiming to study and categorize how the two technologies have been used together for different purposes. While looking into this, we saw that many surveys already try to understand and sort out the mix of these two technologies for different purposes. But there is something important missing — most of the existing research does not explain well how AI can help applications that use blockchain. Instead, they either group similar applications together in general groups or focus only on some aspects of this merge. Moreover, the surveys that already exist usually only look at applications that use both AI and blockchain in certain specific areas (Zhang et al., 2020).

Table 3 summarizes the most important surveys and reviews that study applications using both blockchain and AI. The target specifies if the work is related to Blockchain for AI (BC→AI), AI for blockchain (AI→BC) or both, in this case, the target is labeled as “Mixed”. Some works consider AI and blockchain solutions specific to a certain field of application, such as metaverse (Yang et al., 2022), Iot/IIoT (Wu et al., 2021; Atlam et al., 2020), Healthcare (Mamoshina et al., 2018), IoV (Wang et al., 2021a) and Big Data (Rabah, 2018). For these cases, a check mark divides the topic-related surveys from the general ones. As it emerges from the Table, there are not many papers that specifically address how AI techniques have been used for blockchain technology or, if they are “mixed” ones, they mostly address a particular type of application.

Under these criteria, our study falls in the AI for blockchain (AI→BC) domain and it is not topic-specific. Indeed, differently to other previous works, we present a clear and well-structured survey that explains the real advantages of exploiting AI and machine learning algorithms in blockchain applications. We explore not only different application areas where these two technologies are already used in synergy, but also provide a clear understanding of which domains the merge is most useful to and in which way it manifests. Furthermore, we navigate through existing limitations that persist within current works and propose diverse mitigation strategies to address these concerns, fostering the potential for enhanced outcomes in subsequent research.

4. Applications areas

The advantages offered by blockchain technology lead to its adoption in a wide range of fields, such as infrastructure, governance, supply chain, healthcare, transportation, and finance (Arooj et al., 2022). The transparent, secure, and decentralized nature of blockchain makes it ideal not only for transactions, but also for data sharing, management and storage.

In this section, we explore existing solutions that leverage both blockchain and AI belonging to some of the most studied application areas: healthcare, internet of vehicles, decentralized finance, cryptocurrency and internet of things.

4.1. Federated learning, edge computing and digital twins

Traditional AI techniques consist of training a model using data stored locally within the same machine. As machine learning algorithms require substantial data volumes to effectively address specific problems, sharing data among different parties has emerged as an appealing solution. Another constraint in the training process relates to the requirement for significant computational resources, typically accompanied by substantial costs. Federated or collaborative learning, introduced by Google in 2016 (Hou et al., 2021), can be the solution for both of these problems. This paradigm consists of collaboratively training a model across distributed devices while preserving data privacy, making it ideal for scenarios where centralized data aggregation is not feasible. Coordinating this model training process is a central server. Initially, each client undertakes the training of a localized machine learning model using their own data and subsequently transmits the resulting model to the central server. The central server subsequently aggregates these different models into an updated global model, distributing it back to the respective clients. In client–server federated learning scenarios, the availability of a robust and dependable central server is a prerequisite; however, its presence is not universally guaranteed (Zhu et al., 2023). In this context, blockchain can be utilized to ensure the integrity of model updates and the transparency of the training process. This addresses concerns of data authenticity and trust among the distributed participants, while it removes the need for a central server or authority to evaluate the results. While federated

Table 3
Table of most cited surveys on blockchain and AI, from 2023 to 2018.

List of Surveys						
Year	Title	Description	Target	Topic	Source	Ref
2023	"A Bibliometric Analysis of Research on the Convergence of Artificial Intelligence and Blockchain in Smart Cities"	Systematic analysis of 505 articles published between 2017 and 2023 about the integration of artificial intelligence and blockchain to manage complex interactions between smart connected devices, individuals, government agencies, and the private sector.	Mixed	✓	MDPI	Alaeddini et al. (2023)
2023	"Blockchain-empowered federated learning: Challenges, solutions, and future directions"	Systematic analysis of 505 articles published between 2017 and 2023 about the integration of artificial intelligence and blockchain to manage complex interactions between smart connected devices, individuals, government agencies, and the private sector.	BC→AI	✗	ACM	Zhu et al. (2023)
2022	"Blockchain-enabled federated learning: A survey"	Survey on the integration of blockchain in federated learning. The authors discuss the advantages of employing a distributed environment such as authenticity, Byzantine resilience, persistence, and anonymity, while at the same time examining the resistance of several attacks.	BC→AI	✗	ACM	Qu et al. (2022b)
2022	"Blockchain for deep learning: review and open challenges"	A review of existing blockchain-based deep learning frameworks mainly targeting healthcare, vehicular networks, cellular traffic management, and blockchain safety and protection from adversarial attacks.	Mixed	✗	Springer	Shafay et al. (2022)
2022	"Fusing Blockchain and AI With Metaverse: A Survey"	A study that describes the characteristics of the ecosystem of metaverse and the current state of the art of its integration with Blockchain and AI solutions.	Mixed	✓	IEEE	Yang et al. (2022)
2022	"Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review"	The authors focus on how blockchain and AI can support the decentralized energy trading and decision making processes in the smart grids for facilitating prosumers to participate in energy markets.	Mixed	✓	Elsevier	Hua et al. (2022)
2021	"Federated learning meets blockchain in edge computing: Opportunities and challenges"	A study on the integration of blockchain and federated learning in mobile-edge computing. The authors identify common issues, such as communication cost, resource allocation, incentive mechanism, security and privacy protection, and discuss relative solutions.	BC→AI	✓	IEEE	Nguyen et al. (2021)
2021	"Deep reinforcement learning for blockchain in industrial IoT: A survey"	A survey that summarizes and analyzes the applications of blockchain and machine learning in Industrial IoT from three important aspects: consensus mechanism, storage and communication.	AI→BC	✓	Elsevier	Wu et al. (2021)
2021	"Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey"	The survey presents state-of-the-art communication technologies in vehicular networks along with their applications as well as novel techniques exploiting machine learning, mostly for defense purposes.	Mixed	✓	IEEE	Dibaei et al. (2021)
2021	"The Applications of Blockchain in Artificial Intelligence"	Comprehensive review of how blockchain can benefit AI: from secure data sharing (for model training), preserving data privacy, and supporting trusted AI decision and decentralized AI.	BC→AI	✗	Hindawi Limited	Wang et al. (2021a)
2021	"Blockchain for securing AI applications and open innovations"	Meticulous recovering and analysis of published documents about AI and BC. It mainly focuses on how BC components such as smart contracts, distributed networks and shared ledgers can help to mitigate problems and attacks common in AI applications.	BC→AI	✗	MDPI	Shinde et al. (2021)
2021	"Artificial intelligence and blockchain: A review"	A study with a clean structure that analyzes how BC can be integrated into various applications, with an insight on the cloud.	Mixed	✗	Wiley Online Library	Hussain and Al-Turjman (2021)
2021	"Machine learning in/for blockchain: Future and challenges"	Short review of works integrating AI and BC for specific applications, considering some supervised/unsupervised learning problems with and w/o deep learning, federated learning and some applications using reinforcement learning in the IoT domain. Interesting analysis of possible future research challenges.	Mixed	✗	Wiley Online Library	Chen et al. (2021)
2021	"Coalescence of Artificial Intelligence with Blockchain: A Survey on Analytics Over Blockchain Data in Different Sectors"	Short review on how security provided by blockchain to the data in the sectors of medical healthcare, IoT, and cryptocurrency has accelerated the usage of AI-powered analytics.	Mixed	✓	Springer	Singhal et al. (2021)
2020	"On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda"	A review on the convergence of AI and DLT. They explore AI for DLT in three different groups: security, automated referee and governance, and privacy-preserving personalization.	Mixed	✗	IEEE	Pandl et al. (2020)

(*continued on next page*)

Table 3 (*continued*).

2020	"Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology"	In-depth study of security issues associated with IoT and possible mitigations, using also blockchain and AI (separately).	Mixed	✓	Elsevier	Mohanta et al. (2020)
2020	"Survey on Blockchain and Deep Learning"	The survey analyzes works using both AI and BC on five specific topics: infrastructure, finance and trade, transportation and logistics, smart contract, and information security.	Mixed	✓	IEEE	Zhang et al. (2020)
2020	"Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city"	It includes integrated blockchain-AI ongoing projects.	Mixed	✓	Elsevier	Singh et al. (2020a)
2020	"A Review of Blockchain in Internet of Things and AI"	Review on how BC technology can solve problems such as single point of failure, security, privacy, transparency, and data integrity, typical of IoT centralized systems. One short chapter mentions how AI can be integrated into BC and applications using IoT.	Mixed	✓	MDPI	(Atlam et al., 2020)
2020	"A Systematic Literature Review of Integration of Blockchain and Artificial Intelligence"	Systematically collection of all papers published that integrate both AI and BC. They aim to answer to 3 research goals: which are the latest studies, what are the use cases and which application can benefit from this integration	Mixed	✗	Springer	Ekramifard et al. (2020)
2019	"Blockchain for AI: Review and Open Research Challenges"	Detailed analysis of blockchain for AI: types of BC, consensus algorithms, infrastructures, decentralized AI operations and applications.	BC→AI	✗	IEEE	Salah et al. (2019)
2019	"Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward"	Systematic review paper for ML adoption in BC. They separate papers according to goal-oriented, layer-oriented, countermeasures and smart applications.	Mixed	✗	IEEE	Tanwar et al. (2019)
2018	"AI and blockchain: A disruptive integration"	The authors show how AI and BC are a perfect match to mitigate each other weaknesses. In particular, they show how BC can help AI for Secure data sharing, explainable AI and Coordinating untrusting devices, while using AI on BC can help with scalability, personalization and governance.	Mixed	✗	IEEE	Dinh and Thai (2018)
2018	"Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare"	Healthcare application focused review exploring advances in BC and AI and their possible interactions. The authors pay significant attention to the cost of data acquisition, and/or generation, and data analysis.	Mixed	✓	Impact Journals, LLC	Mamoshina et al. (2018)

learning always involves the training of a machine learning model, this might not be the final purpose. In the context of blockchain, the training requirement can be integrated into the consensus algorithm, contributing to the criteria for the election of the publisher of the next block, for example by evaluating the goodness of the proposed models.

Edge computing, on the other hand, shifts computational tasks closer to data sources, reducing latency and enhancing real-time decision-making capabilities. The combination of these two concepts is particularly intriguing due to their potential to create efficient, privacy-conscious, and decentralized AI solutions. The integration between federated learning, blockchain and edge computing is particularly well-suited for tasks such as data sharing, content caching and crowdsensing (Nguyen et al., 2021).

Another concept closely related to all these topics is digital twins. Digital twins are virtual representations of physical objects, systems, or processes. They are enriched with real-time data and simulations to mirror the behavior and attributes of their real-world counterparts. Digital twins provide insights, enable predictive analysis, and facilitate optimization by allowing stakeholders to interact with and understand the virtual model. They can be particularly useful in the Industrial Internet of Things (IIoT) context (Xu et al., 2023), and when connected in a network they can be combined with both federated learning and AI to improve automation, privacy, and security (Qu et al., 2022a).

4.2. Healthcare

Artificial intelligence has been extensively used on medical data, including patient data, medical research, and clinical trials. Machine learning techniques can help healthcare providers to make better decisions and improve patient outcomes, by identifying patterns and making predictions about diseases and treatments. AI can also be used to develop personalized treatment plans based on a patient's unique health profile. In this context, Blockchain can be used to securely store and share medical data, such as patient records and clinical trial data, across different healthcare providers and systems. This approach can improve data integrity and accuracy, as well as patient privacy and security. Blockchain can also enable more efficient and transparent transactions between different parties in the healthcare ecosystem, such as insurance companies, healthcare providers, and patients. In particular, wearable smart devices are becoming more and more ubiquitous in our everyday life.

The usage of such devices has made the process of collecting medical data easier. All these data are collected, shared, and managed through Electronic Health Records (EHRs). The privacy, confidentiality, and consistency of these records are fundamental requirements from an IT point of view (Andrew et al., 2023). Moreover, the amount of data collected is larger than what a single and *classic* database can handle. To tackle this issue, a lot of papers proposed to use blockchain-based technology to store EHRs. Once data have been stored, it is straightforward to think of a way to use them in order to prevent/predict the presence of diseases. In this case, AI comes in help, thanks to its ability to process large volumes of data in real-time.

Examples of the Blockchain - AI integration for Healthcare can be found in Aich et al. (2021), Bhattacharya et al. (2021). Aich et al. (2021) tackled the problem of sharing EHR without privacy issues, allowing global and real-time usage. The privacy issues are addressed using blockchain technology — which provides privacy by design. Data are available globally and for real-time usage thanks to the adoption of the Federated Learning technique. Federated Learning is a Machine learning-based approach that trains the models in a decentralized way without losing privacy. The proposed model is structured as follows. Each university, hospital, etc. which owns some medical data, proceed to train some particular AI model with their data—with no privacy leaks. Once all the models are trained, they are sent to the federated server which averages them and creates a final model. This model is then interrogated by the Blockchain ecosystem in any case it is required. Hence, privacy is preserved both in the training phase (since each agent trains its own model without sharing the data) and during the fetch time thanks to the Blockchain technique. To the best of our knowledge, the model has not been implemented yet. Anyway authors in Aich et al. (2021) think it could be a good architecture to share and fetch clinical data without privacy issues.

A similar problem is addressed also in Bhattacharya et al. (2021). Starting from the idea that cloud services are too malicious attacks-prone, blockchain is suggested as a solution for security issues. The access to the blockchain where data are stored is handled via lattice-base cryptography. The authors also refer to this as the *first phase* of the technique. The *second phase* is the adoption of Deep Learning as-a-Service (DaaS) to predict future diseases starting from the EHRs datasets. The model adopted to solve this task is an LSTM trained over data in the blockchain. The first and the second phases together are referred to as *BinDaaS* architecture. The authors run tests over parameters like accuracy, mining time, and computation costs. The results showed that *BinDaaS* outperforms similar architectures with respect to all the aforementioned benchmarks.

Wearable devices are not the only type of technology allowed to collect medical data. For example, information can be obtained via IoT devices. Internet of Medical Things, IoMT for short, is the family of IoT appliances indicated for medical purposes (Kashani et al., 2021). These types of devices are usually split into three families:

1. in-body: in which we have all the wearable devices capable of gathering medical information;
2. in-home: all the devices that are installed in the houses of the patients to monitor their conditions. For example, we can have smart oxygen tanks or smart beds;
3. in-clinic: in this last category we find all the smart devices installed in the hospitals. For example monitors capable of collecting and sharing medical images taken from patients.

Privacy, security, and real-time usage are among the main problems in IoMT. In Veeramakali et al. (2021), the problem of intelligent diagnoses using data gathered in the IoMT is tackled. The model proposed, called optimal deep-learning-based secure blockchain (ODLSB), is composed of three major phases:

1. secure transaction,
2. hash value encryption,
3. medical diagnosis.

The first two steps are obtained using blockchains' by-design properties. The last step is accomplished using an optimal deep neural network (ODNN) used as a classification model. Performances of such models have been studied in the use case of healthcare image transmission and analysis. The results obtained showed a value over 90% for both sensitivity and accuracy.

The problem of security in medical image transmission has been tackled also in Alqaralleh et al. (2021). In this paper, the authors designed a deep learning (DL) with blockchain-assisted secure image transmission and diagnosis model for the IoMT environment. The presented model comprises a few processes namely data collection, secure transaction, hash value encryption, and data classification. As in the above cases, the first three processes are done using blockchain properties together with encryption techniques. The last process, namely the data classification, is done through a Deep Belief Network (DBN) used for the classification process. A DBN is a particular neural network architecture made of Boltzmann machines. In each layer we have both a visible and a hidden layer.

An extensive set of simulations is carried out to evaluate the proposed model. The outcome shows that the technique can reach both sensitivity and accuracy greater than 96%.

4.3. Internet of Things (IoT)

Traditional IoT systems typically rely on a centralized, cloud-based architecture. The data gathered from interconnected devices is sent to the cloud for processing, analysis, and subsequent transmission back to the devices for further action. Although the advent of machine learning analytics brought IoT and AI together, the centralized architecture still faces scalability issues and weaker network security. Fortunately, the decentralized architecture of blockchain technology offers a solution to this problem (Chen et al., 2020; Saxena et al., 2021; Sengupta et al., 2020).

Despite the introduction of blockchain, two main problems of IoT devices still remain. On the one hand, we want to collect the greatest amount of data without using too much energy and without requiring too much sensing range in the devices. On the other hand, data security and privacy have to be guaranteed. In Liu et al. (2019) the authors propose a model to address both problems. The proposed scheme is a combination of the Ethereum blockchain and deep reinforcement learning. The former is used to solve the security/privacy problem, while the latter is exploited to achieve maximum performance with respect to the amount of collected data.

The same set of problems has also been taken into account in Lu et al. (2020). In this case, private data sharing is obtained through federated learning techniques. For what concerns energy consumption, it is kept within correct ranges by incorporating federated learning into the permissioned consensus blockchain method.

Another approach to addressing the same problems has led to the development of *BlockDeepNet* (Rathore et al., 2019b). Such a model is based on blockchain and deep learning. Collaborative DL is obtained at IoT device level, while the problem of security is issued with blockchain.

In both cases (Lu et al., 2020; Rathore et al., 2019b) the models proposed have been implemented and tested in real-time scenarios. In the first case, while the performances were quite good, the authors think that the usage of AI-based techniques to ensure privacy is still an open problem. The main reason behind this statement is the following: the tested models were trained on a predefined set of possible attacks. Hence, if new attacks were designed, there would be no assurance that the federated learning models would not be deceived.

The authors in the second case acknowledge the high computational demands of DL tasks when applied at the IoT device level. Hence, they suggest avoiding applying BlockDeepNet in devices with low computational power, and enhancing the architecture with an offloading mechanism wherein devices with low computation power can offload their DL task to the edge server via blockchain transactions. In this way, an edge server takes care of DL tasks, allowing low computational power devices to take part in the BlockDeepNet.

A similar solution is presented in Zhao et al. (2023). The authors exploit the "Baas" (blockchain as a Service) paradigm, which allows developers to avoid directly dealing with the blockchain-based IoT system, where the blockchain complexity involves high levels of maintenance and monitoring. They propose a *Proof of Evolutionary Model* (PoEM) consensus protocol based on federated learning, where the goal is to solve constrained learning to rank problems using supervised machine learning algorithms. While PoEM exhibits the same linear complexity for communication time as other classical approaches, the reduced model size (1 MB) allows to store it even on devices with limited storage and computing capability.

Other proposals try to *remove* the computationally heavy components of IoT devices. For example, in Luong et al. (2017), the authors took into account the idea of adopting Edge computing, offered by the Edge Computing Service Provider, to offload mobile devices from some heavy tasks — like mining a blockchain block. This kind of approach creates the issue of ensuring incentive compatibility and individual rationality. The proposal was to use an optimal auction based on deep learning for the edge resource allocation.

4.4. Internet of Vehicles (IoV)

One of the most promising and interesting technologies of the last years is *Internet of Vehicles* (IoV). Academy, government, and industry have been focusing their efforts on making transportation not only more efficient, but safer. Thousands of people, if not millions worldwide, die every year because of car accidents. The main goal of IoV is to create a network connecting different types of vehicles that gather local information and can exchange data both with other vehicles in proximity, and with an underlying infrastructure. Even if not all vehicles are connected to this network, collecting and analyzing enough data still allows for the prevention or reduction of potential crushes and the creation of a more efficient transportation system, by suggesting optimal routes or providing information such as expected time of arrival.

Internet of Vehicles is directly connected with the great advances achieved in the field of *Connected and Automated Vehicles (CAVs)* (a.k.a., connected and autonomous vehicles and driverless cars). This technology has great potential as it offers many benefits, such as reducing traffic accidents, enhancing quality-of-life, and improving the efficiency of transportation systems (Elliott et al., 2019). Autonomous driving can result in higher throughput due to reduced distance between vehicles, lower car insurance premiums, and decreased costs for traffic enforcement departments. One of the most advantageous solutions, though, would be to exploit car-sharing, as it would directly imply reducing the number of cars per family, with the associated costs. A driverless car can return home by itself, ready to be used by other individuals in the family, or it can be even rented for a certain time slot or trip (Bajpai, 2016). A more efficient transportation network also directly implies reduced parking lot space and better alternatives to public transportation for people who do not have a driving license.

In order to exchange information, vehicles use networks commonly called *Vehicular ad hoc networks* (VANETs). They exploit wireless networking technology such as DSRC (Dedicated Short Range Communication) and LTE or 5G, where different types of communication are separated according to which parties are exchanging data. In particular, some of the communications involved can be classified as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). These last can be further separated into vehicle-to-pedestrian (V2P) and vehicle-to-everything (V2X). The use of vehicle communications could potentially reduce and/or eliminate up to 80% of crashes of any type from non-impairment (NHTSA, 2017). The architecture of modern VANETs is divided into perception, network, and application layers. The perception layer includes all the sensors and input sources used by the vehicles to collect local data. The network layer covers communication technology standards and protocols, and the security of the system. Finally, in the last layer applications are usually divided according to their purpose, for example, we have safety-related applications, including collision warnings and other notifications, traffic efficiency, concerning suggested speed, route and other navigation information, and entertainment or comfort applications.

Blockchain has been proposed as the perfect technology to support IoV, not only for VANETS (Saad et al., 2022; Grover, 2022), but also for transportation systems in general (Singh et al., 2022). Indeed, the decentralized nature of IoV makes it the perfect candidate for a blockchain-based approach. Multiple advantages are coming from adopting this technology: blockchain can be used to secure and manage data in the Internet of Vehicles (IoV) ecosystem by providing a tamper-proof record of all transactions. This can ensure that all parties have access to the same information, making the data more transparent and traceable. At the same time, it can be used to secure the identification and authentication of vehicles and their components, ensuring that only authorized parties can access the data and resources of the IoV ecosystem.

In this context, machine learning plays an important role also in detecting cybersecurity attacks on electric and intelligent vehicles, and in protecting in-vehicle networks, as well as inter-vehicle communications (Dibaei et al., 2021; Li et al., 2023). For instance, AI-based approaches can be used to classify network traffic into normal and malicious ones for the identification of unexpected patterns and anomaly detection (Li et al., 2019).

4.5. Smart cities

A broader application area that leverages both IoT and IoV is *smart cities*. Smart cities consist of strategies and solutions aimed to enhance the quality of life for citizens, by integrating information technology in various aspects of daily life. This requires collecting and managing a large amount of data coming from different sources, such as smart connected devices, individuals, government agencies, and the private sector (Alaeddini et al., 2023). Many researchers already propose the integration of AI and blockchain to tackle different problems, such as e-government (Kassen, 2022), urban mobility (Singh et al., 2022), healthcare (Rajawat et al., 2022), water management (Ktari et al., 2022), waste management (Chen, 2022), clean energy production and consumption, energy saving (Li et al., 2022), payment (Rahman et al., 2019), housing (Samuel et al., 2022), safety (Rawat et al., 2023), and accessibility (Sundaresan et al., 2021). Recent research shows how the integration of AI and Blockchain can address issues such as security, scalability, privacy, sustainability, and more (Badidi, 2022; Singh et al., 2020a).

There is no formal and commonly accepted definition of smart cities, and most of the time the related literature either refers to IoT systems improved by blockchain and artificial intelligence technology (Sharma et al., 2021), or the authors do not explore how actually AI is exploited (Salha et al., 2019). A higher-level approach instead consists in defining possible frameworks exploiting both blockchain and AI, for various purposes. Authors in Kumar et al. (2021) propose a Trustworthy Privacy-Preserving Secured Framework (TP2SF) for smart cities that ensures a higher level of security. They deploy a blockchain-based enhanced Proof of Work (ePoW) paired with Principal Component analysis (PCA) to transform data into a new reduced shape, for preventing inference and poisoning attacks. They also exploit an optimized gradient tree boosting system (XGBoost) for intrusion detection. Another framework solution adopts deep learning at the cloud layer to enhance production, automate data analysis, and increase the communication bandwidth of the smart factory and smart manufacturing applications in smart cities (Singh et al., 2021).

In a similar fashion, Serrano in Serrano (2022) presents a model using various AI techniques to validate and verify data marketplace. Live and static data streams are collected from smart buildings, infrastructure, cities, or real estate systems to address both digital and data challenges. The model applies a hierarchical process for data verification and data validation, by defining three different levels. The first level exploits classification algorithms that include naive Bayes, decision trees, random forests, support vector machines, and k-nearest neighbors to perform data selection, retrieval, and filtering, and to guarantee that the data are real and authentic. The second level uses unsupervised learning techniques including k-means, fuzzy, or hierarchical to perform data analysis and to report uncompliant values that do not meet a predefined threshold, range, or rule. This kind of verification can be particularly relevant for insurers, property managers, or operators. The last level makes predictions by using regression algorithms that include linear regression, lasso regression, logistic regression, multivariate regression, and multiple regression, which can be useful to asset managers or property developers. The author demonstrated that combining private Ethereum blockchain and smart contracts with AI can successfully deliver value-added services in a decentralized network.

4.6. Decentralized Finance (DeFi)

DeFi stands for Decentralized Finance, which is a new financial system that is built on top of blockchain technology. In contrast to traditional finance, which relies on centralized financial institutions such as banks and governments to manage financial transactions, DeFi aims to create a more open and transparent financial system that is accessible to anyone with an internet connection. DeFi platforms use smart contracts as self-executing contracts with the terms of the agreement between buyer and seller. Smart contracts can be used to create financial instruments like loans, insurance, and savings accounts, among others. These instruments can then be traded on decentralized exchanges, which allow users to exchange assets without the need for an intermediary. Even if DeFi is often associated with cryptocurrencies like Bitcoin and Ethereum, it is more than just cryptocurrencies: it represents a wide range of financial products and services that are built on top of these blockchain platforms.

Examples of popular DeFi applications are:

- Decentralized Exchanges (DEXs): DEXs (such as Uniswap, SushiSwap, and Curve Finance) allow users to trade a wide range of cryptocurrencies in a decentralized and trustless manner, without the need for a central authority or intermediary.
- Lending Platforms: DeFi lending platforms allow users to lend or borrow cryptocurrencies without the need for an intermediary like a bank. DeFi lending platforms like Aave, Compound, MakerDAO and Dharma use smart contracts to facilitate decentralized lending and borrowing, reducing costs, friction, and delay in such processes (Chen and Bellavitis, 2020).
- Stablecoins: Stablecoins are cryptocurrencies that are pegged to the value of a real-world asset like the US dollar, gold, or other cryptocurrencies. Examples of popular stablecoins include Tether (USDT), USD Coin (USDC), and Dai. Even if they are not Defi applications, they are often used by DeFi apps to solve the problem of volatility typical of other cryptocurrencies (Chen and Bellavitis, 2020).
- Prediction Markets: Prediction markets are platforms that allow users to bet on the outcome of events like political elections, sports matches, and other future events. Examples of DeFi prediction markets include Augur and Gnosis.
- Insurance: DeFi insurance platforms provide insurance products and services using smart contracts. Examples of DeFi insurance platforms include Nexus Mutual and Etherisc.
- Yield Farming: Yield farming is a way to earn rewards in the form of cryptocurrencies by providing liquidity to DeFi platforms. Examples of yield farming platforms include Yearn.finance, Harvest Finance, and SushiSwap.

One of the most important roles in DeFi is played by price oracles. An oracle is a system that provides off-chain data to on-chain smart contracts. Data come from real-world events such as price feeds, weather data, stock price changes, and much other information necessary for executing complex financial transactions e.g., lending, borrowing, and trading. Examples of DeFi oracle systems include Chainlink, Band Protocol, and API3, among others (Liu et al., 2021b). A relevant type of oracles used in the DeFi ecosystem is price oracles, which are used to determine the value of various digital assets, such as cryptocurrencies, stablecoins, and synthetic assets (Caldarelli and Ellul, 2021). Trustworthiness of oracles is of crucial importance, and even for this task, AI can come to aid (Taghavi et al., 2023).

DeFi applications using AI. The use of AI in DeFi is still in its early stages, but it has the potential to transform the DeFi landscape by making it more efficient, secure, and accessible. AI models can be used to improve many aspects, like risk assessment for lending companies (Mhlanga, 2021), optimize trading decisions by identifying patterns and trends in the market data or suggest customized investment strategies and even monitor the market in real-time and adjust prices based on supply and demand to ensure liquidity.

Such strategies are already implemented by many companies, like AnChain.AI (Anon, 2023a), a platform launched in 2018 that uses AI for security, risk, and compliance. It offers multiple solutions, ranging from enhancing smart contracts security to anti-money-laundering strategies that connect cryptocurrency to real-world entities, enabling securing crypto assets and quantifying risk.

DeepDAO (Anon, 2023b) is a DeFi application that is focused on providing insights and analytics on decentralized autonomous organizations (DAOs) (Faqir-Rhazoui et al., 2021). Decentralized autonomous organizations are organizations that are run by a decentralized network of stakeholders using blockchain technology for decision-making and governance. DAOs are unique in that they are not controlled by a central authority or hierarchy, but instead, operate through a consensus-based voting system. Members of a DAO typically hold governance tokens, which entitle them to vote on proposals and other matters related to the organization. DAOs can be used for a variety of purposes, such as managing shared resources, allocating funds to projects or initiatives, or facilitating community-driven decision-making processes. By leveraging the power of blockchain, DAOs can operate in transparently and democratically, with all members having an equal say in the decision-making process.

The DeepDAO platform allows users to track and analyze various metrics related to DAOs, such as their performance, voting patterns, and governance structure. The platform provides a comprehensive database of DAOs, allowing users to search for and compare different organizations based on a range of criteria. DeepDAO aims to provide greater transparency and insight into the world of DAOs, helping users to make more informed decisions about which organizations to support or participate in. DeepDAO is not only the most comprehensive dataset of DAO participants, but it also uses both rule-based queries and sophisticated machine learning algorithms to create time series data, insights, and predictions for multiple use cases. A simpler, non-commercial application for DAO analysis has been recently proposed by Arroyo et al. (2022).

Another decentralized application strictly related to AI is SingularityNET (Kolonin, 2023; Anon, 2023c). SingularityNET is a platform for artificial intelligence (AI) that aims to facilitate the creation, sharing, and monetization of AI services and applications. The platform is built on blockchain technology, which enables secure and transparent interactions between AI agents and allows developers to access a global market for their AI services. Moreover, it uses AI to optimize the allocation of computing resources and to improve the accuracy of AI algorithms. Even if SingularityNET is not considered a DeFi (decentralized finance) application in the traditional sense, it is still built on blockchain, and it is focused on creating a decentralized marketplace for AI services and applications rather than financial services. SingularityNET offers a marketplace for AI services that allows developers to sell their AI algorithms and applications to other developers, businesses, and individuals. The platform also includes tools and resources for developing and deploying AI services, as well as a community of developers, researchers, and AI enthusiasts. One of the key goals of SingularityNET is to create a decentralized AI network that is more accessible, democratic, and beneficial for everyone, rather than being controlled by a small number of powerful companies or institutions.

GameFi. GameFi is a new subset of DeFi that combines gaming and decentralized finance using blockchain technology. It allows players to earn cryptocurrency by participating in various gaming activities, such as battling, breeding, and trading digital assets. These kinds of games implement a new concept, known as Play-to-Earn (P2E), where the players are offered economic incentives to play. GameFi platforms typically use AI to optimize game mechanics, personalize game experiences, and manage in-game assets. GameFi platforms (such as Aixie Infinity, The Sandbox, My Neighbor Alice and Spliterlands) use AI algorithms to analyze player behavior and preferences and create a personalized gaming experience for users. In some cases AI also helps to manage in-game assets, such as digital pets or player cards, ensuring that they are balanced and valuable. Additionally, AI can create personalized game experiences for users based on their preferences and behavior (Kiong, 2021).

Blockchain technology also plays a vital role in GameFi by enabling decentralized markets for in-game assets and creating DAOs that govern the rules of the game. Blockchain technology allows for decentralized markets for in-game assets, enabling players to buy, sell, and trade assets securely and transparently. DAOs governed by blockchain technology ensure fairness and transparency in GameFi by creating decentralized autonomous organizations that manage the rules of the game (Proelss et al., 2023).

However, GameFi also poses some challenges. Ensuring data security and platform stability is crucial for the success of GameFi platforms. Regulatory uncertainty and scalability issues need to be addressed to fully realize the potential of GameFi. Nevertheless, with the right balance of AI and blockchain technology, GameFi has the potential to revolutionize both the gaming and DeFi industries.

4.7. Cryptocurrency

Today there are thousands of different cryptocurrencies in the world, but they all share the same properties: they are decentralized (not controlled by any authority or bank), they are based on blockchain technology and they use cryptography to encrypt their coins, which are usually stored in digital wallets. Cryptocurrencies are based on coins and tokens. While they are not the same thing, some of their functionalities overlap. Coins are native to their blockchains: they are intended as a form of currency and, if the protocol is using PoW, they can be mined. Like coins, tokens are digital assets, but they are usually implemented on the blockchain using a certain standard. For example, the Ethereum blockchain has a native currency called Ether and uses smart contracts that implement the ERC-20 standard to define fungible tokens.

When talking about coins, we are usually referring to Bitcoins or Ether, while all the other types of cryptocurrencies are called altcoins (alternative coins), which can be native coins, but also stablecoins, security tokens and utility tokens.

In the context of cryptocurrencies and AI, there is a significant body of literature exploring the intersection of these two fields. Machine learning techniques are largely exploited to address two different types of problems: cryptocurrency price prediction and attack detection (see Section 5.1). Even though in this survey we mainly consider methods related to the two most known cryptocurrencies at the moment e.g., Bitcoin and Ether, given enough data the same techniques can also be applied to other cryptocurrencies.

In particular, there is a significant number of proposals in the literature for models to predict the price of Bitcoin. Main machine learning techniques used for price prediction are logistic regression, SVM, deep learning, reinforcement learning and gradient boosting (Khedr et al., 2021). In Dixon et al. (2019), the authors use transaction graph activity for the volatility of intraday Bitcoin prices, which refers to the amount of variation or fluctuation in the price of Bitcoin within a single day. This is achieved by studying the impact of sub-graphs called "chainlets" having an influence on Bitcoin price predictions and further characterizing the types signifying extreme losses. They fit a generalized autoregressive conditional heteroscedasticity (GARCH) model, popular in financial econometric literature, with these extreme chainlets to model the impact on the intraday process and volatility.

On the other hand, in Besarabov and Kolev (2018) the authors addressed the problem of asset prediction, which consists in forecasting the future price or value of a certain currency. In particular, they started by noticing that standard models used to solve this kind of problem take advantage of Long-Short Term Model (LSTM). They tried to exploit the properties of such models together with CNNs to increase the accuracy. What they achieved is a four times smaller error. Moreover, using other techniques such as blockchain account distribution histograms, spatial dataset modeling, and a convolutional architecture, the error was further reduced.

As for Bitcoin, machine learning techniques can be used also to predict the price of Ether. For example, in Politis et al. (2021) the authors try different state-of-the-art deep learning models for sequence prediction, including LSTM, Gated Recurrent Units (GRU), Temporal Convolutional Networks (TCN) as well as model ensembles for this task. With the ensemble, they were able to achieve an accuracy of 84.2% after one day and 78.9% after one week. A similar work (Poongodi et al., 2020) exploits linear regression (LR) and support vector machine (SVM) to achieve even higher accuracy. Authors in Kim et al. (2021) also use SVM, but they also train a neural network for the prediction. Moreover, they consider multiple sources of data, such as macroeconomy factors and information from other blockchains. Their custom NN can predict Ether price with an RMSE of 0.068. Notice that even if these are only some of the methods used for Ether price prediction, to our knowledge there are no currently available studies that take into consideration the recent update to Proof of Stake, and if or how this has changed the stock price in Ethereum.

More in general, stock exchange prediction is a very active area for research, and one of the most important platforms in this regard is called Numerai. Numerai is a global hedge fund that uses artificial intelligence and machine learning to make investment decisions. The company operates as a decentralized, blockchain-based platform and its unique approach to machine learning involves creating a model based on many other machine learning models, to make more accurate predictions about stock prices. Indeed, it runs one of the most challenging existing data science tournaments, where data scientists from around the world can submit predictive models to help the hedge fund make better investment decisions. Participants in the tournament are rewarded with cryptocurrency prizes for their successful predictions. Numerai constantly updates its dataset with more than 100000 entries per week, each made by 310 features. The amount and quality of data freely available make the dataset the perfect ground to develop many types of AI models, and in particular, some of them have been publicly released (Singh et al., 2020b; Vasudevan et al., 2021; Singh and Sharma, 2018).

5. Artificial intelligence for blockchain

Due to the popularity of blockchain technology, the number of proposed applications and frameworks based on it has been growing exponentially. As blockchain deals with data integrity by design, it solves some of the most troublesome problems that ML algorithms usually have to deal with, such as errors in the dataset due to duplication, missing entries, and noise. The blockchain mechanism also incentivizes data sharing by rewarding miners. In this way, machine learning techniques can benefit from the large datasets available to extract meaningful patterns and information.

As the two technologies can support each other, they can also interact in many possible ways. This survey focuses on how ML algorithms, and AI in general, can improve blockchain-based applications, not simply by performing a post-analysis on the data in the blocks, but by directly interacting with the blockchain protocol and actively participating in the decision-making process.

Integration between artificial intelligence and blockchain technology can occur at various components of a blockchain. Due to the intricate nature of the blockchain protocol, researchers have delineated distinct layers, often with slightly varying nomenclature (Xie et al., 2019; Homoliak et al., 2020; Belotti et al., 2019; Wu et al., 2019). These layers can be broadly categorized as:

- **Data Layer**: At the core of the blockchain architecture is the Data Layer. It consists of data blocks, each timestamped and linked using cryptographic hashes to create a continuous chain. Blocks are divided into headers containing metadata and bodies containing transactions. This layer ensures data integrity, immutability, and transparency.
- **Network Layer**: Above the Data Layer is the Network Layer, responsible for distributed communication among blockchain peers. This layer enables peer-to-peer networking, ensuring timely block distribution, forwarding, and verification. It facilitates the broadcasting of transactions, verification acknowledgments, and peer interactions.
- **Consensus Layer**: The consensus layer ensures that all participants in the blockchain network agree on the state of the blockchain. It determines how new transactions are added to the blockchain and how conflicts are resolved. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT).
- **Incentive Layer**: The Incentive Layer introduces the concept of economic motivation within the blockchain network. In decentralized systems like Bitcoin, this layer rewards participants, often miners, for their contributions. Rewards, typically in cryptocurrency, incentivize participation and secure the network. Conversely, penalties and deposits can also be enforced.
- **Contract Layer (Smart Contract Layer)**: The Contract Layer, also known as the Smart Contract Layer, brings programmability to the blockchain. It enables the creation of self-executing contracts, known as smart contracts, which automate processes based on predefined conditions. These contracts run on the network and are a cornerstone of decentralized applications, enabling dynamic interactions.
- **Application Layer**: The Application Layer represents the interface through which users interact with the blockchain network. It encompasses a wide range of use cases, including financial transactions, supply chain management, and identity verification. Decentralized applications (DApps) are built on this layer, utilizing the underlying layers' functionalities to provide innovative solutions across various industries.

These layers work together to create a functional blockchain system. However, it is important to note that the boundaries between these layers are not always strict, and in some cases, certain functions might overlap. Additionally, different blockchain platforms might have their own terminology or variations of these layers, but the general concepts remain relatively consistent across various blockchain implementations.

In this context, we focus on what kind of advantage or property can benefit from injecting AI models and algorithms in such a structure. We have conducted a comprehensive analysis to identify macro areas where artificial intelligence (AI) can augment blockchain-based applications, as illustrated in Fig. 3.

We have identified four key domains where AI integration proves highly advantageous within the blockchain ecosystem: security, smart contracts, consensus mechanisms, and auction/smart grid optimization. These AI techniques are strategically aimed at various layers within the blockchain's structural framework.

To begin, the realm of security and privacy enhancement through AI encompasses a substantial body of research. These methods permeate the entire blockchain structure and address diverse data aspects, extending across different layers of the blockchain itself. For instance, fraud detection techniques can leverage information stored both within the data layer and within the incentive layer, where regulations governing rewards and penalties are defined.

Moving on, the subsection dedicated to smart contracts covers methods associated with the contract layer. Here, the focus revolves around how AI contributes to the formulation, examination, and validation of smart contract code.

Furthermore, we delve into alternative consensus algorithms, which incorporate machine learning mechanisms targeting the consensus layer. An example of this is federated learning, as discussed in the preceding section, which is significant not for AI's assistance to blockchain, but for its influence in the opposite direction.

Lastly, we present methodologies and frameworks pertinent to auctions and smart grids. Unlike the studies outlined in Section 4, which predominantly inhabit the upper application layer, these approaches are included in this section due to their intricate interactions with lower levels such as the network layer. They directly alter the blockchain protocol to deliver specific advantages.

The interaction of AI with the blockchain is closely tied to its data. As we have defined, there are primarily three types of machine learning algorithms: supervised, unsupervised, and reinforcement learning. In supervised learning, the process involves classifying new observations after learning significant patterns from a large, pre-labeled dataset. This classification of new entries can uncover vulnerabilities, attacks, or malicious entities, and it can be integrated into the protocol at different layers to address such events.

Unsupervised learning and clustering can be applied in a comparable manner: through the aggregation of akin data, the potential to discern various behaviors arises. This facilitates the formulation of distinct regulations based on the grouping into which novel data aligns. Furthermore, this approach aids in anomaly detection, which is extensively harnessed to amplify security. It proves especially effective in cases where the availability of labeled data is unfeasible, even if it does not attain the same precision as supervised learning.

Reinforcement learning can be harnessed to learn varying policies, including the formulation of novel architectures and protocols within a blockchain. This process aims to enhance not only security and privacy attributes but also the overall operational efficiency of the blockchain.

In the subsequent sections, we delve into the myriad of AI-powered solutions proposed for each of these areas.

5.1. Security

Machine learning and deep learning approaches are largely exploited in the financial domain, not only in the decision-making processes for trading activities, payments and customer credit, but also and especially to fight criminal activities such as money laundering, tax evasion, ransomware, phishing, impersonation and many other frauds (Nicholls et al., 2021). According to CipherTrace, a cryptocurrency intelligence company owned by Mastercard, Decentralized Finance (DeFi) hacks are responsible for 60% of the total hack volume as of 2021.

Many types of attacks can be performed on a blockchain, in Table 4 we can see some of them, grouped according to their target.

These are only a few of the possible attacks and security issues related to blockchains, and it is impossible to address all of them in this survey. Fortunately, most of these issues can be efficiently identified using methods for anomaly detection, since anomalous behavior usually corresponds to possible attacks and malicious entities.

Even if most of the security problems in blockchain can be solved with anomaly detection techniques (Hassan et al., 2022a; Bugliesi et al., 2012; Bossi et al., 2003; Bernardi et al., 2008; Hillston et al., 2021), the number and type of possible problems are very large. Most of them are identified as methods for detecting frauds in Bitcoin/Ethereum, behavior pattern classification, framework design anomaly, and transaction relative similarity clustering.

A typical strategy to detect anomalies is to use supervised methods. By dividing available data according to the presence/absence of anomalies, it is possible to train various machine learning classifiers to learn the classification task, such as neural networks (NN), deep neural networks (DNN), convolutional neural networks (CNNs), support vector machine (SVM), and many others (Kim et al., 2022).

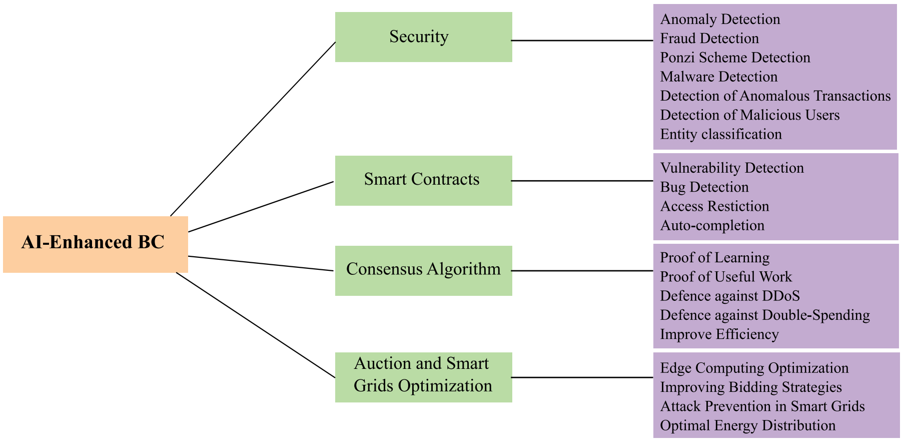


Fig. 3. Main contributions of AI algorithms to blockchain technology.

Table 4
Some of the most common attacks or vulnerabilities that can occur on blockchains.

Target	Possible attacks
Account	Anomalous peers, wallet theft, key theft, market manipulation cryptojacking
Transaction (Tx)	Tx tampering, currency/token theft, malicious tx, money mixing, double spending
Smart Contract	Honeypots, coin freezing, reentrancy, dependant tx execution, bytecode-based bugs
System	BGP hijacking, modifying logs, DDoS attack, divergent paths, malicious network requests
Consensus	Race attack, eclipse attack, 51% attack, balance attack, fork formation

Other solutions exploit clustering methods like k-means, deep belief network (DBA), and DBSCAN. The clusters are used to determine the behavior of new observations, based on the principle that the reconstruction error will be low for normal values and high for abnormal ones (Li et al., 2021; Iyer et al., 2019). In Li et al. (2021), the authors adopted a dataset containing data from the MIT-BIH Arrhythmia database (Hamilton and Tompkins, 1986). On the other hand, the testing phase in Iyer et al. (2019) was carried out using a dataset provided by the 2030 Wastewater Resources Group. The proposed model obtained a F1-score of 0.9048. In a similar way, methods like k-nearest neighbors (k-NN), local outlier factor and local probability outlier detect abnormal activities as inputs falling far from dense areas, which represent normal activities (Wang et al., 2021b). Generative models such as Generative Adversarial Networks (GANs) can model the complex high-dimensional distributions of real-world data, and derive adversarially learned features for the anomaly detection task. By using the reconstruction errors it is then possible to determine whether a data sample is anomalous (Zenati et al., 2018; Xia et al., 2022).

Authors in Zenati et al. (2018) tested their technique against a tabular and an image dataset. For the tabular data, KDDCup99 10% dataset was used—taken from the UCI machine learning repository. It contains data about network intrusions. For the image case, SVHN and CIFAR-10 were adopted. The F1-score of the proposed models was given only for the tabular case: the best value obtained was 0.9501.

The last category of models used for anomaly detection in blockchain involves reinforcement learning. Methods like Q-learning, Deep Q-learning, QR-DQN, and model-based value estimation can be trained for this task by rewarding the correct identification of blockchain anomalies (Pang et al., 2021). The datasets adopted by the authors for the testing phase, are manifold.

- UNSW_NB15 from network intrusion
- Annthyroid from disease detection
- HAR from human activity recognition
- Covertpe from forest cover type recognition

All the above-mentioned datasets are taken from Pang et al. (2019), Ting et al. (2017). Both papers tackle the problem of anomaly detection.

One of the most relevant problems in the crypto trading market is fraud. In particular, the problem of fraud detection in Bitcoin has been addressed in Harlev et al. (2018), Chen et al. (2018), Sun Yin and Vatrapu (2017). A possible cause of illegal activities is the complete anonymity ensured by blockchain. Hence, in Harlev et al. (2018), the authors attempted to reduce the anonymity of Bitcoin using a classifier. The training phase has been done using a cluster of already identified Bitcoin addresses. The work showed that by utilizing already identified and categorized addresses, it is possible to predict the type of an unknown cluster with 77% accuracy. This proves that the level of anonymity of the Bitcoin Blockchain is not as high as believed.

An illegal activity that Blockchain has somehow inherited from the real-world market is the Ponzi scheme. A Ponzi scheme is a pyramid-type fraudulent investment scheme that promises high returns to investors and pays returns to earlier investors using contributions from more recent investors. It relies on the constant inflow of new investors to generate returns for earlier investors, and it ultimately collapses when there are not enough new investors to pay returns to existing ones. In Chen et al. (2018), the authors proposed to address the problem of identifying and avoiding the Ponzi scheme in Blockchain using a regression tree. The result they obtained is the detection of Ponzi scheme contracts at the time of their creation. Moreover, they were also able to identify the existence of smart Ponzi schemes already running in the Ethereum chain.

Up to now, we only considered particular cases of fraud (Ponzi scheme) or ways to reduce illegal activities (anonymity). The authors of Sun Yin and Vatrapu (2017) proposed a ML-based technique to discover/estimate the percentage of criminal activities in the Bitcoin system. To maximize the probability of success, a total of 13 classifiers were trained. The four models that obtained a Cross-Validation accuracy higher than 75% are: Random Forests, Extremely Random Forests, Bagging, and Gradient Boosting. The other 9 models that were adopted can be found inside the Scikit-Learn[1] python package.

The model was able to find several components with malicious activities in the Bitcoin network. Similarly, a recent work (Nerurkar

[1] https://scikit-learn.org/stable/

et al., 2021) aims to uncover malicious users by implementing an ensemble of decision trees for supervised learning. They extract a dataset of 1216 real-life entities on Bitcoin and categorize them into 16 classes. They achieve classification accuracy equal to 0.91, but the misclassification errors are high for the classes with fewer examples.

The other most popular cryptocurrency is Ethereum and multiple works focused on fraud detection in this specific blockchain. In particular, two works specialize in identifying the DAO attack (Scicchitano et al., 2020; Kumar et al., 2020). In Scicchitano et al. (2020) the authors detect deviant behaviors on Blockchain by strengthening an encoder–decoder model to compute an outlier score for each observation. The work in Kumar et al. (2020) instead, focuses on identifying malicious accounts. In particular, they apply two distinct machine learning models according to whether the account is an Externally Owned Account (EOA) or a smart contract account. Their supervised models are able to separate fraudulent nodes and legitimate users with high accuracy.

A recent paper (Aziz et al., 2022) proposes a novel approach to detect anomalous transactions with high accuracy without being vulnerable to overfitting. The authors use a Light Gradient Boosting Machine (LGBM), a customized machine learning approach using gradient boosting algorithms that can detect anomalous transactions with high accuracy without being vulnerable to overfitting. Their solution outperforms other ML techniques such as Random Forest (RF), Multi-Layer Perceptron (MLP), and Extreme Gradient Boosting (XGBoost). The dataset that was taken into account for the tests is the Ethereum Classic, available at Kaggle website. The testing phase showed the best performances with the LGBM classifier, with a 0.9486 F1 score.

In Tan et al. (2021) the authors use a Graph Neural Network (GNN) to detect Ethereum frauds, by mining Ethereum-based transaction records. They use web crawlers to capture labeled fraudulent addresses, and then reconstruct a transaction network based on the public transaction book. After using an embedding algorithm to extract node features for identifying fraudulent transactions, the authors use a GNN to classify addresses into legal and fraudulent ones.

Among different possible frauds, one is related to malware, malicious software that can infect, reveal and steal a victim's files, as well as change the behavior of the infected computer.

Authors in Mohanta et al. (2020) propose a Deep Learning (DL) and Blockchain framework to detect malware attacks in Autonomous Vehicles with an accuracy of 97.56%. They adopt a classic approach, which consists of using a CNN (ResNet50V2) to classify binary code, previously converted into greyscale images.

The study in Alabdulatif et al. (2022) focuses on trying multiple AI techniques, such as logistic regression (LR), support vector machine (SVM), random forest (RF), perceptron, and Naive Bayes (NB) to find malware in smart healthcare systems. The malware-free data (classified by the AI models) are then passed to the blockchain for secure data storage.

Another example of malware related to blockchain technology is cryptocurrency mining malware, which forces the victim's computer to use its CPU to mine for the attacker. By using SVM, k-NN and random forest, authors in Handaya et al. (2020) were able to find this type of malware that also exploits fileless attack techniques, which are able to evade antivirus mechanisms. The database adopted for the tests is EMBER.

Machine learning algorithms are also largely adopted in IoT systems to improve their security (Majeed et al., 2021). BlockSecIoT-Net (Rathore et al., 2019a) is an architecture deploying several machine learning attack detection models at fog level. The local models are then merged with a model fusion strategy to detect attacks such as DDoS and ICMP/TCP flooding.

Certainly, the methods discussed in this section showcase how AI can be seamlessly woven into blockchain design. Anomaly detection techniques, ranging from supervised methods to clustering and generative models, can be directly integrated to monitor and swiftly identify unusual activities, fortifying security measures. Fraud detection, facilitated by AI-driven classification models, contributes to separating authentic from fraudulent transactions, leading to potential design modifications that prioritize thorough scrutiny of suspicious transactions. Preventing malware intrusions involves incorporating AI-driven analysis of data and code, which could prompt adjustments in the blockchain architecture to include real-time scanning mechanisms.

5.2. *Smart contracts*

Smart contracts are the key feature offered by Vitalik Buterin in the Ethereum blockchain. Developers use smart contracts in the development of a DApp (Decentralized Application) running in a dedicated space called Ethereum Virtual Machine (EVM). Sometimes DApps are simply called smart contracts. The programming language most used to implement smart contracts is Solidity, but there are alternative options, such as Vyper and Yul. Even if most smart contracts are developed on Ethereum, given their popularity and potential, many other blockchains have started to offer this feature (Ghosh et al., 2020). One of the most popular among permissioned blockchain infrastructures is Hyperledger Fabric (Androulaki et al., 2018), distributed by IBM. Hyperledger Fabric offers a modular and versatile design to satisfy a broad range of industry use cases. One of its main features is the possibility to develop smart contracts, which they call "chaincode", in various programming languages, such as Go, Javascript and Java.

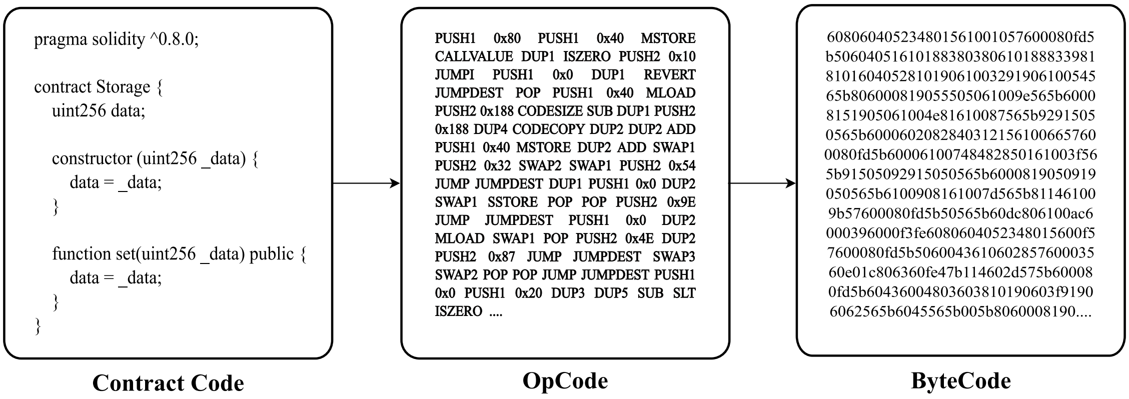
Decentralized application targets range from infrastructures, IoT, healthcare, financial care, logistics, telecommunication and more (Hewa et al., 2021). Since smart contracts are stored in the blockchain, there are both advantages and drawbacks. The immutability of the blocks makes it impossible to modify a smart contract that is already part of the blockchain, guaranteeing some degree of protection from malicious entities, while at the same time ensuring the fairness of the contract (Malakhov et al., 2022), free from possible technicalities typical of regular physical contracts.

At the same time, since the blockchain is public, it is also transparent and miners or other entities can take advantage of this to perform a wide range of attacks. Some of the most common vulnerabilities of Ethereum smart contracts are summarized in Table 5, but there are over 70 possible vulnerabilities currently identified (Vidal et al., 2023). Vulnerabilities can depend on programming errors that can be found in traditional programs, such as missing input validation, typecast bugs, use of untrusted inputs in security operations, unhandled exceptions, exception disorder, and integer overflow/underflow. There are also problems directly connected with smart contract programming, such as greedy contracts that remain alive and lock Ether indefinitely (Nikolić et al., 2018), allowing it to be released under no conditions, or unprotected selfdestruct instructions (see SWC-106 Anon, 2023d), where an attacker can call a smart contract's public function containing a selfdestruct to terminate the smart contract, resulting in a Denial of Service (DoS) (Lutz et al., 2021). Early detection of these kinds of problems is of critical importance to avoid the possibility of attacks.

Machine learning approaches to address these issues mainly consist of training deep learning models for early detection of vulnerabilities. Even if some solutions directly use the source code of smart contracts, this is not always publicly available, and for this reason, many works instead rely on bytecodes or opcodes, which can always be retrieved from the public blockchain. While there already exists non-AI methods for vulnerability detection such as Oyente (Luu et al., 2016), Mythril (Anon, 2019) and Securify (Tsankov et al., 2018), which mostly consist of symbolic execution and flow analysis, they usually require significant time for the detection (from a few seconds up to some minutes for a single vulnerability) and they are usually able to identify only a subset of all possible problems that might occur. A common approach consists of exploiting these methods together to perform vulnerability detection and label the smart contracts, contributing to dataset creation, which is used later during the training phase. Fig. 4

Table 5
Some of the most commonly found vulnerabilities in smart contracts.

Vulnerability name	Description
Integer overflow/underflow	Integer values in blockchain are unsigned, so the minimum is 0 and the maximum is 2^8. Some operations can make the value go beyond these limits, assigning a different value which may result in a different behavior of the smart contract.
Transaction-ordering dependence (TOD)	The sequence of transactions can be manipulated by an attacker.
Timestamp dependency	The timestamp is used as call condition, and miners can take advantage of this dependency by setting a particular timestamp, as they can freely change it within a 900 s span.
Callstack depth attack vulnerability	The number of invocations exceeds the space allocated for the pending requests.
Reentrancy vulnerability	External calls can be used to force the contract to execute reentrant code such as calling back themselves (which is what happened during the DAO attack in 2016).



```
pragma solidity ^0.8.0;

contract Storage {
    uint256 data;

    constructor (uint256 _data) {
        data = _data;
    }

    function set(uint256 _data) public {
        data = _data;
    }
}
```

```
PUSH1 0x80 PUSH1 0x40 MSTORE
CALLVALUE DUP1 ISZERO PUSH2 0x10
JUMPI PUSH1 0x0 DUP1 REVERT
JUMPDEST POP PUSH1 0x40 MLOAD
PUSH2 0x188 CODESIZE SUB DUP1 PUSH2
0x188 DUP4 CODECOPY DUP2 DUP2 ADD
PUSH1 0x40 MSTORE DUP2 ADD SWAP1
PUSH2 0x32 SWAP2 SWAP1 PUSH2 0x54
JUMP JUMPDEST DUP1 PUSH1 0x0 DUP2
SWAP1 SSTORE POP POP PUSH2 0x9E
JUMP JUMPDEST PUSH1 0x0 DUP2
MLOAD SWAP1 POP PUSH2 0x4E DUP2
PUSH2 0x87 JUMP JUMPDEST SWAP3
SWAP2 POP POP JUMP JUMPDEST PUSH1
0x0 PUSH1 0x20 DUP3 DUP5 SUB SLT
ISZERO ....
```

```
6080604052348015610010576000080fd5
b50604051610188380380610188833981
810160405281019061003291906100545
65b806000819055505061009e565b6000
8151905061004e81610087565b9291505
0565b6000602082840312156100665760
0080fd5b6000610074848285016100 3f56
5b91505092915050565b6000819050919
050565b6100908161007d565b81146100
9b57600080fd5b50565b60dc806100ac6
000396000f3fe608060405234801560 0f5
7600080fd5b5060043610602857600035
60e01c806360fe47b114602d575b60008
0fd5b6043600480360381019060 3f9190
6062565b6045565b005b8060008190....
```

Fig. 4. A simple example of an Ethereum contract written in Solidity and compiled into its relative OpCode and Bytecode.

shows the source code of a smart contract compiled into its relative bytecodes and opcodes.

In literature, many approaches use deep learning to address this problem. Inspired by some malware detection techniques, one possible method is to transform the source code of the smart contracts (or related bytecodes) into 2D images, which are then fed to a classical Convolutional Neural Network (CNN), such as in Huang (2018) and Hwang et al. (2022).

Authors in Wang et al. (2020) train different machine learning algorithms, such as boosting, random forest, SVM and k-NN, to detect 6 different types of vulnerabilities. They use 49502 real-world smart contracts from the Ethereum official website from which they extract 1619 dimensional bigram features from simplified operation codes to construct a feature space. They found that by using XGBoost for training the models and SMOTETomek for balancing the training set they can predict if a smart contract presents vulnerabilities with an F1-score over 96%.

Similarly, authors in Momeni et al. (2019) investigate the use of various machine learning techniques to identify 16 different types of vulnerabilities. Specifically, they use SVM, Random Forest, Decision Tree, and a custom NN and compare the results and execution time to traditional techniques such as static code analyzers (Mythril and Slither Feist et al., 2019). Results show that machine learning approaches can detect vulnerabilities with an average of 95% accuracy in less than one second, while static techniques can require more than one hour of processing. Another advantage of this approach is the use of Abstract Syntax Tree (AST) from Solidity source codes, which allows the model to be adopted for other languages and platforms without dependencies.

An interesting solution is proposed by Lutz et al. (2021), where they focus on model scalability by separating the relevant feature extraction process from the actual classification. They propose a multi-output RNN that achieves an average of 95% detection accuracy in terms of F1-score across eight vulnerability classes in 0.02 s and can be quickly adapted to the new vulnerability data.

Graph Neural Networks (GNNs) are one of the deep learning models that have recently been gaining attention. They are inspired by conventional NN, but they are designed to work on graph data. This approach has been exploited by Zhuang et al. (2020a), Liu et al. (2021a), Cai et al. (2023). In particular, Zhuang et al. (2020a) construct a contract graph to represent both syntactic and semantic structures of a smart contract function. They propose a degree-free graph convolutional neural network (DR-GCN) and a novel temporal message propagation network (TMP) to detect 3 types of vulnerabilities (reentrancy, timestamp dependence, and infinite loop). A similar approach is proposed in Liu et al. (2021a), where the authors focus on detecting three types of vulnerabilities on smart contracts from Ethereum and VNT Chain platforms.

Cai et al. (2023) construct a graph representation for a smart contract function with syntactic and semantic features by combining an abstract syntax tree (AST), a control flow graph (CFG), and a program dependency graph (PDG). They then train a Bidirectional Gated Graph Neural Network model with hybrid attention pooling to identify 9 different potential vulnerabilities in smart contracts. Their detection model can find vulnerabilities with a F1-score higher than 91%.

A different approach is proposed in Deebak and Fadi (2021), where the authors claim that another way to improve the privacy and security of smart contracts is by restricting access privileges. In detail, they use XGBoost to perform regression over a dataset of 72 thousand claim requests, to determine whether the client request is fraud or non-fraud.

Artificial Intelligence Generated Content (AIGC) is another area where AI can play a role in smart contracts. AIGC refers to the use of AI algorithms, such as Natural Language Processing (NLP) and Computer Vision (CV), to generate various forms of data, including text, images, and audio. A recent breakthrough in this field has been achieved by ChatGPT-3, a large transformer model developed by OpenAI.

ChatGPT-3 can perform a large variety of tasks, including grammar checking, serving as a virtual assistant or chatbot, language translation, and the ability to comprehend and generate code written in different programming languages. Even if it is a probabilistic model, thus not 100% reliable, it has the potential to be a useful tool for smart contract development, especially to help programmers understand pieces of uncommented code by providing easy explanations of what the code does.

5.3. Consensus algorithm

One of the key components of blockchain technology is the consensus algorithm, which ensures that all nodes on the network agree on the state of the ledger. However, traditional consensus algorithms can have limitations, such as slow processing times, high energy consumption, and susceptibility to malicious attacks.

To address these challenges, artificial intelligence can be used to improve the consensus algorithm in blockchain technology in many ways. One example of how AI can interact with the consensus algorithm is by optimizing the algorithm's parameters. Machine learning algorithms can analyze large amounts of data to identify the most effective parameters to use for a particular blockchain network. For example, AI can help to optimize parameters such as block size, block time, difficulty level, and consensus mechanism itself. This can lead to faster, more efficient, and more secure consensus algorithms. AI can also improve the fault tolerance of consensus algorithms. By analyzing the behavior of nodes on the network, AI can identify potential failures or malicious behavior. This can help ensure that the consensus algorithm remains stable and secure, even in the presence of faulty or malicious nodes. Another application of AI algorithms to the consensus deals with scalability. By analyzing network traffic patterns and predicting future demand, AI can help to optimize the consensus algorithm to handle increased traffic, without sacrificing performance or security.

An application of how machine learning can improve the consensus is proposed by Safana et al. (2020). The authors train a model to identify which parameters are relevant with respect to the time needed for the miners to find the nonce value. The criteria include time traffic, size, number of connected nodes, number of transactions and network size. As the results show there is a linear relationship between the increase in size and the average time taken to generate a block, this information can be used to enhance the mining efficiency of the protocol. In a similar approach, authors in Baniata et al. (2022) identify linear relationships between inputs and outputs of classical mining processes, which typically use Brute-force. They then develop two models to predict the solutions of the mining process—*nonces*. To evaluate the performances of the proposed algorithms, they measured the *success* of the models. With success, they refer to the event of a correct mining. Using more than 780k real Bitcoin blocks for training and testing, they obtained up to 70.5% success score, which outperforms the claimed 50% of a classical miner. The experiments proved that a miner that uses this approach can compute a correct solution for the tested mining problem faster than a classical miner.

Machine learning, and in particular deep learning, are largely adopted to solve a variety of tasks, ensuring high performance and accuracy. One of the most troublesome problems coming from training such models, though, is the heavy computational cost required. The availability of accelerating hardware, such as graphics processing units (GPUs), is imperative to train within a reasonable time all the machine learning models with a great amount of parameters. During the last few years, there has been a high demand in the GPU market due to the stock value of Bitcoin. Indeed, GPUs are not only necessary to train the many weights of a network in parallel, but also to test multiple values for a possible nounce at the same time. A smart solution to efficiently utilize this hardware for both purposes is to define a new consensus protocol that allows for the substitution of the unsustainable (Ogawa et al., 2018) and less useful PoW with other tasks, such as model training.

More specifically, the consensus algorithm *Proof of Learning (PoL)* (Jia et al., 2021; Bravo-Marquez et al., 2019) uses the computational power required by PoW for the training phase of a model, requiring miners to prove that they have correctly obtained a set of model parameters. In the distributed learning scenario, one of the miners acts as the prover while the model owner acts as the verifier. This strategy provides several benefits: it gives a new, more meaningful purpose to mining, and it also addresses the problem of transparency and explainability that is typical of AI models.

Another solution is named *Proof of Useful Work (PoUW)*. Under this category, we can find many works: in particular, in Ball et al. (2017) the nodes are asked to solve a wide array of computational problems, including Orthogonal Vectors, 3SUM, All-Pairs Shortest Path, and any problem that reduces to them. Authors in Loe and Quaglia (2018) developed a PoUW based on the Traveling Salesman Problem (TSP), since it is a NP-hard problem.

Similar to PoL, some works define a PoUW consensus algorithm that requires solving artificial intelligence tasks. Authors in Lihu et al. (2020) propose a solution that is more cost-efficient to a client than regular cloud machine learning training, as well as more useful than Bitcoin mining. In Merlina (2019) usefulness is achieved by the supervised training of neural networks. A related protocol was suggested by Mittal and Aggarwal (2020). They called their consensus schema *Proof of Deep Learning with Hyperparameter Optimization (PoDLwHO)*, where they train deep learning models using Bayesian Optimization.

A different combination of AI and consensus algorithm is proposed in Chakraborty et al. (2022). The authors propose an AI Adaptive PoW meant to protect from Distributed Denial of Service (DDoS) attacks. The protocol injects latency during communication by generating client reputation adaptive puzzles, which need to be solved by a client before the server begins processing a request. The framework adaptively tunes the difficulty of a puzzle based on a reputation score calculated by an AI model. In this way, the volume of incoming adversarial traffic is slowed down. Additionally, the framework compels the adversary to incur a cost per connection, hence making it expensive for an adversary to sustain a volumetric DDoS attack.

Authors in Reddy and Sharma (2020) focus instead on preventing double spending attacks, by proposing an unsupervised learning-based consensus protocol. They consider the ledger as a Directed Acyclic Graph (DAG) rather than a chain of blocks. Their protocol is divided into two steps. First, they apply a graph clustering algorithm based on spectral graph theory for separating the blocks created by the non-cooperating miners (attackers) in the blockchain network. Then they use an ordering algorithm based on the topological ordering of the DAG using the references included in the block header. With respect to PoW, their solution guarantees higher transaction throughput without compromising the security of the blocks from double-spending attacks.

Lastly, authors in Geng and Du (2022) combine deep reinforcement learning (DRL) and consensus algorithm to improve the efficiency of IoT-based manufacturing industry. The deep reinforcement consensus algorithm (DRCA) is trained by a DRL training set and is adapted to the intelligent manufacturing business model. Authors show how their blockchain-oriented DRCA based on node validity can effectively improve system decentralization, by saving data storage space and improving efficiency in intelligent manufacturing. As part of the testing phase, the authors make a comparison between the DRL proposed approach and classical approaches from Xiong and Li (2022), Sondhi et al. (2021). The results show that the proposed approach outmatches the classic techniques. The system response rate is higher in both the test cases designed by the authors.

5.4. Auctions and smart grids optimization

A *smart grid* is the combination of an information network and an electric distribution grid. The aim of this structure is to handle electricity distribution in a smart fashion. While in a standard electric distribution system we find a single source for the whole amount of energy, in smart grids there are also small energy producers. In particular, some consumers are converted into *prosumers* who have the capability to not only use but also generate energy to be sold. The *extra* energy needs to be somehow distributed, and this led to the creation of modern electricity markets. Such markets adopt auction-based energy trading to handle multiple transactions smoothly (Tanwar et al., 2020). In the majority of cases, these auctions are carried out by a centralized auctioneer – a centralized smart grid utility – and all the nodes depend on such an auctioneer. This of course creates a trust issue since all bidders must rely on the central utility's trustworthiness. Hence, in the last years, a lot of efforts have been put in order to decentralize the auction process. Blockchain enters the game by providing both its decentralized nature and the trust that it creates thanks to its internal mechanisms. Of course, auction mechanisms differ when applied to centralized and decentralized structures. A vast amount of research has been carried out to define blockchain-based energy auctions. All the methods can be grouped into 3 main categories (Hassan et al., 2022b):

- *First Price Auction*: it is a standard form of auction, where the higher bidder wins and pays the bidding price. Usually, all bids are hidden.
- *Double Auction*: while in First Price Auction only bidders have to compete with each other, in this case also sellers have to compete.
- *Vickrey Auctions*: in this case, bidders do not share their bids with other buyers, but instead, send them to some trusted auctioneer. This particular category of auction can be further divided into two families:
  - *Kth price auction*: the winner is the one with the highest bid, but the price is one of the kth bid, with k that is pre-decided.
  - *VCG auction*: VCG auction is a game-theoretic generalized form of Vickrey auctions in which the buyer pays for the amount of *harm* they cause to other buyers.

The main problem in the adoption of blockchain is resource-related: nodes that are part of a blockchain are computationally inefficient in carrying out complex consensus algorithms. Therefore, there is a need to develop greener and computationally lighter auction techniques to carry out decentralized energy trading.

In this sense, authors in Luong et al. (2017) proposed to use Edge computing. Resources are provided by the Edge Computing Service Provider (ECSP) and can be adopted to offload the mining process from mobile devices—miners in the blockchain. The ECSP owns edge computing resources which are distributed across the network to provide mobile users with computing resource services. Since the edge computing resource unit is only assigned to a single mobile user, they compete to buy the unit. Hence, the ECSP needs to solve the problem of auction optimality to determine the winner, while maximizing its own revenue. Such a problem is solved by the authors using a deep learning approach where two steps are executed:

1. Miners bids are transformed using a monotone application;
2. Miners calculate allocation and conditional payment rules for the miners.

The values computed by the miners in the last step are used as input to adjust the NN parameters. The objective function is the revenue for the ECSP.

The authors compared their approach with a classic one taken from Vickrey (1961). They referred to such method as *baseline*. The results obtained show that the NN model can quickly converge to a solution at which the revenue of the ECSP is significantly higher than that obtained by the baseline scheme.

Another strategy to improve the bidding strategies for smart grid users has been proposed in Ye et al. (2020). In this case, the authors applied a Recurrent Neural Network technique to solve the problem of strategic bidding for energy. The problem has been converted into a multidimensional continuous state that allows users to receive feedback regarding the impact of their biddings and eventually adapt their strategies with respect to such results. The proposed architecture seems to have a faster convergence time w.r.t. other architectures dealing with the same problem while requiring a high computational time. Authors compared their architecture also against the state-of-the-art *Mathematical programs with Equilibrium Constraints* (MPEC) approach. They studied two different scenarios in which they modified the shape of the solution space. In the first case, even if the MPEC approach obtained a higher profit, the proposed method obtained a profit that is only 0.04% lower. On the other hand, in the second scenario the RNN technique achieved a significantly higher profit with respect to MPEC.

Recurrent Neural Networks have also been used as part of the model proposed by Zhang and Yang (2020). In this work, the authors addressed the problem of energy trading in smart grids when using the double auction mechanism. In particular, they wanted to devise an optimal bidding algorithm for both sellers and buyers. The authors proposed a Deep Reinforcement Learning approach to devise the aforementioned strategies. The Neural Network architecture used in this work is composed of two levels: a Recurrent Neural Network, used to process sequences of data, followed by a Feed Forward NN, used to make the actual predictions. The evaluation technique was based on an empirical algorithm in which the buyer and the seller only care about obtaining the minimum payment and the maximum return in the current time period. What has been observed is that when the number of competitors in energy trading increases, the average cost of buyers will increase, and the average profit of sellers will decrease. The simulation results also prove that the proposed approach can effectively help buyers and sellers in energy trading to obtain lower costs and greater benefits, respectively.

Consumers becoming prosumers is not the only peculiarity of smart grids. This paradigm also integrates classic power grids with computational, controlling and monitoring capabilities. Blockchain and Machine Learning techniques can be applied together to improve these aspects.

For example, in Ferrag and Maglaras (2020), the authors tackled the problem of attacks in Smart Grids. The basic idea is to exploit Blockchain properties to store data about energy usage and trading, while Machine Learning techniques are applied to detect attacks. Such model has been called DeepCoin, and it applies a Recurrent Neural Network model on the ML side, while adopting Practical Byzantine Fault Tolerance (PBFT) consensus for the blockchain part—a consensus algorithm that allows reaching a consensus even if some amount of nodes show malicious behavior. The performances and effectiveness of the model have been tested using different datasets: CICIDS2017, a power system dataset, and a web robot (Bot)-Internet of Things (IoT) dataset. The results show an improvement with respect to the other models in the literature dealing with the same problem.

Electric Vehicles (EVs) charging stations are usually connected to a smart grid. Hence, when an EV connects to recharge, the grid needs a fast and efficient algorithm to decide from which source to take the energy to charge the vehicle. In this sense, in Ashfaq et al. (2022), the authors tackled this problem using a BC and ML approach. A k-NN algorithm is used to compute the EV to charging station distance. Nodes in the smart grid with surplus energy take care of finding the closest charging station when a vehicle asks for energy. All the communications involved are handled with Blockchain. The authors did not check the efficiency and the performance of their proposed method. On the other hand, they analyzed and showed the robustness against particular attacks.

6. Open problems and future challenges

Blockchain is a disruptive technology doomed to change not only the paradigm used for transactions but also the way data are usually stored in many applications. For example, many blockchain-based cloud storage solutions have been recently emerging: the idea is to store private files that are first encrypted and then shattered across multiple nodes. This solution drastically increases the level of security, as any information leak would only reveal a small part of a file, and it also comes with higher download speed, since when the owner requests to visualize the file each shard is recovered through a peer-to-peer system.

6.1. Blockchain open problems

At the same time, as any new technology, blockchain presents many challenging limits that need smart solutions. Most of the drawbacks usually associated with blockchain belong to one of the following areas: complexity, privacy, immutability of data, data storage, speed, transaction cost, sustainability, and politics.

Complexity
As popular as blockchain technology might be, it takes a considerable amount of time for a newbie to grasp the intrinsic mechanisms at the base of blockchain. The mathematics behind the cryptography used to sign the transactions, as well as the consensus algorithm and the whole concept of miners/validators, make the technology complex to understand and rise the possibility of misunderstandings or errors, even for expert programmers.

Privacy
Privacy concerns are another common complaint that is often raised. Even if cryptographic keys appear to offer anonymity, each and every transaction is recorded on a public ledger, so it is openly available. As you transfer a certain amount of coins to another person, you also see its related address, and in this way, you can check their other transactions. Using this and other tricks, it is often possible to de-anonymize some entities in the blockchain, invalidating one of the main pillars at the base of this technology. Another critical problem associated with signatures is the importance of private keys: if they are lost or stolen, there is no other way to demonstrate ownership and it is impossible to access or perform any operation.

Immutability of Data
Guaranteeing the immutability of data stored in the blocks is a great feature to avoid malicious entities from performing any attack to modify such data. At the same time, even if there are low probabilities, most blockchains are not free from the possibility of double spending (an example is the hard fork following the DAO attack on Ethereum). In this eventuality, denying the possibility to delete or undo any operation on data that has already been published in a block might be a considerable issue.

Data Storage
The ledger nature of blockchain requires every transaction to be stored. This applies not only to one node but to each node in the blockchain that verifies and publishes the blocks. As the storage required increases as much as roughly 50 GB every year, this leads to the impossibility of saving the whole ledger for many blocks, with all the problems connected.

Speed
Another significant limitation of this technology involves speed. As Visa and Mastercard can process thousands of requests per second, the average number of transactions per second that most public blockchains are able to handle varies from 7 to 30 (belonging to Bitcoin and Ethereum, respectively). As more and more people are getting interested in cryptocurrencies, and the number of available dapps keeps increasing, this low throughput cannot keep pace with the number of requests.

Transaction Cost
The most prominent public blockchain is certainly Ethereum, especially thanks to the features it provides for writing complex smart contracts. At the same time the transaction fees, or *gas*, required makes each interaction with the blockchain very expensive. At the same time, smart contracts are very prone to bugs or vulnerabilities, which are not usually checked before entering a block.

Sustainability
Even if Ethereum has already migrated to PoS, Bitcoin and other cryptocurrencies still heavily rely on PoW, which wastes huge amounts of electricity, making it not sustainable. The recent rise in electricity costs resulted in many blockchains having fewer miners, greatly lowering the transaction speed as well as the value of the coins.

Politics and Government
Finally, one of the problems involves politics, as many governments are contrary to cryptocurrencies. The obvious reasons concern their inability to control such a large flow of money, as well as not being able to apply any taxes on such currency and the possibility of transactions being used for money laundering and terrorism purposes.

Even if most of these problems can be greatly mitigated in private blockchains, they are still very challenging issues that highly limit public ones.

6.2. Limitations of artificial intelligence for blockchain

Other than the possible computational overhead, the limitations related to artificial intelligence and machine learning are also present when these algorithms are combined with blockchain technology. They can be mainly defined as:

- **Data-related problems**
- **Scalability**
- **Replicability**

Public blockchains, especially prominent cryptocurrencies, accumulate vast terabytes of stored data. However, the effectiveness of machine learning models is contingent upon both data volume and quality. Many AI-driven solutions addressing blockchain issues contend with limited or unreliable datasets. A noticeable absence of benchmark datasets devoid of mislabeling and showcasing robust diversity is evident. A classic case of this issue surfaces in smart contract vulnerability detection. Despite millions of accessible contracts, such as in Ethereum's blockchain, numerous contracts are essentially replicas of the same code. This challenge becomes even more pronounced in addressing specific vulnerabilities due to the inadequacy of available contracts to comprehensively tackle the issue. This problem is even more pronounced in private blockchains, where available data is considerably scarcer.

Even when sufficient data is assured, the performance of neural networks can rapidly deteriorate if the input's nature changes or novel detection challenges emerge. In this case, training a new model from scratch to include such variations (e.g., an update in the programming language used or a new possible attack or vulnerability) is usually a long process, and since at first there are not many observations the model can learn from, it can perform poorly or need multiple re-trainings. To give an example, after the latest update of Solidity (version 0.8.0) the compiler automatically checks for integer overflows in smart contracts (Anon, 2023e), making the available deep learning models trained for vulnerability detection partially deprecated or redundant.

In particular, while most machine learning techniques proposed for vulnerability detection are highly accurate and faster than other detection techniques, such as static analyzers, they often do not scale well when a new vulnerability emerges or the software version is updated. Another issue that emerged is the lack of a common dataset or benchmark, as the datasets used in different papers greatly vary from the acquisition process to the number of smart contracts considered. Different machine learning models are trained on different types and number of vulnerabilities, since some works only focus on detecting the most troublesome ones (such as reentrancy), making it difficult to compare the results. Even if AI models can detect vulnerabilities with fast accuracy and low latency, they are not able to guarantee that all the available security vulnerabilities have been identified.

Finally, replicability in machine learning refers to the challenge of reproducing and confirming research outcomes across various contexts, impacting the credibility of results. In the context of blockchain, this issue gains significance as machine learning techniques are integrated to enhance blockchain technology. Ensuring consistent and replicable outcomes is crucial for building reliable AI-enhanced blockchain systems. The scarcity of standardized benchmark datasets, the evolving nature of both AI and blockchain, and the intricate interactions between algorithms and blockchain structures contribute to this challenge. Replicability issues can impede the widespread adoption of AI-driven solutions in blockchain, as inconsistent results may hinder the development of reliable and secure applications. Therefore, addressing replicability concerns is vital to establish a robust foundation for the integration of AI and blockchain technologies.

6.3. Analysis of AI contributions to blockchain

As emerged from this survey, machine learning most relevant contributions in mitigating such problems can be divided into two categories: either they aim to *improve the overall security*, or they contribute in *optimizing decision processes* related to the blockchain protocol or applications using it (see Fig. 5). While these solutions represent important improvements and provide significant help to blockchain-based applications in exhibiting the best possible behavior, they barely tackle most of the above-mentioned limitations belonging to this technology. In particular, even if many AI-based alternative consensus protocols have been proposed, these can rarely be applied to many applications, or they also come with multiple problems (such as the need of a task supplier). Although deep learning solutions can help improving overall security in multiple ways, the same techniques can be used instead to perform various attacks, for example by using adversarial generative networks.

During our research, we uncovered that the security aspect of blockchain splinters into a thousand different sub-problems, each requiring its own *ad hoc* solution. Among these problems, a substantial number are linked to long-standing issues typical of distributed systems, networks, and data sharing. In contrast, other challenges are distinct to the blockchain protocol, making them comparatively more recent. These issues predominantly pertain to the incentive, consensus, and contract layers.

We noted that while considerable attention is directed towards issues linked to the financial aspects of the protocol (for understandable reasons), the focus and dedication given to smart contracts and the consensus algorithm do not align at the same level. Specifically, within the context of smart contracts, the application of intelligent methods exhibits certain limitations, particularly in their ability to effectively identify a wide array of vulnerabilities. Often, these methods rely on static analysis techniques, which may not always be fully comprehensive or consistently effective.

Furthermore, AI-driven consensus algorithms emerge as compelling alternatives to Proof of Work (PoW). However, despite their potential, their implementation often introduces time delays and computational requirements that render them less desirable compared to other well-established consensus protocols.

Examining the possible time delay in AI-enhanced blockchains compared to their original counterparts is a pertinent subject. Interestingly, this aspect often remains overlooked both in broader surveys and individual articles. This omission may stem from the prevalent perception that while training machine learning models demands time, such concerns are less salient during the inference phase. For instance, even a slight delay of a few seconds is usually manageable in real-time scenarios. Notably, these scenarios could involve security-sensitive applications like identifying vulnerabilities in smart contracts or detecting anomalies in cybercrime. Given the absence of built-in mechanisms for these purposes in current blockchain protocols, introducing a minor delay could be a reasonable trade-off to significantly heighten security levels.

6.4. Future directions

While artificial intelligence algorithms and models have been extensively integrated into a wide array of tasks, significant gaps persist in our exploration of their potential integration into various facets of blockchain technology. In this study, we have presented a substantial body of work showcasing how AI can elevate both the security and optimization of blockchain-based applications. However, AI's potential extends beyond these realms, encompassing aspects that have yet to be fully explored within this context.

More specifically, machine learning algorithms have already demonstrated successful implementation in diverse areas. These include the design of more efficient hardware architectures (Mirhoseini et al., 2021), assessing the probability of a node in a distributed environment fulfilling a task within a specified time frame, enhancing cloud performance and security (Grzonka et al., 2018), and even contributing to the creation of improved hash functions (Singh and Gupta, 2022).

The primary gap that surfaced from our analysis revolves around the machine learning methods currently employed for vulnerability detection in smart contracts. A significant portion of the existing methods is applicable solely to the Ethereum blockchain, concentrating on a limited set of vulnerabilities and lacking a foundation in a comprehensive benchmark dataset. There remains substantial room for advancement in this arena.

Both blockchain and AI are pervasive technologies. While AI has already been integrated into many daily-use devices, enhancing not only quality of life but also optimizing processes and experiences, blockchain emerged slightly later. However, its adoption is rapidly expanding across domains due to the reliability and security it offers within distributed environments.

Likewise, other technologies have been recently explored, particularly in conjunction with blockchain and AI. Notably, blockchain and AI harmonize effectively with concepts such as federated learning, particularly within the realm of the Internet of Things (IoT). Industrial IoT (IIoT), Internet of Vehicles (IoV), healthcare, and similar applications collectively represent distinct facets of IoT, closely interlinked with the challenges of optimizing and securing applications in a distributed system. Furthermore, optimization stands as a central objective in domains like digital twins and edge computing, where artificial intelligence emerges as the tool of choice. Presently, machine learning techniques are extensively employed to enhance the performance of numerous systems, including blockchain-based applications.

Several promising areas for the synergistic application of AI and blockchain require further investigation. These include the development of more efficient methods to enhance scalability within blockchain networks, fostering interoperability between diverse blockchains facilitated by AI-driven communication protocols. Additionally, exploring the implementation of AI in creating digital assets (tokens) representing tangible items and delving deeper into ethical compliance through AI-driven verification mechanisms within blockchain systems remain critical areas for advancement.

However, what lies ahead is a frontier unexplored. The convergence of AI and blockchain with emerging paradigms like federated learning, the Internet of Things (IoT), 6G telecommunications, quantum computing, and the metaverse introduces a realm brimming with potential.

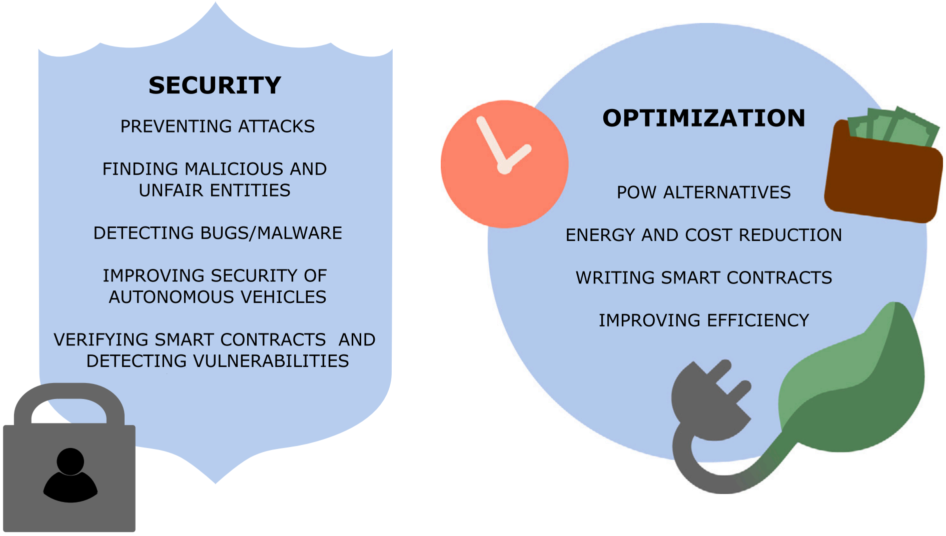

SECURITY
PREVENTING ATTACKS
FINDING MALICIOUS AND UNFAIR ENTITIES
DETECTING BUGS/MALWARE
IMPROVING SECURITY OF AUTONOMOUS VEHICLES
VERIFYING SMART CONTRACTS AND DETECTING VULNERABILITIES
OPTIMIZATION
POW ALTERNATIVES
ENERGY AND COST REDUCTION
WRITING SMART CONTRACTS
IMPROVING EFFICIENCY

Fig. 5. Most significant AI contributions in improving blockchain technology.

Nevertheless, it is crucial to acknowledge that these promises demand more than theoretical speculation; they require substantial realizations, underpinned by concrete implementations, validated through real-world case studies, and supported by robust frameworks.

7. Conclusion

This review has examined the potential benefits of using artificial intelligence in blockchain-based applications. Unlike other studies, we have focused on solutions that use intelligent algorithms to modify the behavior of blockchain protocols or workflows. Our analysis has identified two main categories of AI solutions for blockchain: those that increase security and those that optimize efficiency. We have also highlighted the application areas that can benefit the most from the integration of AI and blockchain, with numerous examples from both academia and industry. Finally, we have discussed the key limitations of both technologies and provided insights on further research directions. Our findings suggest that the combination of AI and blockchain holds great promise for creating more secure, efficient, and transparent systems, but further work is needed to address challenges around data privacy, scalability, and interoperability.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Dalila Ressi, Carla Piazza and Sabina Rossi reports financial support was provided by Government of Italy Ministry of Education University and Research.

Data availability

No data was used for the research described in the article.

Acknowledgments

This research was partially supported by the PRIN project NiRvAna – Noninterference and Reversibility Analysis in Private Blockchains, and by the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

Aich, S., Sinai, N.K., Kumar, S., Ali, M., Choi, Y.R., Joo, M.-I., Kim, H.-C., 2021. Protecting personal healthcare record using blockchain & federated learning technologies. In: 2021 23rd International Conference on Advanced Communication Technology. ICACT, pp. 109–112. http://dx.doi.org/10.23919/ICACT51234.2021.9370566.

Alabdulatif, A., Khalil, I., Saidur Rahman, M., 2022. Security of blockchain and AI-empowered smart healthcare: Application-based analysis. Appl. Sci. 12 (21), 11039.

Alaeddini, M., Hajizadeh, M., Reaidy, P., 2023. A bibliometric analysis of research on the convergence of artificial intelligence and blockchain in smart cities. Smart Cities 6 (2), 764–795.

Alarab, I., Prakoonwit, S., Nacer, M.I., 2020. Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In: Proceedings of the 2020 5th International Conference on Machine Learning Technologies. pp. 11–17.

Alqaralleh, B.A., Vaiyapuri, T., Parvathy, V.S., Gupta, D., Khanna, A., Shankar, K., 2021. Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment. Pers. Ubiquitous Comput. 1–11.

Andrew, J., Deva Priya, I., K. Martin, S., Bharat, S., Jennifer, E., 2023. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. J. Netw. Comput. Appl. 215, 103633.

Andriyanov, N., Andriyanov, D., 2020. The using of data augmentation in machine learning in image processing tasks in the face of data scarcity. In: Journal of Physics: Conference Series, vol. 1661, no. 1, IOP Publishing, 012018.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference. pp. 1–15.

Anon, 2019. Mythril project. [Online]. https://github.com/ConsenSys/mythril.

Anon, 2023a. AnChain.AI official website. Online. https://www.anchain.ai. (Accessed March 2023).

Anon, 2023b. DeepDAO official website. Online. https://deepdao.io/organizations. (Accessed March 2023).

Anon, 2023c. SinglarityNET white paper. Online. https://public.singularitynet.io/whitepaper.pdf. (Accessed March 2023).

Anon, 2023d. Smart contract weakness classification registry. Online. https://swcregistry.io. (Accessed 2023).

Anon, 2023e. Solidity documentation, visited in January 2023. https://docs.soliditylang.org/en/v0.8.17/080-breaking-changes.html.

Arooj, A., Farooq, M.S., Umer, T., 2022. Unfolding the blockchain era: Timeline, evolution, types and real-world applications. J. Netw. Comput. Appl. 103511.

Arroyo, J., Davó, D., Martínez-Vicente, E., Faqir-Rhazoui, Y., Hassan, S., 2022. DAO-analyzer: Exploring activity and participation in blockchain organizations. In: Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing. pp. 193–196.

Ashfaq, T., Khalid, M.I., Ali, G., Affendi, M.E., Iqbal, J., Hussain, S., Ullah, S.S., Yahaya, A.S., Khalid, R., Mateen, A., 2022. An efficient and secure energy trading approach with machine learning technique and consortium blockchain. Sensors 22 (19), http://dx.doi.org/10.3390/s22197263, URL https://www.mdpi.com/1424-8220/22/19/7263.

Atlam, H.F., Azad, M.A., Alzahrani, A.G., Wills, G., 2020. A review of blockchain in Internet of Things and AI. Big Data Cogn. Comput. 4 (4), 28.

Awan, M.K., Cortesi, A., 2017. Blockchain transaction analysis using dominant sets. In: IFIP International Conference on Computer Information Systems and Industrial Management. Springer, pp. 229–239.

Aziz, R.M., Baluch, M.F., Patel, S., Ganie, A.H., 2022. LGBM: a machine learning approach for ethereum fraud detection. Int. J. Inf. Technol. 1–11.

Bach, S., Binder, A., Montavon, G., Klauschen, F., Müller, K.-R., Samek, W., 2015. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. PLoS One 10 (7), e0130140.

Backstrom, L., Dwork, C., Kleinberg, J., 2007. Wherefore art thou R3579x? Anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of the 16th International Conference on World Wide Web. pp. 181–190.

Badidi, E., 2022. Edge AI and blockchain for smart sustainable cities: promise and potential. Sustainability 14 (13), 7609.

Baek, H., Oh, J., Kim, C.Y., Lee, K., 2019. A model for detecting cryptocurrency transactions with discernible purpose. In: 2019 Eleventh International Conference on Ubiquitous and Future Networks. ICUFN, IEEE, pp. 713–717.

Bajpai, J.N., 2016. Emerging vehicle technologies & the search for urban mobility solutions. Urban Plan. Transp. Res. 4 (1), 83–100.

Balemans, D., Casteels, W., Vanneste, S., de Hoog, J., Mercelis, S., Hellinckx, P., 2020. Resource efficient sensor fusion by knowledge-based network pruning. Internet Things 11, 100231.

Ball, M., Rosen, A., Sabin, M., Vasudevan, P.N., 2017. Proofs of useful work. Cryptology ePrint Archive, Paper 2017/203. URL https://eprint.iacr.org/2017/203.

Baniata, H., Prodan, R., Kertesz, A., 2022. Machine learning for alternative mining in pow-based blockchains: Theory, implications and applications. TechRxiv.

Belotti, M., Božić, N., Pujolle, G., Secci, S., 2019. A vademecum on blockchain technologies: When, which, and how. IEEE Commun. Surv. Tutor. 21 (4), 3796–3838.

Bernardi, G., Bugliesi, M., Macedonio, D., Rossi, S., 2008. A theory of adaptable contract-based service composition. In: SYNASC 2008, 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. IEEE Computer Society, pp. 327–334. http://dx.doi.org/10.1109/SYNASC.2008.38.

Besarabov, Z., Kolev, T., 2018. Predicting digital asset market based on blockchain activity data. http://dx.doi.org/10.48550/ARXIV.1810.06696, URL https://arxiv.org/abs/1810.06696.

Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., Kumar, N., 2021. BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Trans. Netw. Sci. Eng. 8 (2), 1242–1255. http://dx.doi.org/10.1109/TNSE.2019.2961932.

Birjali, M., Kasri, M., Beni-Hssane, A., 2021. A comprehensive survey on sentiment analysis: Approaches, challenges and trends. Knowl.-Based Syst. 226, 107134.

Bossi, A., Focardi, R., Macedonio, D., Piazza, C., Rossi, S., 2003. Unwinding in information flow security. In: Electronic Notes in Theoretical Computer Science, vol. 99, Elsevier, pp. 127–154. http://dx.doi.org/10.1016/J.ENTCS.2004.02.006.

Bouraga, S., 2021. A taxonomy of blockchain consensus protocols: A survey and classification framework. Expert Syst. Appl. 168, 114384.

Bravo-Marquez, F., Reeves, S., Ugarte, M., 2019. Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions. In: 2019 IEEE International Conference on Decentralized Applications and Infrastructures. DAPPCON, IEEE, pp. 119–124.

Bugliesi, M., Gallina, L., Marin, A., Rossi, S., Hamadou, S., 2012. Interference-sensitive preorders for MANETs. In: Ninth International Conference on Quantitative Evaluation of Systems. QEST 2012, IEEE Computer Society, pp. 189–198. http://dx.doi.org/10.1109/QEST.2012.15.

Buhrmester, V., Münch, D., Arens, M., 2021. Analysis of explainers of black box deep neural networks for computer vision: A survey. Mach. Learn. Knowl. Extr. 3 (4), 966–989.

Buterin, V., et al., 2014. A next-generation smart contract and decentralized application platform. White Pap. 3 (37), 1–36.

Cai, J., Li, B., Zhang, J., Sun, X., Chen, B., 2023. Combine sliced joint graph with graph neural networks for smart contract vulnerability detection. J. Syst. Softw. 195, 111550.

Caldarelli, G., Ellul, J., 2021. The blockchain oracle problem in decentralized finance—a multivocal approach. Appl. Sci. 11 (16), 7572.

Castellano, G., Fanelli, A., Pelillo, M., 1997. An iterative pruning algorithm for feedforward neural networks. IEEE Trans. Neural Netw./ Publ. IEEE Neural Netw. Counc. 8, 519–531. http://dx.doi.org/10.1109/72.572092.

Chakraborty, T., Mitra, S., Mittal, S., Young, M., 2022. AI_Adaptive_POW: An AI assisted Proof Of Work (POW) framework for DDoS defense. Softw. Impacts 13, 100335.

Chen, X., 2022. Machine learning approach for a circular economy with waste recycling in smart cities. Energy Rep. 8, 3127–3140.

Chen, Y., Bellavitis, C., 2020. Blockchain disruption and decentralized finance: The rise of decentralized business models. J. Bus. Ventur. Insights 13, e00151.

Chen, F., Wan, H., Cai, H., Cheng, G., 2021. Machine learning in/for blockchain: Future and challenges. Canad. J. Statist. 49 (4), 1364–1382.

Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J., Yu, S., 2020. Blockchain for internet of things applications: A review and open issues. J. Netw. Comput. Appl. 172, 102839.

Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., Zhou, Y., 2018. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In: Proceedings of the 2018 World Wide Web Conference. WWW '18, International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, pp. 1409–1418. http://dx.doi.org/10.1145/3178876.3186046.

Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., Bharath, A.A., 2018. Generative adversarial networks: An overview. IEEE Signal Process. Mag. 35 (1), 53–65.

Dabre, R., Chu, C., Kunchukuttan, A., 2020. A survey of multilingual neural machine translation. ACM Comput. Surv. 53 (5), 1–38.

Davis, E., Marcus, G., 2016. The scope and limits of simulation in automated reasoning. Artificial Intelligence 233, 60–72.

Deebak, B.D., Fadi, A.-T., 2021. Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. J. Inf. Secur. Appl. 58, 102749.

Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., Hierons, R., 2018. Smart contracts vulnerabilities: a call for blockchain software engineering? In: 2018 International Workshop on Blockchain Oriented Software Engineering. IWBOSE, IEEE, pp. 19–25.

Dibaei, M., Zheng, X., Xia, Y., Xu, X., Jolfaei, A., Bashir, A.K., Tariq, U., Yu, D., Vasilakos, A.V., 2021. Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. IEEE Trans. Intell. Transp. Syst. 23 (2), 683–700.

Dinh, T.N., Thai, M.T., 2018. AI and blockchain: A disruptive integration. Computer 51 (9), 48–53.

Dixon, M.F., Akcora, C.G., Gel, Y.R., Kantarcioglu, M., 2019. Blockchain analytics for intraday financial risk modeling. IO: Productivity.

Ekramifard, A., Amintoosi, H., Seno, A.H., Dehghantanha, A., Parizi, R.M., 2020. A systematic literature review of integration of blockchain and artificial intelligence. Blockchain Cybersecur. Trust Priv. 147–160.

Elliott, D., Keen, W., Miao, L., 2019. Recent advances in connected and automated vehicles. J. Traffic Transp. Eng. (Engl. Ed.) 6 (2), 109–131.

Faqir-Rhazoui, Y., Arroyo, J., Hassan, S., 2021. A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. J. Internet Serv. Appl. 12 (1), 1–20.

Feist, J., Grieco, G., Groce, A., 2019. Slither: a static analysis framework for smart contracts. In: 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain. WETSEB, IEEE, pp. 8–15.

Ferrag, M.A., Maglaras, L., 2020. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Trans. Eng. Manage. 67 (4), 1285–1297. http://dx.doi.org/10.1109/TEM.2019.2922936.

Gasparetto, A., Ressi, D., Bergamasco, F., Pistellato, M., Cosmo, L., Boschetti, M., Ursella, E., Albarelli, A., 2018. Cross-dataset data augmentation for convolutional neural networks training. In: 2018 24th International Conference on Pattern Recognition. ICPR, IEEE, pp. 910–915.

Geng, T., Du, Y., 2022. Applying the blockchain-based deep reinforcement consensus algorithm to the intelligent manufacturing model under internet of things. J. Supercomput. 78 (14), 15882–15904.

Ghosh, A., Gupta, S., Dua, A., Kumar, N., 2020. Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects. J. Netw. Comput. Appl. 163, 102635.

Grover, J., 2022. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Veh. Commun. 100458.

Grzonka, D., Jakóbik, A., Kołodziej, J., Pllana, S., 2018. Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security. Future Gener. Comput. Syst. 86, 1106–1117.

Hamilton, P.S., Tompkins, W.J., 1986. Quantitative investigation of QRS detection rules using the MIT/BIH arrhythmia database. IEEE Trans. Biomed. Eng. BME-33 (12), 1157–1165. http://dx.doi.org/10.1109/TBME.1986.325695.

Handaya, W., Yusoff, M., Jantan, A., 2020. Machine learning approach for detection of fileless cryptocurrency mining malware. In: Journal of Physics: Conference Series, vol. 1450, no. 1, IOP Publishing, 012075.

Harlev, M.A., Yin, H.S., Langenheldt, K.C., Mukkamala, R.R., Vatrapu, R., 2018. Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning. In: Hawaii International Conference on System Sciences.

Hassan, M.U., Rehmani, M.H., Chen, J., 2022a. Anomaly detection in blockchain networks: A comprehensive survey. IEEE Commun. Surv. Tutor..

Hassan, M.U., Rehmani, M.H., Chen, J., 2022b. Optimizing blockchain based smart grid auctions: A green revolution. IEEE Trans. Green Commun. Netw. 6 (1), 462–471. http://dx.doi.org/10.1109/TGCN.2021.3095424.

Hewa, T., Ylianttila, M., Liyanage, M., 2021. Survey on blockchain based smart contracts: Applications, opportunities and challenges. J. Netw. Comput. Appl. 177, 102857.

Hillston, J., Marin, A., Piazza, C., Rossi, S., 2021. Persistent stochastic non-interference. Fund. Inform. 181 (1), 1–35.

Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., Szalachowski, P., 2020. The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. IEEE Commun. Surv. Tutor. 23 (1), 341–390.

Hou, D., Zhang, J., Man, K.L., Ma, J., Peng, Z., 2021. A systematic literature review of blockchain-based federated learning: Architectures, applications and issues. In: 2021 2nd Information Communication Technologies Conference. ICTC, IEEE, pp. 302–307.

Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R., Lin, X., 2021. A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems. Patterns 2 (2), 100179.

Hua, W., Chen, Y., Qadrdan, M., Jiang, J., Sun, H., Wu, J., 2022. Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review. Renew. Sustain. Energy Rev. 161, 112308.

Huang, T.H.-D., 2018. Hunting the ethereum smart contract: Color-inspired inspection of potential attacks. arXiv preprint arXiv:1807.01868.

Hussain, A.A., Al-Turjman, F., 2021. Artificial intelligence and blockchain: A review. Trans. Emerg. Telecommun. Technol. 32 (9), e4268.

Hwang, S.-J., Choi, S.-H., Shin, J., Choi, Y.-H., 2022. CodeNet: Code-targeted convolutional neural network architecture for smart contract vulnerability detection. IEEE Access 10, 32595–32607.

Iyer, S., Thakur, S., Dixit, M., Katkam, R., Agrawal, A., Kazi, F., 2019. Blockchain and anomaly detection based monitoring system for enforcing wastewater reuse. In: 2019 10th International Conference on Computing, Communication and Networking Technologies. ICCCNT, IEEE, pp. 1–7.

Jay, P., Kalariya, V., Parmar, P., Tanwar, S., Kumar, N., Alazab, M., 2020. Stochastic neural networks for cryptocurrency price prediction. IEEE Access 8, 82804–82818.

Jia, H., Yaghini, M., Choquette-Choo, C.A., Dullerud, N., Thudi, A., Chandrasekaran, V., Papernot, N., 2021. Proof-of-learning: Definitions and practice. In: 2021 IEEE Symposium on Security and Privacy. SP, IEEE, pp. 1039–1056.

Kanare, H.M., 1985. Writing the Laboratory Notebook. ERIC.

Karamitsos, I., Papadaki, M., Al Barghuthi, N.B., et al., 2018. Design of the blockchain smart contract: A use case for real estate. J. Inf. Secur. 9 (03), 177.

Kashani, M.H., Madanipour, M., Nikravan, M., Asghari, P., Mahdipour, E., 2021. A systematic review of IoT in healthcare: Applications, techniques, and trends. J. Netw. Comput. Appl. 192, 103164.

Kassen, M., 2022. Blockchain and e-government innovation: Automation of public information processes. Inf. Syst. 103, 101862.

Kazeminia, S., Baur, C., Kuijper, A., van Ginneken, B., Navab, N., Albarqouni, S., Mukhopadhyay, A., 2020. GANs for medical image analysis. Artif. Intell. Med. 109, 101938.

Khedr, A.M., Arif, I., El-Bannany, M., Alhashmi, S.M., Sreedharan, M., 2021. Cryptocurrency price prediction using traditional statistical and machine-learning techniques: A survey. Intell. Syst. Account. Finance Manag. 28 (1), 3–34.

Kim, H.-M., Bock, G.-W., Lee, G., 2021. Predicting Ethereum prices with machine learning based on Blockchain information. Expert Syst. Appl. 184, 115480.

Kim, J., Nakashima, M., Fan, W., Wuthier, S., Zhou, X., Kim, I., Chang, S.-Y., 2022. A machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking. IEEE Trans. Netw. Serv. Manag. 19 (3), 3619–3632.

Kim, H., Park, J., Bennis, M., Kim, S.-L., 2019. Blockchained on-device federated learning. IEEE Commun. Lett. 24 (6), 1279–1283.

Kiong, L.V., 2021. DeFi, NFT and GameFi Made Easy: A Beginner's Guide to Understanding and Investing in DeFi, NFT and GameFi Projects. Liew Voon Kiong.

Kolonin, A., 2023. Reputation system design for SingluarityNET. Online. https://blog.singularitynet.io/reputation-system-design-for-singularitynet-8b5b61e8ed0e. (Accessed March 2023).

Krizhevsky, A., Sutskever, I., Hinton, G.E., 2012. Imagenet classification with deep convolutional neural networks. Adv. Neural Inf. Process. Syst. 25.

Ktari, J., Frikha, T., Hamdi, M., Elmannai, H., Hmam, H., 2022. Lightweight AI framework for industry 4.0 case study: water meter recognition. Big Data Cogn. Comput. 6 (3), 72.

Kumar, P., Gupta, G.P., Tripathi, R., 2021. TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning. J. Syst. Archit. 115, 101954.

Kumar, N., Singh, A., Handa, A., Shukla, S.K., 2020. Detecting malicious accounts on the ethereum blockchain with supervised learning. In: International Symposium on Cyber Security Cryptography and Machine Learning. Springer, pp. 94–109.

Lai, R., Chuen, D.L.K., 2018. Blockchain–from public to private. In: Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2. Elsevier, pp. 145–177.

Lamport, L., Shostak, R., Pease, M., 2019. The Byzantine generals problem. In: Concurrency: The Works of Leslie Lamport. pp. 203–226.

Li, J., Herdem, M.S., Nathwani, J., Wen, J.Z., 2022. Methods and applications for artificial intelligence, big data, Internet-of-Things, and blockchain in smart energy management. Energy AI 100208.

Li, J., Izakian, H., Pedrycz, W., Jamal, I., 2021. Clustering-based anomaly detection in multivariate time series data. Appl. Soft Comput. 100, 106919.

Li, P., Ou, W., Liang, H., Han, W., Zhang, Q., Zeng, G., 2023. A zero trust and blockchain-based defense model for smart electric vehicle chargers. J. Netw. Comput. Appl. 213, 103599.

Li, X., Xu, G., Zheng, X., Liang, K., Panaousis, E., Li, T., Wang, W., Shen, C., 2019. Using sparse representation to detect anomalies in complex WSNs. ACM Trans. Intell. Syst. Technol. 10 (6), 1–18.

Lihu, A., Du, J., Barjaktarevic, I., Gerzanics, P., Harvilla, M., 2020. A proof of useful work for artificial intelligence on the blockchain. arXiv preprint arXiv:2001.09244.

Lin, S.-Y., Zhang, L., Li, J., Ji, L.-l., Sun, Y., 2022. A survey of application research based on blockchain smart contract. Wirel. Netw. 28 (2), 635–690.

Liu, C.H., Lin, Q., Wen, S., 2019. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. IEEE Trans. Ind. Inform. 15 (6), 3516–3526. http://dx.doi.org/10.1109/TII.2018.2890203.

Liu, Z., Qian, P., Wang, X., Zhuang, Y., Qiu, L., Wang, X., 2021a. Combining graph neural networks with expert knowledge for smart contract vulnerability detection. IEEE Trans. Knowl. Data Eng..

Liu, B., Szalachowski, P., Zhou, J., 2021b. A first look into defi oracles. In: 2021 IEEE International Conference on Decentralized Applications and Infrastructures. DAPPS, IEEE, pp. 39–48.

Loe, A.F., Quaglia, E.A., 2018. Conquering generals: an np-hard proof of useful work. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems. pp. 54–59.

Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y., 2019. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans. Ind. Inform. 16 (6), 4177–4186.

Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y., 2020. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans. Ind. Inform. 16 (6), 4177–4186. http://dx.doi.org/10.1109/TII.2019.2942190.

Luong, N.C., Xiong, Z., Wang, P., Niyato, D., 2017. Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach, CoRR abs/1711.02844. arXiv:1711.02844.

Lutz, O., Chen, H., Fereidooni, H., Sendner, C., Dmitrienko, A., Sadeghi, A.R., Koushanfar, F., 2021. ESCORT: ethereum smart contracts vulnerability detection using deep neural network and transfer learning. arXiv preprint arXiv:2103.12607.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., Hobor, A., 2016. Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 254–269.

Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.A., Salah, K., Hong, C.S., 2021. Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges. J. Netw. Comput. Appl. 181, 103007.

Malakhov, I., Marin, A., Rossi, S., Smuseva, D., 2022. On the use of proof-of-work in permissioned blockchains: Security and fairness. IEEE Access 10, 1305–1316. http://dx.doi.org/10.1109/ACCESS.2021.3138528.

Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., et al., 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 9 (5), 5665.

Marella, V., Upreti, B., Merikivi, J., Tuunainen, V.K., 2020. Understanding the creation of trust in cryptocurrencies: the case of bitcoin. Electron. Mark. 30 (2), 259–271.

Merkle, R.C., 1979. Secrecy, Authentication, and Public Key Systems. Stanford university.

Merlina, A., 2019. Blockml: a useful proof of work system based on machine learning tasks. In: Proceedings of the 20th International Middleware Conference Doctoral Symposium. pp. 6–8.

Mhlanga, D., 2021. Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. Int. J. Financ. Stud. 9 (3), 39.

Michalski, R., Dziubałtowska, D., Macek, P., 2020. Revealing the character of nodes in a blockchain with supervised learning. IEEE Access 8, 109639–109647.

Mirhoseini, A., Goldie, A., Yazgan, M., Jiang, J.W., Songhori, E., Wang, S., Lee, Y.-J., Johnson, E., Pathak, O., Nazi, A., et al., 2021. A graph placement methodology for fast chip design. Nature 594 (7862), 207–212.

Mittal, A., Aggarwal, S., 2020. Hyperparameter optimization using sustainable proof of work in blockchain. Front. Blockchain 3, 23.

Mittal, K., Jain, A., Vaisla, K.S., Castillo, O., Kacprzyk, J., 2020. A comprehensive review on type 2 fuzzy logic applications: Past, present and future. Eng. Appl. Artif. Intell. 95, 103916.

Mohanta, B.K., Jena, D., Satapathy, U., Patnaik, S., 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things 11, 100227.

Momeni, P., Wang, Y., Samavi, R., 2019. Machine learning model for smart contracts security analysis. In: 2019 17th International Conference on Privacy, Security and Trust. PST, IEEE, pp. 1–6.

Monamo, P., Marivate, V., Twala, B., 2016. Unsupervised learning for robust bitcoin fraud detection. In: 2016 Information Security for South Africa. ISSA, IEEE, pp. 129–134.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus. Rev. 21260.

Neill, J.O., 2020. An overview of neural network compression. arXiv preprint arXiv:2006.03669.

Nerurkar, P., Bhirud, S., Patel, D., Ludinard, R., Busnel, Y., Kumari, S., 2021. Supervised learning model for identifying illegal activities in bitcoin. Appl. Intell. 51 (6), 3824–3843.

Nguyen, D.C., Ding, M., Pham, Q.-V., Pathirana, P.N., Le, L.B., Seneviratne, A., Li, J., Niyato, D., Poor, H.V., 2021. Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet Things J. 8 (16), 12806–12825.

Nicholls, J., Kuppa, A., Le-Khac, N.-A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. IEEE Access.

Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., Hobor, A., 2018. Finding the greedy, prodigal, and suicidal contracts at scale. In: Proceedings of the 34th Annual Computer Security Applications Conference. pp. 653–663.

Ogawa, T., Kima, H., Miyaho, N., 2018. Proposal of proof-of-lucky-id (PoL) to solve the problems of PoW and PoS. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 1212–1218.

Ostapowicz, M., Żbikowski, K., 2020. Detecting fraudulent accounts on blockchain: a supervised approach. In: International Conference on Web Information Systems Engineering. Springer, pp. 18–31.

Otter, D.W., Medina, J.R., Kalita, J.K., 2020. A survey of the usages of deep learning for natural language processing. IEEE Trans. Neural Netw. Learn. Syst. 32 (2), 604–624.

Outchakoucht, A., Hamza, E.-S., Leroy, J.P., 2017. Dynamic access control policy based on blockchain and machine learning for the Internet of Things. Int. J. Adv. Comput. Sci. Appl. 8 (7).

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

Pang, G., van den Hengel, A., Shen, C., Cao, L., 2021. Toward deep supervised anomaly detection: Reinforcement learning from partially labeled anomaly data. In: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. pp. 1298–1308.

Pang, G., Shen, C., van den Hengel, A., 2019. Deep anomaly detection with deviation networks. arXiv:1911.08623.

Patel, M.M., Tanwar, S., Gupta, R., Kumar, N., 2020. A deep learning-based cryptocurrency price prediction scheme for financial institutions. J. Inf. Secur. Appl. 55, 102583.

Pintelas, E., Livieris, I.E., Stavroyiannis, S., Kotsilieris, T., Pintelas, P., 2020. Investigating the problem of cryptocurrency price prediction: a deep learning approach. In: IFIP International Conference on Artificial Intelligence Applications and Innovations. Springer, pp. 99–110.

Politis, A., Doka, K., Koziris, N., 2021. Ether price prediction using advanced deep learning models. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency. ICBC, IEEE, pp. 1–3.

Poongodi, M., Sharma, A., Vijayakumar, V., Bhardwaj, V., Sharma, A.P., Iqbal, R., Kumar, R., 2020. Prediction of the price of Ethereum blockchain cryptocurrency in an industrial finance system. Comput. Electr. Eng. 81, 106527.

Proelss, J., Sevigny, S., Schweizer, D., 2023. GameFi-the perfect symbiosis of blockchain, tokens, DeFi, and NFTs? Tokens, DeFi, and NFTs.

Qu, Y., Gao, L., Xiang, Y., Shen, S., Yu, S., 2022a. Fedtwin: Blockchain-enabled adaptive asynchronous federated learning for digital twin networks. IEEE Netw. 36 (6), 183–190.

Qu, Y., Uddin, M.P., Gan, C., Xiang, Y., Gao, L., Yearwood, J., 2022b. Blockchain-enabled federated learning: A survey. ACM Comput. Surv. 55 (4), 1–35.

Rabah, K., 2018. Convergence of AI, IoT, big data and blockchain: a review. Lake Inst. J. 1 (1), 1–18.

Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F., Guizani, M., 2019. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. IEEE Access 7, 18611–18621.

Rajawat, A.S., Bedi, P., Goyal, S., Shaw, R.N., Ghosh, A., Aggarwal, S., 2022. Ai and blockchain for healthcare data security in smart cities. AI IoT Smart City Appl. 185–198.

Rathore, S., Kwon, B.W., Park, J.H., 2019a. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. J. Netw. Comput. Appl. 143, 167–177.

Rathore, S., Pan, Y., Park, J.H., 2019b. BlockDeepNet: A blockchain-based secure deep learning for IoT network. Sustainability 11 (14), http://dx.doi.org/10.3390/su11143974.

Rawat, B., Bist, A.S., Apriani, D., Permadi, N.I., Nabila, E.A., 2023. AI based drones for security concerns in smart cities. APTISI Trans. Manag. (ATM) 7 (2), 125–130.

Reddy, S., Sharma, G., 2020. Ul-blockdag: Unsupervised learning based consensus protocol for blockchain. In: 2020 IEEE 40th International Conference on Distributed Computing Systems. ICDCS, IEEE, pp. 1243–1248.

Ressi, D., Pistellato, M., Albarelli, A., Bergamasco, F., 2022. A relevance-based cnn trimming method for low-resources embedded vision. In: AIxIA 2021–Advances in Artificial Intelligence: 20th International Conference of the Italian Association for Artificial Intelligence. Virtual Event, December 1–3, 2021, Revised Selected Papers, Springer, pp. 297–309.

Ressi, D., Romanello, R., Piazza, C., Rossi, S., 2023. Neural networks reduction via lumping. In: AIxIA 2022 – Advances in Artificial Intelligence. Springer International Publishing, pp. 75–90.

Saad, M., Khan, M.K., Ahmad, M.B., 2022. Blockchain-enabled vehicular Ad Hoc networks: A systematic literature review. Sustainability 14 (7), 3919.

Safana, M.A., Arafa, Y., Ma, J., 2020. Improving the performance of the proof-of-work consensus protocol using machine learning. In: 2020 Second International Conference on Blockchain Computing and Applications. BCCA, IEEE, pp. 16–21.

Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A., 2019. Blockchain for AI: Review and open research challenges. IEEE Access 7, 10127–10149.

Salamon, J., Bello, J.P., 2017. Deep convolutional neural networks and data augmentation for environmental sound classification. IEEE Signal Process. Lett. 24 (3), 279–283.

Salha, R.A., El-Hallaq, M.A., Alastal, A.I., 2019. Blockchain in smart cities: Exploring possibilities in terms of opportunities and challenges. J. Data Anal. Inf. Process. 7 (3), 118–139.

Samuel, O., Javaid, N., Alghamdi, T.A., Kumar, N., 2022. Towards sustainable smart cities: A secure and scalable trading system for residential homes using blockchain and artificial intelligence. Sustainable Cities Soc. 76, 103371.

Saxena, S., Bhushan, B., Ahad, M.A., 2021. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. J. Netw. Comput. Appl. 181, 103050.

Scicchitano, F., Liguori, A., Guarascio, M., Ritacco, E., Manco, G., 2020. Deep autoencoder ensembles for anomaly detection on blockchain. In: Foundations of Intelligent Systems: 25th International Symposium, ISMIS 2020, Graz, Austria, September 23–25, 2020, Proceedings. Springer, pp. 448–456.

Sengupta, J., Ruj, S., Bit, S.D., 2020. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and iIoT. J. Netw. Comput. Appl. 149, 102481.

Serrano, W., 2022. Verification and validation for data marketplaces via a blockchain and smart contracts. Blockchain Res. Appl. 3 (4), 100100.

Shafay, M., Ahmad, R.W., Salah, K., Yaqoob, I., Jayaraman, R., Omar, M., 2022. Blockchain for deep learning: review and open challenges. Cluster Comput. 1–25.

Sharma, A., Podoplelova, E., Shapovalov, G., Tselykh, A., Tselykh, A., 2021. Sustainable smart cities: convergence of artificial intelligence and blockchain. Sustainability 13 (23), 13076.

Shinde, R., Patil, S., Kotecha, K., Ruikar, K., 2021. Blockchain for securing ai applications and open innovations. J. Open Innov. Technol. Mark. Complex. 7 (3), 189.

Shorten, C., Khoshgoftaar, T.M., 2019. A survey on image data augmentation for deep learning. J. Big Data 6 (1), 1–48.

Singh, S.K., Azzaoui, A., Kim, T.W., Pan, Y., Park, J.H., 2021. DeepBlockScheme: A deep learning-based blockchain driven scheme for secure smart city. Hum.-Centric Comput. Inf. Sci. 11 (12), 1–13.

Singh, P., Elmi, Z., Lau, Y.-y., Borowska-Stefańska, M., Wiśniewski, S., Dulebenets, M.A., 2022. Blockchain and AI technology convergence: Applications in transportation systems. Veh. Commun. 100521.

Singh, A., Gupta, S., 2022. Learning to hash: A comprehensive survey of deep learning-based hashing methods. Knowl. Inf. Syst. 64 (10), 2565–2597.

Singh, S., Sharma, S., 2018. Forecasting stock price using partial least squares regression. In: 2018 8th International Conference on Cloud Computing, Data Science & Engineering. Confluence, IEEE, pp. 587–591.

Singh, S., Sharma, P.K., Yoon, B., Shojafar, M., Cho, G.H., Ra, I.-H., 2020a. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities Soc. 63, 102364.

Singh, K., Tiwari, R., Johri, P., Elngar, A.A., 2020b. Feature selection and hyper-parameter tuning technique using neural network for stock market prediction. J. Inf. Technol. Manag. 12 (Special Issue: The Importance of Human Computer Interaction: Challenges, Methods and Applications), 89–108.

Singhal, T., Bhargavi, M., Hemavathi, P., 2021. Coalescence of artificial intelligence with blockchain: A survey on analytics over blockchain data in different sectors. Emerg. Technol. Data Min. Inf. Secur. 703–711.

Soares, M.A.C., Parreiras, F.S., 2020. A literature review on question answering techniques, paradigms and systems. J. King Saud Univ.-Comput. Inf. Sci. 32 (6), 635–646.

Sondhi, S., Saad, S., Shi, K., Mamun, M., Traore, I., 2021. Chaos engineering for understanding consensus algorithms performance in permissioned blockchains. arXiv:2108.08441.

Sun Yin, H., Vatrapu, R., 2017. A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In: 2017 IEEE International Conference on Big Data. Big Data, pp. 3690–3699. http://dx.doi.org/10.1109/BigData.2017.8258365.

Sundaresan, S., Kumar, K.S., Nishanth, R., Robinson, Y.H., Kumar, A.J., 2021. Artificial intelligence and machine learning approaches for smart transportation in smart cities using blockchain architecture. In: Blockchain for Smart Cities. Elsevier, pp. 35–56.

Taghavi, M., Bentahar, J., Otrok, H., Bakhtiyari, K., 2023. A reinforcement learning model for the reliability of blockchain oracles. Expert Syst. Appl. 214, 119160.

Tan, R., Tan, Q., Zhang, P., Li, Z., 2021. Graph neural network for ethereum fraud detection. In: 2021 IEEE International Conference on Big Knowledge. ICBK, IEEE, pp. 78–85.

Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P.K., Hong, W.-C., 2019. Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access 8, 474–488.

Tanwar, S., Kaneriya, S., Kumar, N., Zeadally, S., 2020. ElectroBlocks: A blockchain-based energy trading scheme for smart grid systems. Int. J. Commun. Syst. 33 (15), e4547. http://dx.doi.org/10.1002/dac.4547.

Ting, K.M., Washio, T., Wells, J.R., Aryal, S., 2017. Defying the gravity of learning curve: A characteristic of nearest neighbour anomaly detectors. http://dx.doi.org/10.1007/s10994-016-5586-4.

Treleaven, P., Brown, R.G., Yang, D., 2017. Blockchain technology in finance. Computer 50 (9), 14–17.

Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Buenzli, F., Vechev, M., 2018. Securify: Practical security analysis of smart contracts. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 67–82.

Tubino, R.R., Robardet, C., Cazabet, R., 2022. Towards a better identification of bitcoin actors by supervised learning. Data Knowl. Eng. 102094.

Ullah, F., Al-Turjman, F., 2021. A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. Neural Comput. Appl. 1–22.

Vasudevan, B., et al., 2021. Effective implementation of neural network model with tune parameter for stock market predictions. In: 2021 2nd International Conference on Smart Electronics and Communication. ICOSEC, IEEE, pp. 1038–1042.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł., Polosukhin, I., 2017. Attention is all you need. Adv. Neural Inf. Process. Syst. 30.

Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P.C., Krishnaraj, N., 2021. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. J. Supercomput. 77 (9), 9576–9596. http://dx.doi.org/10.1007/s11227-021-03637-3.

Vickrey, W., 1961. Counterspeculation, auctions, and competitive sealed tenders. J. Finance 16 (1), 8–37, URL http://www.jstor.org/stable/2977633.

Vidal, F.R., Ivaki, N., Laranjeiro, N., 2023. OpenSCV: An open hierachical taxonomy for smart contract vulnerabilities. arXiv preprint arXiv:2303.14523.

Waltl, B., Sillaber, C., Gallersdörfer, U., Matthes, F., 2019. Blockchains and smart contracts: a threat for the legal industry? In: Business Transformation Through Blockchain. Springer, pp. 287–315.

Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., Wang, F.-Y., 2019. Decentralized autonomous organizations: Concept, model, and applications. IEEE Trans. Comput. Soc. Syst. 6 (5), 870–878.

Wang, R., Luo, M., Wen, Y., Wang, L., Raymond Choo, K.-K., He, D., 2021a. The applications of blockchain in artificial intelligence. Secur. Commun. Netw. 2021, 1–16.

Wang, W., Song, J., Xu, G., Li, Y., Wang, H., Su, C., 2020. Contractward: Automated vulnerability detection models for ethereum smart contracts. IEEE Trans. Netw. Sci. Eng. 8 (2), 1133–1144.

Wang, X., Wang, X., Wilkes, M., Wang, X., Wang, X., Wilkes, M., 2021b. A k-nearest neighbour spectral clustering-based outlier detection technique. In: New Developments in Unsupervised Outlier Detection: Algorithms and Applications. Springer, pp. 147–172.

Wang, Y., Wu, C., Herranz, L., van de Weijer, J., Gonzalez-Garcia, A., Raducanu, B., 2018. Transferring gans: generating images from limited data. In: Proceedings of the European Conference on Computer Vision. ECCV, pp. 218–234.

Wong, E., 1986. Retrieving dispersed data from SDD-1: A system for distributed databases. In: Distributed Systems, Vol. II: Distributed Data Base Systems. pp. 227–245.

Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., Rong, C., 2019. A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet Things J. 6 (5), 8114–8154.

Wu, Y., Wang, Z., Ma, Y., Leung, V.C., 2021. Deep reinforcement learning for blockchain in industrial IoT: A survey. Comput. Netw. 191, 108004.

Xia, X., Pan, X., Li, N., He, X., Ma, L., Zhang, X., Ding, N., 2022. GAN-based anomaly detection: a review. Neurocomputing.

Xie, J., Tang, H., Huang, T., Yu, F.R., Xie, R., Liu, J., Liu, Y., 2019. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. 21 (3), 2794–2830.

Xiong, Y., Li, Z., 2022. Privacy-preserved average consensus algorithms with edge-based additive perturbations. Automatica 140, 110223.

Xu, H., Wu, J., Pan, Q., Guan, X., Guizani, M., 2023. A survey on digital twin for industrial internet of things: Applications, technologies and tools. IEEE Commun. Surv. Tutor..

Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., Zheng, Z., 2022. Fusing blockchain and AI with metaverse: A survey. IEEE Open J. Comput. Soc. 3, 122–136.

Ye, Y., Qiu, D., Sun, M., Papadaskalopoulos, D., Strbac, G., 2020. Deep reinforcement learning for strategic bidding in electricity markets. IEEE Trans. Smart Grid 11 (2), 1343–1355. http://dx.doi.org/10.1109/TSG.2019.2936142.

Zenati, H., Romain, M., Foo, C.-S., Lecouat, B., Chandrasekhar, V., 2018. Adversarially learned anomaly detection. In: 2018 IEEE International Conference on Data Mining. ICDM, IEEE, pp. 727–736.

Zhang, S., Lee, J.-H., 2020. Analysis of the main consensus protocols of blockchain. ICT Express 6 (2), 93–97.

Zhang, Y., Liu, Y., Chen, C.-H., 2020. Survey on blockchain and deep learning. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications. TrustCom, IEEE, pp. 1989–1994.

Zhang, F., Yang, Q., 2020. Energy trading in smart grid: A deep reinforcement learning-based approach. In: 2020 Chinese Control and Decision Conference. CCDC, pp. 3677–3682. http://dx.doi.org/10.1109/CCDC49329.2020.9164350.

Zhao, Y., Qu, Y., Xiang, Y., Zhang, Y., Gao, L., 2023. A lightweight model-based evolutionary consensus protocol in blockchain as a service for IoT. IEEE Trans. Serv. Comput..

Zhi, X., Satsangi, Y., Moran, S., Eloul, S., 2022. Ledgit: A service to diagnose illicit addresses on blockchain using multi-modal unsupervised learning. In: Proceedings of the 31st ACM International Conference on Information & Knowledge Management. pp. 5069–5073.

Zhu, J., Cao, J., Saxena, D., Jiang, S., Ferradi, H., 2023. Blockchain-empowered federated learning: Challenges, solutions, and future directions. ACM Comput. Surv. 55 (11), 1–31.

Zhuang, Y., Liu, Z., Qian, P., Liu, Q., Wang, X., He, Q., 2020a. Smart contract vulnerability detection using graph neural network.. In: IJCAI. pp. 3283–3290.

Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., Xiong, H., He, Q., 2020b. A comprehensive survey on transfer learning. Proc. IEEE 109 (1), 43–76.

Zou, W., Lo, D., Kochhar, P.S., Le, X.-B.D., Xia, X., Feng, Y., Chen, Z., Xu, B., 2019. Smart contract development: Challenges and opportunities. IEEE Trans. Softw. Eng. 47 (10), 2084–2106.

Dalila Ressi is a postdoc researcher of computer science at University of Udine. She received her Ph.D. degree in computer science in 2022 from University Ca' Foscari of Venice. During her Ph.D. she focused on providing and optimizing AI-based solutions for Microtec s.r.l., a leading company for scanning and optimization approaches in sawmilling and wood processing industry. Her current research consists in combining machine learning techniques and distributed ledger technology, especially to mitigate security issues.

Riccardo Romanello is a Ph.D. student in Computer Science and Artificial Intelligence at University of Udine.

His main research focus is Quantum Computing. In particular, the topics he is currently investigating are Graphs encoding in Quantum Computing, Quantum Automata and Quantum Circuit synthesis.

Nevertheless, he also works on classical computer science topics like automata minimization and neural network compression.

Carla Piazza received her Ph.D. in computer science in 2002 from the University of Udine. She is currently full professor of computer science at the University of Udine. She has been visiting scholar at the New York University (2004). Her research interests include formal methods and algorithms on graphs with application to the analysis of complex systems in different fields such as systems biology, quantum computing, blockchain models.

Sabina Rossi received her Ph.D. in computational mathematics and informatics from the University of Padova in 1994. She is a full professor of computer science at the University Ca' Foscari of Venice. She has been a visiting professor at Universitè Paris 7 (2007) and a research fellow at the Universitè Catholique de Louvain-la-Neuve, Belgium (1997). Her current research focuses on the development of formal tools for analysis and verification based on process algebraic techniques and, specifically, on stochastic process algebras. The proposed theoretical models have been used to verify the correctness and evaluate the performance of ad hoc mobile wireless networks, systems with fork-join constructs, distributed systems with load balancing, blockchain systems.