A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments

Article *in* IEEE Access · January 2022

DOI: 10.1109/ACCESS.2022.3203568

CITATIONS
7

READS
247

4 authors, including:

Oumaima Fadi
Université Internationale de Rabat
5 PUBLICATIONS **12** CITATIONS
SEE PROFILE

Karim Zkik
ESAIP École d'Ingénieurs
53 PUBLICATIONS **720** CITATIONS
SEE PROFILE

Abdellatif el Ghazi
Université Internationale de Rabat
17 PUBLICATIONS **193** CITATIONS
SEE PROFILE

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A survey on blockchain and Artificial intelligence technologies for enhancing security and privacy in smart environments

FADI Oumaima[1], ZKIK Karim[2], EL GHAZI Abdellatif[1], BOULMALEF MOHAMMED[1]

[1] TICLab , International University of Rabat, Sale Al Jadida, Morocco.

[2] CERADE, Esaip école d'ingénieur, Agers, France.

Corresponding author: FADI Oumaima (e-mail: oumaima.fadi@ uir.ac.ma).

ABSTRACT Smart environments consist of a collection of sensors, actuators, and numerous computing units that improve human life. With the booming of smart environments, data generation has been notably increasing in recent years, which must be managed in a smart and optimal manner. The components (i.e., workstations and cloud) that are used for data processing are not the best to recommend since it is risky and resource costing. For that matter, enterprises, firms and companies are deploying blockchain technologies (BT) as a more suitable alternative. In fact, blockchain is a distributed transaction ledger ensuring the reliability and transparency of data. However, BT faces some inherent security challenges such as DoS, eclipse and double spending attacks as well as Advanced Persistent Threat (APT) and malware. Thus, advanced anomaly detection and mitigation approaches, especially the ones using artificial intelligence (AI) techniques (e. g. Machine Learning, Deep Learning, Federated Learning) are required to address the aforementioned issues. In combination, AI and BT are capable of detecting anomalies within blockchain networks with high accuracy. In this paper, with a focus on cyber security issues, we explore the challenges of blockchain deployment in smart environments. Additionally, we explore the use of anomaly and prevention AI-based techniques as a ledger of blockchain technologies to address the security issues in smart environments. Thus, we propose a framework that emphasizes the challenges of BT, values and capabilities of BT-AI integration. We also present research trends to illustrate potential research paths for improving the security of blockchain networks through artificial intelligence.

INDEX TERMS Blockchain Technology – Artificial Intelligence – Security and privacy – Smart environments- Machine Learning- Anomaly detection

I. INTRODUCTION

Due to its unique and efficient approach for storing and transmitting data in a traceable and secure manner, blockchain technology has infiltrated most industries in recent years. Concurrently, as smart environments evolve, more data is generated, which needs to be securely stored and managed. In fact, the blockchain is performing a key role in preserving users' data and maintaining network members' anonymity. Additionally, blockchain technology has emerged as the most ideal ledger for transfer and storage of data; it is a distributed tamperproof ledger with proven security. In fact, blockchain is being embraced by many worldwide firms since it is adopted in a variety of fields such as industry and logistics, health, finance, and so on. Moreover, the adoption of blockchain technology in the industry remediates congestion, data loss risk, data fraud, and cost inflation. According to [1], blockchain technology is reaching its full potential in any application era, providing a secure, transparent and distributive alternative to centralized applications.

Many initiatives combining blockchain and IoT technology have been developed to provide safe, reliable, and cost-effective storage/transmission of data. [108]. However, IoT blockchain-based networks have been subjected to numerous attacks, including DAO attacks, DoS attacks, eclipse attacks, APT attacks, and malware attacks, revealing their security vulnerabilities. Therefore, blockchain-based networks raise some security and privacy concerns, creating trending research gaps.

Due to its ability to process and analyze huge amounts of data, Artificial Intelligence and its branches (Machine Learning, Federated Learning, Deep Learning…) are able to solve many open issues.

Leveraging AI algorithms will enable the blockchain networks to execute high computation operations and carry out complex tasks. For instance, AI can be extremely useful in automating tasks (e.g. automated sign-in for blockchain nodes). AI can be also applied for detecting attacks and invoking appropriate security mechanisms, as well as isolating the compromised elements or predicting potential cyber-crime activities and/or cyber-criminal entities within blockchain networks [2]. Following an introduction to BC technology, including its architecture and protocols, this paper examined the main challenges associated with blockchain networks. We aim to provide a detailed and critical analysis of related work integrating blockchain and artificial intelligence for enhancing security and privacy in smart environments. To achieve that, our approach incorporates a framework introducing the challenges of blockchain, the faculties in which we highlight how AI can assist blockchain networks security, as well as the resulting values of this integration. We conclude our work by suggesting research trends to pursue research within the BT-AI vision in smart environments.

This paper is organized as followed: Section 2 presents an

overview of the blockchain technology and the artificial intelligence; in which we introduce the background, the taxonomy and the architecture of both technologies. The research scope and methodology approaches are carried out in section3, it also emphasizes multiple related works that discuss the inherent challenges of the blockchain networks and suggest the integration of AI as a solution to these issues. Section 4 discusses some boarder perspective of the future works and research trends. Thereafter, we conclude our work in the conclusion section.

II. OVERVIEW OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

A. BLOCKCHAIN TECHNOLOGY

1. Blockchain technology overview

Companies, institutions, and organizations mostly use centralized networks, which are managed by third parties; transactions are transmitted in a centralized manner, resulting in less efficient data flow. In fact, the blockchain technology has been introduced to secure resources, solve the central control issues by avoiding the bottle neck problems and optimize storage points [3]. In addition, blockchain addresses trust issues such as data loss or abuse by eliminating the need to control or manage data by third parties. The data is stored in distributed areas around the world and the data updates are simultaneously executed in all the blockchain nodes. Plus, the blockchain is a tamper-proof ledger, which makes it hard to modify or delete data. Lastly, the consensus protocols ensure the fluent functioning of the blockchain networks (transactions and blocks validation) [4]. Therefore, the blockchain solves the authority issues of centralized architecture and ensures data privacy using hash mechanisms [98].

The blockchain is a layer-based technology. As figure 1 illustrates, the infrastructure layer encapsulates the time-stamped data blocks which has control over the storage of the nodes. The platform layer is composed of Web API and the distributed computing layer consists of various consensus algorithms and security policies such as hashing operations. Moreover, the application layer brings programmability into blockchain and it is composed of blockchain-based business applications.

Because the blockchain network is decentralized, an automated mechanism is needed to ensure the agreement of nodes on valid transactions. Consensus-mechanism algorithms handle this vital task. Consensus is considered as the backbone of the blockchain functionality, this implies that the peer-to-peer communication between numerous nodes must be controlled in a way that no center entity control is needed, so any behavior inside the blockchain network can't be executed without the agreement of the network members [6]. Blockchain adopts multiple consensus mechanisms such as the proof of work (PoW), the proof of stake (PoS), the proof of authority (PoA) etc.

Lastly, the blockchain is a modern technology that changed the world perspectives and impacted multiple domains such as industry, finance, health care, energy, advertising, societal applications [5].

2. Blockchain for smart environments: Concepts and challenges

Although in smart environments we deal with big amount of data, blockchain has a vital role to ensure data integrity and reliability. Blockchain technology is able to manage the complexity of multiple devices and applications in a distributed architecture [7]. In fact, blockchain is recently seen as a fundamental infrastructure to manage transactions in Metaverse [96]. According to [8], the ultimate goal of smart environments is to facilitate the citizens access to multiple services, in this part we will illustrate some of most common applications deployed in smart environments (e.g. smart healthcare, smart transportation, smart manufacturing).

Smart Healthcare: it's one of the sectors growing on the blockchain technology. The healthcare industry generates a tremendous amount of data (e.g., clinical trials, patient medical records, medical analyses), for that matter storing all this data in one place is neither secure nor scalable. Thus, blockchain is the best option to ensure the integrity of patients' data and protect its confidentiality [9][95], it also contributes in securing IoT systems for remote patient monitoring [110]. Blockchain provides a decentralized structure to store and manage data in order to avoid any possible data loss or fraud [10][101].

Smart transportation: Smart vehicles have gained

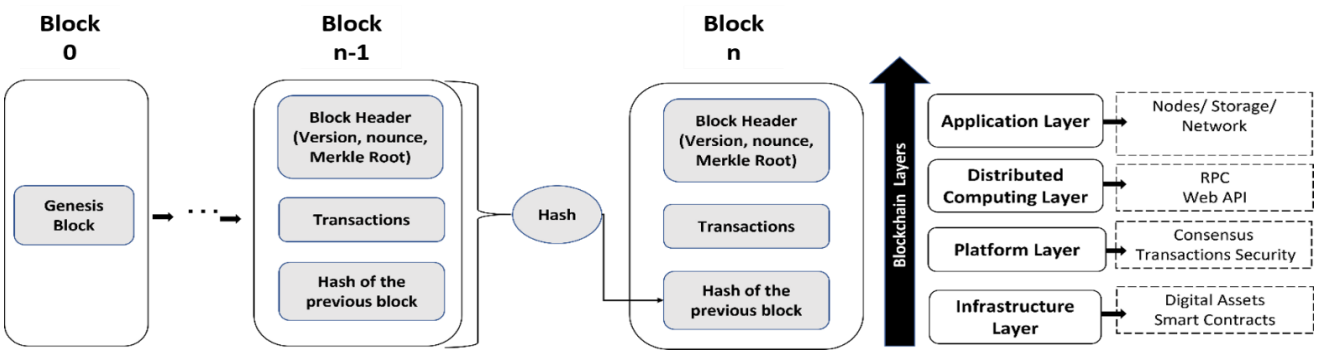

Figure 1: Blockchain structure

significant attention in recent years since it efficiently solves the congestion problems and provide safety [95]. Vehicles are now able to connect to the Internet and communicate with one another. Also, smart transportation aims to manage traffic and promote its quality while also providing comfort and convenience for drivers and passengers [11][112][113]. The distributed design of blockchain technology has the potential to increase the reliability of smart transportation as well as the vehicles' peer to peer communication and data sharing.

Smart industry: The blockchain records and maintains the metadata of the manufacturing systems. The supply chain is a common ground of application, in which transactional data that includes master databases, financial information, and strategic process is stored and transmitted in a distributed manner [12]. In such cases, the deployment of smart contracts [13] boosts the traceability of the product throughout the production line, it also enhances the transparency and privacy of data between the industry entities e.g. suppliers, retailers, customers. One of the recent works deployed blockchain-based framework to ensure a trustworthy data generation making industrial-based Digital Twin projects more reliable [99].

This paper provides an overall taxonomy of the blockchain technology, the previous section shed the light on the structure of BC, its protocols and areas of applications within smart environments. However, the blockchain faces multiple security issues. AI can assist blockchain networks overcome these issues.

AI-based algorithms, in particular, may assist securing blockchain networks and maintaining their privacy by exploiting training data.

The purpose of this survey is to provide a detailed study of the blockchain challenges and present an overall overview of related work that focus on securing the blockchain inside smart environments using artificial intelligence. To do that, in section 2, we will present an overview of artificial intelligence techniques and methods.

B. ARTIFICIAL INTELLIGENCE: promising path to secure blockchain networks

The concept of artificial intelligence was introduced in 1950, and it has been demonstrated that machines have the ability to think, as it is possible for them to make intelligent decisions. [14]. The artificial intelligence is the science that enable a machine to simulate human intelligence and it is introduced in multiple fields (e.g., science, finance, healthcare, logistics, smart city) [15] [16] [17] [18]. Moreover, artificial intelligence embeds multiple technologies and techniques. Yet, a considerable number of studies focused on the common ones such as machine learning, federated learning and deep learning.

1. Machine Learning overview

Machine learning (ML) has recently received considerable attention for its ability to accurately predict complex phenomena. Additionally, Machine learning algorithms can produce knowledge from given data to make decisions and interpretations similarly to humans. The machine learning methods are now deployed in a variety of fields, such as health care [19], biology science [20], transportation and logistics [21], finance [22]. Machine learning has multiple learning methods, and in this part, we will discuss the four classes of machine learning: Supervised, unsupervised, semi supervised and reinforcement learning.

Supervised learning: The supervised learning-based model is built under the supervision of the practitioner (developer) and trained with labeled data which involves the mapping between the inputs and targets (labels as outputs). The two common types of supervised learning are classification for predicting classes labels and regression for predicting continuous numeric labels.

Unsupervised learning: The machine learning type not requiring human supervision nor labeled data during the training phase. In fact, the model is trained to deduce and emphasize the relationship between the given data. Clustering is one of the common types of unsupervised learning.

Semi supervised learning: it takes the middle floor between supervised and unsupervised learning and it goes through three steps. First, it starts by training the model with the labeled data (supervised learning), then uses the unlabeled data so the model can predict its labels, we get the pseudo labeled data as an output. Third, the pseudo labeled data and the labeled data are all implemented to the model again for the training.

Reinforcement learning: the model learns in this case by interacting with the environment. The incentive and punishment mechanisms are utilized to guide the model getting a better results.

2. Federated Learning

Standard machine learning approaches require centralizing the training data on one machine or datacenter. However, new models are trained by multiple users requiring a distributed interaction on multiple mobile devices, giving rise to federated learning. The model is shared and trained in different devices using the users' data, the model updated is sent to the cloud and upgraded with the other users' models [23]. Federated Learning can be seen as a collaborative Machine Learning without centralized training data. Thus, the main advantages of federated learning are smart models enabling, power optimization, privacy preserving and facility of deployment, also the model can be tailored to the way it has been trained in each device. A federated learning approach is considered to be a suitable AI technique for the distributed architecture of the blockchain. [100].

3. Deep Learning overview

Substitute of machine learning, deep learning is based on ANN (Artificial Neural Network). The model is trained through multiple layers, it progressively extracts features from the input. Deep learning provides significant benefits

in domains such as computer vision, audio recognition, and natural language processing since it is based on unsupervised feature learning and feature hierarchy learning [24]. When high-dimensional weight parameters and large training data are supplied, performance can be excellent. Deep learning models, which have been particularly designed after the human brain, provide an exceptionally sophisticated approach to machine learning and are capable of tackling complex problems [25].

AI is a promising technology that brings more efficiency and performance to many applications in different fields, in the next section, we will illustrate the AI deployment in blockchain technology, and discuss how the AI capabilities can serve the blockchain security.

C. TOWARDS AN INTEGRATIVE FRAMEWORK OF BLOCKCHAIN-BASED ARTIFICIAL INTELLIGENCE

Despite blockchain's potential, the technology is facing different challenges, and artificial intelligence is being employed to overcome them. In this section, we will discuss various cases of BC-AI integration that cover diverse areas. (Energy management, tasks automation, security, privacy and scalability) [26].

It is stated in many studies that PoW (Proof of Work) is an energy consuming consensus mechanism due to the huge computation calculations executed by the miners to create a new block. For that matter, the authors [27] propose a machine learning approach that optimizes the energy consumption in a blockchain network. A machine learning and federated learning models are built to make the mining operation smarter, predict the most important transactions for miners and allow the blockchain transactions to be executed faster and more efficiently. Besides, some other BC-AI integration applications [28] focus on automating the signing up process which ensures time optimization and allows blockchain nodes to only check the credibility of some transactions and not go through all of the transactions. Moreover, the contribution of [29] used supervised ML to detect anomalous behavior and predict future intrusions or attacks.

Aside from the above discussion, the scalability of blockchain is limiting its functionality, due to the exponential increase of transactions [30], blockchain cannot handle the huge amount of data in a short time with a low cost. The study in [31] proved that artificial intelligence could support the growing sophistication of transactions and data in the blockchain and suggested a machine learning approach that applied lighting protocol (sharding and pruning).

One of the main trending research paths focus on securing the blockchain networks that are built in smart environments. This concept introduces the deployment of AI, BT and IoT and its integration in one spectrum. Thus, it opens smart environments to a wide range of possibilities by which data is collected processed and transmitted in a secure manner.

The work in [32] perform the BC-AI integration to share AI data in a safe and transparent way by building a privacy-based framework to share data through blockchain network. For instance, the research in [33] focus on healthcare systems that used blockchain to ensure the confidentiality of the patient's data sharing procedures to implement predictive AI models.

Additionally, the contribution in [34] demonstrates that in an IoT environment, embedding blockchain facilitates the processing of data in a transparent way and ensures its integrity. The smart environments, on the other hand cannot reach a full potential without the adoption of efficient security strategies, and blockchain is the best option to accomplish that [35]. Even so, blockchain adoption does not eliminate all privacy leakage risks [97]. Therefore, AI must be applied to maintain the security in the blockchain networks.

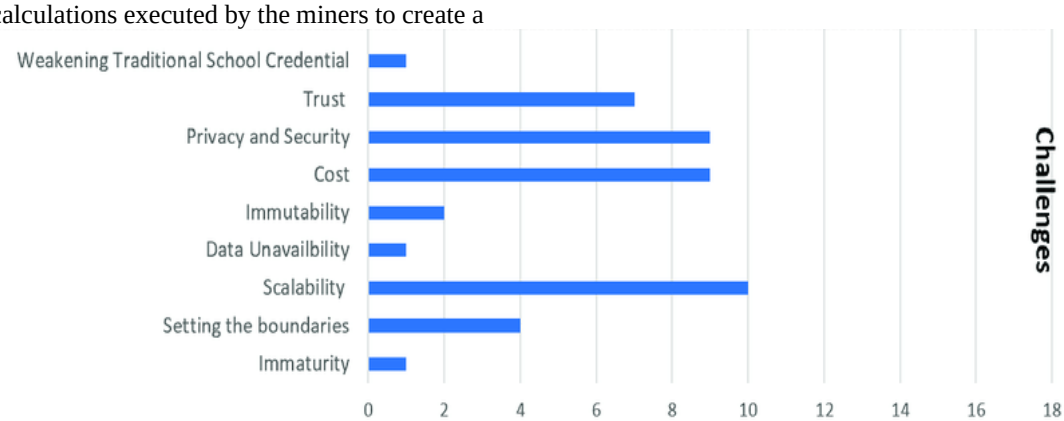

Figure 2: Blockchain challenges

Furthermore, while blockchain-based artificial intelligence appears to be promising, a thorough analysis of the blockchain's challenges is necessary. Since security is considered as the most intrinsic issue of blockchain, many studies have been conducted, as demonstrated in Figure 2.

To sum up, artificial intelligence not only brings more efficiency to the blockchain infrastructure but it secures the network, preserves its privacy and promotes its scalability.

III. RESEARCH SCOPE AND METHODOLOGICAL APPROACHES

In 2008, Satoshi NAKAMOTO published the first paper

on blockchain and the Bitcoin system [36], which led to the publication of numerous works providing an overview of this technology, its architecture, applications, and services. Some other works focused on the security and privacy challenges and vulnerabilities of blockchain technology, following that, more focus was addressed to smart solutions and alternatives to thwart the blockchain attacks and minimize its vulnerabilities. This paper is tackling the artificial intelligence-based solutions towards the aforementioned issues. Specifically, we discuss how AI can assist blockchain-based smart environments in improving scalability, enhancing security, and maintaining privacy.

In order to conduct a systematic survey analyzing BC-AI related contributions, we introduced a framework leading our research process and introducing the blockchain challenges, the blockchain-artificial intelligence faculties and values. Moreover, we adopted PRISMA protocol [114] to conduct this survey, we started the data collection on February 2021.This survey will be accomplished going from data collection, duplicates removement, inclusion and exclusion criteria application, as indicated in Figure3. The first step consists of initiating an effective and comprehensive review of articles from journal articles and conferences in order to fully surround the inherent challenges and shortcomings of blockchain. The second step consists of conducting a detailed critical analysis of the blockchain-AI integration applications to get an overview of the different suggested solutions, its approaches, strength points and limitations.

A. DATA COLLECTION METHOD

To conduct a systematic literature review that embed the existing literature work, we aim the most accurate and cited resources (articles, conference papers, scientific books, official websites…). The initial selection of sources has oriented our research.

This comprehensive research was conducted by browsing in the following digital libraries: Science Direct, Springer, IEEE Xplore, Wiley Online Library, Inderscience, Scopus. The browsing is keywords-based which are illustrated in Table1. The first selection of papers is based on the combination of the selected keywords in the title, abstract, and full text were selected and classified. Mainly, our research has two fundamental paths of research: BT and AI, thereafter we focused on the challenges and vulnerabilities of blockchain and mitigation techniques of AI methods.

Furthermore, we applied the inclusion and exclusion criteria as follow:

Inclusion Criteria (IC):

-IC1: Papers including blockchain technology.

-IC2: Papers including the deployment of artificial intelligence.

-IC3: Papers including the security and privacy issues of blockchain in smart environments.

Exclusion Criteria (EC):

-EC1: Papers focusing on the crypto currencies' behavior and not on the architecture of blockchain networks.

-EC2: Papers discussing the deployment of AI in IoT ecosystems without mentioning the deployment of blockchain.

-EC3: Papers discussing the impact of blockchain technology on the security of AI-based systems.

-EC4: Papers only discussing the applications areas of the BC-AI integration and not tackling its security aspects.

B. LITERATURE ANALYSIS APPROACH

After the data collection from articles journals, conferences and other sources, a classification is performed. The first classification is mainly based on the blockchain technology, its architecture and applications, then an overview of AI techniques including machine learning, deep learning and federated learning. After that, the research is narrowed to focalize not only on the integration of both technologies (BT and AI), but on the different applications in which AI techniques tackle the blockchain vulnerabilities; especially in terms of security improvement and privacy preserving of the blockchain, then the research is oriented to smart environments era; in which the AI techniques are implemented to benefit the privacy function of the blockchain networks.

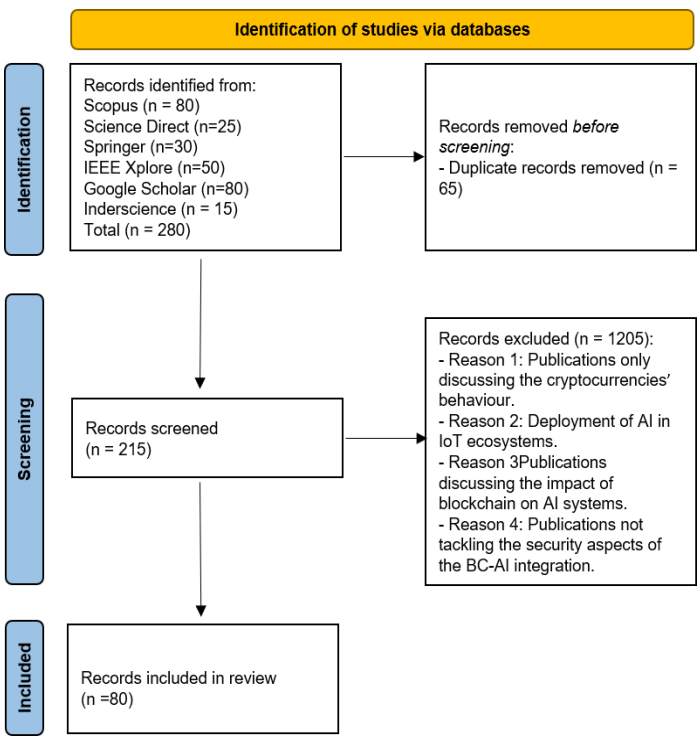

Figure 3:PRISMA flow diagram

IV. LITERATURE ANALYSIS

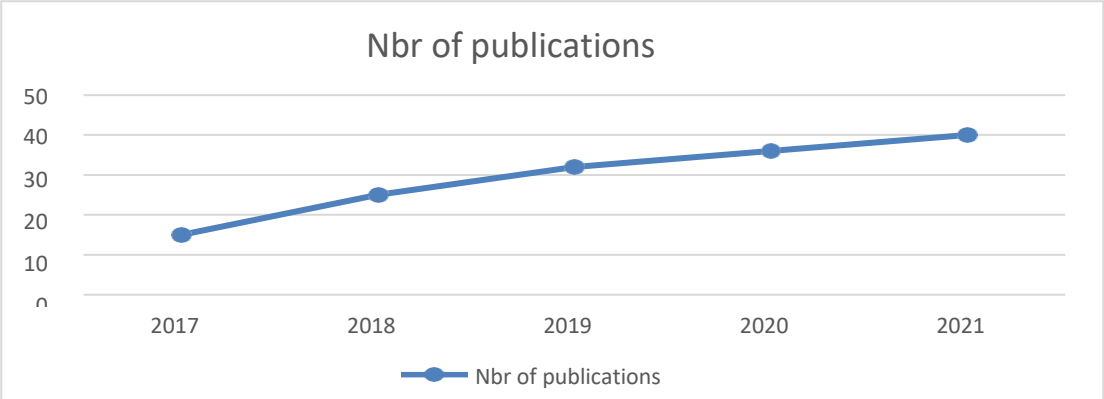

Figure 4: articles per year of publication

A. BIBLIOMETRIC ANALYSIS

1. Distribution of papers per year of publication

This paper gathers two trending technologies: Blockchain and machine learning technologies. To accomplish this survey, we focused on the related articles that were published starting from 2017. As illustrated in Figure 4, since 2017, the number of articles published on blockchain, AI (ML, DL, Federated learning…), and their integration has been rising.

2. Keywords statistics

The collection of articles to complete this survey stood on searching first by keywords. The top most used keywords are as followed: "Blockchain", "Artificial Intelligence", "Machine Learning"," Deep Learning", "blockchain challenges", "security", "Privacy", "Smart environments", "Anomaly Detection", "Transaction classification", "Intrusion detection", "Privacy preservation" … Table 1 lists the most used keywords and their frequency.

Table 1: Keywords frequency

keywords	Frequency	Keywords	Frequency
Blockchain	23	Anomaly detection	5
Machine Learning	24	Privacy Preserving	6
Security	22	Transaction classification	4
Privacy	16	Scalability	6
Smart environments	19	Blockchain vulnerabilities	4
Artificial Intelligence	64	Data Integrity	10

3. Contributing journals

We conducted a statistic study on the contributing journals according to the number of published articles in each journal/Conference. 12% of contributing articles are published in ACM Computing Surveys, 10% published in IEEE Communications Surveys &Tutorials and 24% published in International Conferences. As depicted in Table2, we ensured that our resource collection was diverse; we collected articles from computing science journals, management and economy journals, and production and industrial journals.

Table 2: Contributing journals

Journal	Number of published articles	Percentage
ACM Computing Surveys	7	12%
Future Generation Computer Systems	6	10%
IEEE Communications Surveys & Tutorials	6	10%
Applied Sciences	3	5%
IEEE Access	3	5%
International Journal of Production Research	3	3%
Pattern Recognition Letters	3	5%
Sensors	2	3%
Artificial Intelligence and Statistics	2	5%
Computers & Security	2	3%
The City Reader	1	2%
Telecommunications policy	1	2%
Annual Review of Biomedical Data Science	1	2%
Journal of Systems Architecture	1	2%
Information Processing Letters	1	2%
IEEE Wireless Communications	1	2%
IEEE Transactions on Industrial Informatics	1	2%
Journal of information security and applications	1	2%
IEEE Cloud Computing	1	2%
International conferences	14	20%
Total	**62**	**100%**

B. ISSUES ANALYSIS

In this section, we will review multiple blockchain security vulnerabilities, then we will study the artificial intelligence faculties assisting the aforementioned concerns. Thereafter, we will go through how artificial intelligence can benefit the blockchain and what are the BC-AI integration's added values. In Figure 5, we outline the

overall framework for this paper, starting with blockchain challenges and categorizing different attacks based on attacker intentions, BC-AI faculties and discussing some of the contributions aimed at solving these challenges.

1. Blockchain-based security challenges

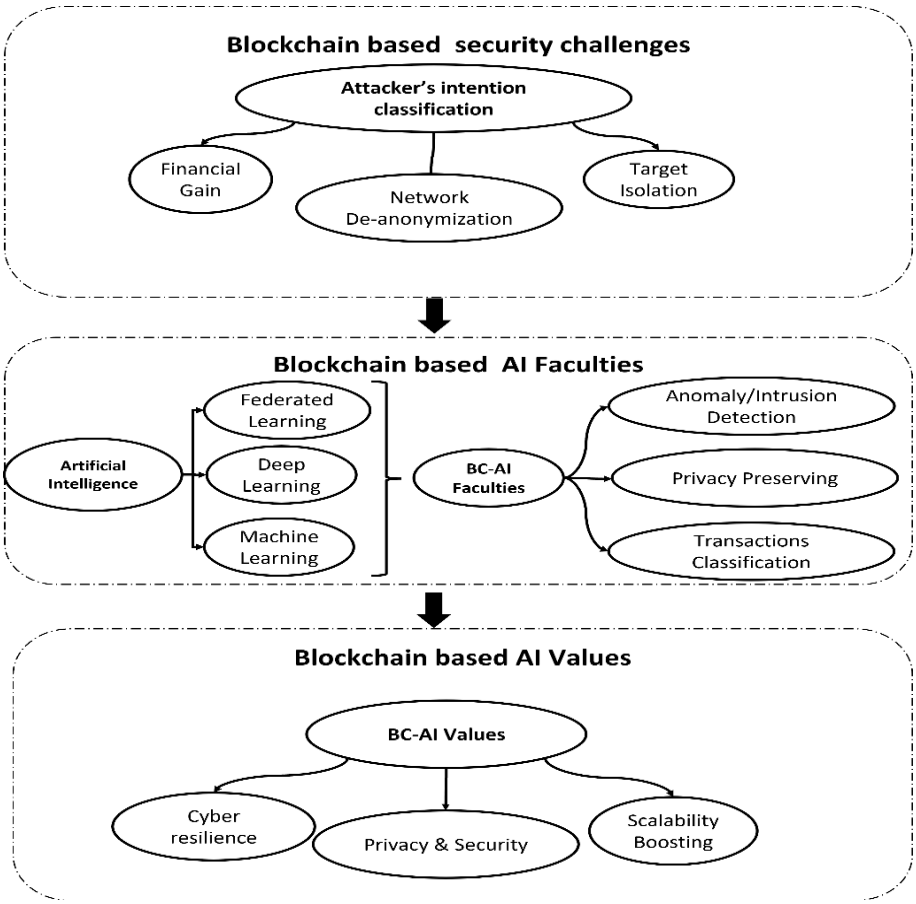

Figure 5:Issues analysis framework

In spite of the fact that blockchain has shown great potential in terms of securing data within a distributed and temper proof network, it is still subject to security and privacy challenges (e.g., DoS, eclipses, APTs, malware attacks).

Table3 introduces our attack's study classification. We divided the most well-known blockchain attacks into three groups based on the attacker's intentions. The first group is financial benefit motive, such as double spending and selfish mining, and the second group objective is node isolation, such as sybil attacks and eclipse attacks. Some other attacks like bloom filter and DAO attacks are included in the de-anonymization category.

Table3 introduces our attack's study classification. We divided the most well-known blockchain attacks into three groups based on the attacker's intentions. The first group is financial benefit motive, such as double spending and selfish mining, and the second group objective is node isolation, such as sybil attacks and eclipse attacks. Some other attacks like bloom filter and DAO attacks are included in the de-anonymization category.

- **FINANCIAL GAIN**

In 2020 blockchain technology market was estimated to be worth USD 3.67 billion [37]. One of the great motives of an attacker is monetary gain. As blockchain deals with millions of transactions worth billions of dollars per second all around the world, attackers use blockchain vulnerabilities to carry out harmful acts and steal assets from network nodes.

The authors in [38] had discovered a vulnerability in the Elliptic Curve Digital Signature Algorithm ECDSA, by this vulnerability an attacker can regenerate the user's private key since it does not contain enough randomness causing by that the private key loss (the wallet loss). Private keys are the user's security credentials, once lost, anyone can access the user's digital assets easily. A user losing their private key cannot be tracked or prevented from changing their blockchain account as blockchain does not have a policy for recovering this problem.

The distributed architecture of blockchain, more specifically, the decentralized cryptocurrency obviates the need of a centralized banking system. However, a new weakness of blockchain has been discovered, thus a new

attack takes place. The double spending attack is a fraudulent activity that enables the perpetrator to spend the same crypto money more than one time [39]. By exploiting the PoW based blockchain, the attacker launches its attack during the time between two the initiation and confirmation of two different transactions [40]. By using the same digital assets in both transactions simultaneously, only one of the two transactions aims to be valid, and the attacker benefits from both transactions outputs before the second transaction is mined to be fraudulent.

Other attacks are performed for the monetary gain purpose, such as selfish mining attack. This type of attack is also based on the PoW consensus mechanism of a blockchain. Within the PoW consensus mechanism, the miners of a blockchain deploy massive amounts of computing power to mine new blocks and receive incentive rewards. If it has enough computation power, the perpetrator exploits this situation and starts forking a private chain and mining their new blocks, the attacker may launch new transactions in their private chain and not announce it publicly. Also in the same context, it is stated that the attacker keeps on mining only on its private blockchain [41]. Expressly, the attacker will always keep tracking new blocks and hold it privately, once the sincere node finds about one of those blocks, the attacker will publish it immediately, then the sincere entities will mine this block on either branch (the private and public chain), however the attacker will mine the new block only on its private chain. By eventually getting longer than the public chain, the private chain will be deemed a sincere chain, and the attacker will receive the block rewards since all blockchain members will be mining on the longest chain.

The PoW consensus process made the blockchain a trustworthy network, but it is 51% vulnerable. In this case, the attacker's goal is to take control of more than half of the network; if completed, it will have the control over every transaction and will have the ability to allow or reject new blocks, reverse transactions and launch double spending attacks. Despite requiring over half of the total network's hashing power, the attack is still feasible on small blockchain networks [41].

- **De-anonymization**

Besides the aforementioned security issues, blockchain has a privacy issue that must be mentioned [42]. As blockchain is a transparent network, every transaction can be tracked back to the first block of the blockchain (genesis). In fact, all user's transaction history is transparent, so malicious entities could easily trace the user's public key, address and exploit that information [43]. The lack of privacy is one of the major blockchain challenges, and the temper-proof aspect of blockchain exacerbates the situation. Expressly, blockchain uses pseudonyms such as public keys to ensure the user's anonymity. However, once the pseudonyms data points are attributed to a user, it is possible for an attacker to trace back their transactions and reveal their identity [44]. The DAO attack is a prime example of this vulnerability. The DAO (Decentralized Autonomous Organization) opened a funding window for a specific initiative in 2016. During this time, the DAO code was compromised, resulting in the theft of cryptocurrencies worth $US3.6 million from the Ether fund [45].

The bloom filters were first suggested by Bloom in 1970 [46]. Aside from the storage space requirements for the blockchain installation, the exponential growth of the blockchain transactional volume aggravates the situation since it must verify the sincerity of new blocks and transactions. This issue becomes crucial when the blockchain users tend to use their mobile devices to perform and transfer their digital assets[47]. Due to the previous challenges, the bloom filters are introduced as a suitable solution. By adopting the SPV (Simple Payment Verification) approach, only small part of the blockchain is downloaded, so every user has a local wallet with which its transactions are performed. The bloom filters aim to embed the SPV clients addresses through these filters, the SPV clients transactions are forwarded between the local blockchain nodes. However, the attackers managed to exploit the bloom filters to reveal the user's addresses. The authors in [46] proved that if an SPV client who have less than 20 addresses is more likely to reveal all his addresses. The bloom filter attack is one of the major attacks that illustrate the privacy leakage issue of the blockchain network.

One of the major de-anonymization issues is the tunneling issue, more exactly the de-anonymization of TOR hidden services through using bitcoin transactions. The use of Bitcoin as a payment service endangers the privacy of TOR secret services and their customers. The contribution in [48] demonstrated that even if Bitcoin is used over an anonym network like TOR, the users are vulnerable to deanonymization and man-in-the-middle attacks at the network layer. Such an attack is achievable by exploiting at least one previous transaction in the Blockchain that contains the user's publicly declared Bitcoin addresses [49].

Furthermore, in a blockchain network, P2P relaying consists of relaying transactions between nodes. In fact, as soon as a node launches a transaction, it sends it to its peers. These peers decide whether the transaction is valid. If the transactions are proven to be valid, they will be propagated across the networks by each node's peers; otherwise, the transaction will be ignored. However, the blockchain relay mechanism is susceptible to a variety of threats. According to the authors [50], a DoS attack has never been successfully executed against a prominent cryptocurrency system.

On the other hand, BDoS (Blockchain Deny of Service) is introduced as the first type blockchain attack exploiting the reward mechanism and affecting miners participation. Expressly, BDOS targets the reward system discouraging the mining operation of some nodes. The attacker floods the servers with spam traffic, overloading them and

rendering them incapable of serving legitimate requests. It consists of publishing to the blockchain a proof that the attacker has a mining advantage. Consequently, the "rational" miners would quit mining if they realize they are at a disadvantage. If the decline in profitability is important enough that all miners quit mining, the attacker will also stop mining. As a result, the blockchain comes to a grinding stop.

- **Isolation intention**

Besides the above attacks, blockchain is also vulnerable to another type of attack that disrupts the link between the target and other nodes in the network. We will discuss the eclipse attack, BGP and Sybil attacks.

The key aim of the eclipse attack is to isolate the target from its peers, by filtering its incoming and outgoing connections. A Bitcoin node will have up to 8 outgoing connections and 117 incoming connections. Since the number of outgoing connections is limited, the attacker may compel the victim to only build connections to malicious nodes provided by the attacker [51]. The victim's computation power would be monopolized to carry out the attacker's malicious behavior [52]. In such cases, the attackers send unsolicited incoming connections to the target on a frequent and rapid basis, using a set of end-host IP addresses over which they have control.

The BGP (Boarder Gateway Protocol) is an exterior gateway routing protocol, it is designed to exchange packets between autonomous systems (AS) on the internet. However, some attackers exploit the BGP architecture to perform some fraudulent activities in the blockchain network. Expressly, the perpetrator intercepts the blockchain network by leveraging and manipulating the BGP routing. The BGP hijacking attack takes control over the network operators and causes delays of the messages between the blockchain nodes.

Moreover, the sybil attack occurs when an adversary creates multiple virtual identities in order to gain control of the blockchain network; these virtual nodes are referred to as sybil nodes. The attacker disconnects the sincere nodes from the blockchain. Miners in blockchain reach the network pool (mining pool) to exchange mining incentives. In fact, an attacker can generate many IDs in a network. Sybil attacks may also be carried out by a malicious pool user; the attacker introduces a large number of zero-power miners into the blockchain network. Such virtual mines contribute to data distribution but are unable to mine new blocks [6]. These virtual nodes forward only the attacker's block in the network and prevent the propagation of genuine users' blocks. Therefore, only the attacker's block is propagated across the network and attached to the blockchain. As a result, an attacker can receive more incentives while decreasing the total throughput of the system.

To schematize blockchain challenges, we provide a taxonomy of BT challenges based on the types of blockchain networks. Table 4 illustrates the usages, pros and cons, attacks and vulnerabilities of each type of blockchain (public, private and consortium). There are three different types of blockchain architecture based on authentication and access control [95]. The public blockchain provides a high degree of anonymity and accountability but it lacks privacy, making it vulnerable to DAO attacks, double spending attacks, and BGP hijacking. Privacy leakage is solved by the private blockchain, which makes it inexpensive. Meanwhile, private blockchains tend to resemble centralized networks, making them vulnerable to selfish mining attacks. Additionally, the consortium blockchain is introduced as a medium alternative form of blockchain ensuring the privacy of nodes and a flexible blockchain network.

Table 3: Blockchain challenges

Attacker's Intention	Attacks	References
Financial Gain	51% attack Selfish Mining Private key attack Double Spending	[53] [54] [55]
Target Isolation	Sybil Attack BGP Hijacking Eclipse Attack	[56] [53] [57] [58] [59] [60] [61]
De-anonymization	Bloom Filter Relay behavior DOS attack TOR Tunneling DAO (Privacy Leakage)	

Table 4: Blockchain Types

BC TYPES	DETAILS	USAGES	PROS	CONS	ATTACKS AND VULNERABILITIE S	REFERENCES
Public Blockchain (Permissionles)	• Creation and access of data is allowed to all nodes. • Smart contract publishment for every member. • Any member can run a node.	Bitcoin Ethereum	• Full Transparency • High level of Anonymity • Crypto economic incentives are given to miners • Distributed architecture	• Slow Performance • Energy inefficient • A major challenge is scaling	• 51% Attack • DAO Attack • Double Spending • BGP Hijacking attack • Selfish mining attack	[53] [54] [55]
Consortium Blockchain	• The validation of blocks process can vary depending on the authorities instructions. • Only predefined and pre-approved nodes contribute in the network and run the nodes. • Varying degree of decentralization and transparency. • Only pre-approved entities can see rhe recorded history. • All participants (nodes are known.	Quorum MultiChain Ethermint Tendermint Hyperledger	Efficient transactions High privacy Fault tolerance-based consensus protocols Decentralized architecture Economic incentive mechanisms	• More likely to gain control over the network • Occurrence of forks	• Eclipse attack • Botnet eclipse • BGP Hijacking attack	[53] [55]
Private Blockchain (Permissioned)	• Not everyone is welcome to join the network • Only predefined and pre-approved nodes contribute in the network and run the nodes. • Only pre-approved entities can access their own transactions • Varying degree • of decentralization and transparency. • Only pre-approved entities can see the recorded history or issue transactions of	• Ripple (XRP) • Hyperledger • Tendermint	• Mining is not required • No need for • crypto economic incentive. • Increased Performance. • Increased Scaling. • Transactions are faster • Consensus algorithms a computationally inexpensive.	• More likely to gain control over the network • Don't offer decentralized security as public blockchain. • Inflexible architecture without the incentive mechanisms • Occurrence of forks	• Eclipse attack • BGP Hijacking attack	[56] [53] [57] [58] [59] [60] [61]

2. Blockchain based AI Faculties

Although blockchain is nearly impossible to hack, its subsequent layers and implementations are not stable. As discussed in the previous section, blockchain faces inherent security and privacy challenges (e.g., DoS, eclipse, APT, malware attacks). With the increasing amount of personal data stored in blockchain- based communication systems and smart environments, privacy becomes a critical problem. In fact, artificial intelligence techniques seem to be the ultimate solution to tackle these problems [62].

In this segment, we will explore relevant work relating to blockchain-based artificial intelligence capabilities. We will categorize our research based on how AI approaches support blockchain networks. The first category focuses on transaction entity classification using supervised and unsupervised learning methods, while the second category studies anomaly detection in a blockchain network using machine learning, federated learning and deep learning techniques, then the third category demonstrates the artificial intelligence approach to protect and preserve the privacy of the blockchain network and de-anonymize its nodes.

- **TRANSACTIONS ENTITY CLASSIFICATION**

Authors in [63] use supervised learning to classify entities in payments that could be involved in cybercrime. The classification model is trained using machine learning. The dataset in this analysis includes not only tor markets, scams, ransomware, mixing, and stolen bitcoins, but also exchange, gambling, merchant services, hosted wallets, mining pools and personal wallets. By comparing accuracy and F1 score of all classifiers, the authors found that Bagging (78.46%) and Gradient Boosting (80.76%) stand out as the best classifiers, which are then applied to analyze the 10000 observations. The classification outcome shows that 5.79% (3.16%) addresses and 10.02% (1.45%) coins are from cybercriminal entities according to the bagging method (gradient boosting method). However, this approach suffers from under sampling and oversampling problems. Expressly, some classes have more samples than others; though personal wallets and exchanges have over 200 observations, categories such as stolen bitcoins have less than 10, which may explain the models' poor performance. Moreover, this approach focuses on classifying transactions only based on their types, it would be more efficient and practical if the classification combines both transactions type and its corresponding service, since each service has a specific spending patterns.

The contribution of [64] proposed a classification approach that categorize the bitcoin ecosystem transactions into four main classes: Exchange, Service, Gambling, MiningPool, based on data collected from 97 sources. The classification techniques used in this case are gradient boosted decision tree algorithm along with a Gaussian process-based optimization procedure that determines optimal hyperparameters. The authors take into account entity modeling, including features relevant for robustness to de-anonymization attacks, namely address re-use patterns. They also propose a discriminative model of transaction-to transaction behavior and show its effectiveness in practice. They analyzed the accuracy of the generative model using a large Bitcoin dataset of more than 10 million address. The accuracy in Exchange, Gambling, and Service categories are high, however, the accuracy in the Mining Pool category is poor. This may indicate that mining activities may not be appropriate as an independent label. However, given the large-scale existence of such public cryptocurrency transaction graphs, designing a tractable training and inference technique is a major challenge for such models with more complicated dependency structure and secret variables.

Other work deployed the stored transactions in the blockchain to classify the IoT nodes when implementing a blockchain in a smart environment, which may affect the user's privacy because the attacker can link the classified data to a certain user and obtain by that its identity. Dorri et al proposed a machine learning technique to solve this type of issues. Since the blockchain in this case is implemented in a smart home and it stores a real smart home traffic data, when applying machine learning, a 90% success rate of devices classification is obtained [65].

Singh et al applied machine learning to develop a model that can forecast the time window in which a mining node would accept and include a transaction in a block. The research also investigates the effects of unbalanced data on the selected classifiers Bayes, Random Forest and Multi-Layer Perceptron (MLP) with SoftMax output as well as alternate performance metrics for dealing with the dataset's imbalanced nature [66]. The authors in [67] use Supervised Machine Learning methods to determine whether an attack is likely to occur. If this is the case, the system should design a set of rules to either prohibit blockchain confirmation from the attacker(s) or to prohibit confirmation of the entire transaction until a new fair transaction is executed, i.e. no payoffs for anybody, in order to maintain fairness and integrity of the network. Also, an intelligent software agent at the network's application layer classifies the stakeholders' intentions and the value of the current service of the transaction. If the stakeholders' intention is found to be malicious in character, with the goal of colluding to commit a majority attack, the transaction is canceled and all stakeholders are requested for another transaction.

- **ANOMALY DETECTION**

A blockchain operated by artificial intelligence algorithm is capable of detecting attacks and malicious events/nodes as well as invoking appropriate security mechanisms and isolating the compromised elements.

The research in [68] deploys ML algorithm that applies automated signing of blockchain transaction, includes personalized identification of anomalous transactions and stores data from the anomaly detection model in the user private environment. The signing process by users is time consuming, not user-friendly and causes managing and controlling obstacles, plus users are not able to recognize possible intrusions while being involved in a digital signing process. The authors deploy isolation forest that splits the data into onliners and outliners, the blockchain node will

only verify before signing the unusual transactions instead of all transactions, and this can be used as reward in reinforcement learning or as a true label for supervised learning methods. Since not all anomalies are known, this approach presents a challenge since we cannot assess whether the anomaly detection system correctly classified the transaction, and the deployed methods are not adapted to the address's transaction patterns.

The approach of [69] consists of using Machine learning methods embedded in IoT devices in order to secure the dataflow and build a consensus-based structure. In fact, the authors implemented a blockchain-based IoT smart home network on hyperledger fabric which has low computational requirements and fast network response time which makes it adequate to IoT applications. By rejecting the inconsistent data, the blockchain network becomes AI-enabled by learning the possible dependencies and identifying those patters that are inconsistent with the rest of the measurements.

Li et al propose a framework to detect electricity consumption anomalies accurately and efficiently using distributed sensors processing ML and Big Data analysis [70]. Then they prepare a detection mechanism not only to detect anomalies timely but to assist stakeholders in making real time decisions in the era of industry 4.0. Additionally, cryptographic keys are used to ensure the security and integrity of the data transmission. KNN method is essentially a distance-based anomaly detection method. After the detection of abnormal electricity consumption and the capture of the anomaly, the substation of the smart grid makes a detection transaction with a signature to the blockchain network. However, the accuracy of the results can be improved, since the dataset could be more granular and the accuracy of deducted consumption classes could be improved.

The anomaly detection in the Bitcoin network is performed by authors in [71], where clients and transactions are considered suspicious.

Preuveneers et al present a permissioned blockchain-based federated learning method that involves updating an anomaly detection machine model. In a federated learning environment, the dataset (CICIDS2017) is spread across real network nodes (e.g. desktops, workstations), and these nodes highly contribute in the model training [72]. The autoencoder is used to detect abnormal activity in a network; the autoencoder is trained to detect benign behavior in the network, and a compressed feature vector is also deployed between the encoder and decoder. The reconstruction operation must be then executed successfully when applied to a benign dataflow. This approach improved the full transparency of the blockchain network over the distributed learning process but only a limited performance rate is achieved (from 5% to 15%). A deep neural network named DeepLog is deployed with the LSTM technique, and it assists the log pattern model in learning from regular execution and flagging anomalies from regular system execution [73]. Additionally, another contribution investigates the attacks performance against the deep learning-based intrusion detection on the NSL-KDD dataset [74]. They also state that deep learning allows an attacker to deceive the networks into misclassification, and that the vulnerabilities of neural networks used by intrusion detection systems have been empirically proven. Although the Deep learning-based anomaly detection is a promising approach, it still faces some issues in complex environments such as resource constraints, communication latencies and privacy concerns[75].

As for Bogner et al, they propose an IoT system for monitoring interconnected components [76]. It combines online machine learning for anomaly detection that is optimized for interpretability with the public Ethereum blockchain to ensure data integrity. The contribution of Meng focused on machine learning-based intrusion detection systems and collaborative intrusion detection networks, evaluating and researching the integration's major challenges: data sharing and trust management [77].

The contribution in [111] introduced SecureSVM for privacy preserving of IoT data during the training of a SVM classifier. In order to address data privacy, integrity, and ownership concerns when training SVM classifiers using IoT data from multiple providers, the authors combine the Paillier cryptosystem and blockchain techniques. Expressly, the user’s data to collect locally encrypted with Paillier using homomorphic encryption before being recorded on blockchain. In this way, the communication between the data provider and the data analyst is stored in the blockchain as transactions with inputs (the data provider's address, the type of IoT device, and the encrypted data) and outputs (the analyst's address). During the training process, Secure SVM evaluates the scalability of the system as the number of IoT data providers changes.

Other works deploy deep learning -based framework for anomaly detection in order to enhance the security of IoT-enabled MTS (Maritime Transportation Systems) by automating Cyber Threat Intelligence (CTI) strategies. The authors in [113] introduced a DL-based framework DLTIF for modeling and identifying cyber-attacks in MTS with 3 modules:

- Deep Feature Extractor (DFE) to extract hidden patterns from the network communication statistics using LSTM model.
- CTI-driven detection (CTIDD) for threat detection using Bi-GRU and sigmoid function.
- CTI attack type identification to identify exact threat and adopt defensive strategies using Bi- GRU and softmax function.

The DLTIF model is trained and tested on TON-IoT dataset (around 99% of validation accuracy).

- **PRIVACY PRESERVING**

There are some advanced techniques that are able to link blockchain user’s and cluster their addresses to real-world identities. Authors in [78] admit that this idea goes against the blockchain belief of the user’s privacy. Building upon this

idea, they investigate the anonymity of blockchain (especially the bitcoin users) and study the possibility of revealing to some extent the identity of users using supervised learning techniques. Using Supervised Machine Learning, the previous contribution develops a unique way for categorizing yet-unidentified clusters on the Bitcoin Blockchain. Using Gradient Boosting Classifier, they predict the category of an unidentified cluster on the Bitcoin Blockchain with 77 % (and an F1-score of 0.75). The dataset used in this research contains approximately 200 million transactions pertaining to 434 unique clusters. In order to perform an analysis for the Bitcoin transactions, this study applies the following supervised learning methods: k-Nearest Neighbors, Random Forests, Extra Trees, AdaBoost, Decision Trees, Bagging Classifier, Gradient Boosting. The results suggest that it is possible to categorize yet-unidentified clusters, implying that it is feasible to identify the category of a considerable fraction of entities on the Bitcoin Blockchain, challenging widespread views about Bitcoin's actual anonymity.

In terms of practical applications, this methodology has the potential to aid in criminal investigation, namely detecting suspect entities such as ransomware and spam. Even though this methodology provides a thorough analysis on bitcoin transactions and is able to identify unknown transactions, it cannot provide an effective solution to prevent de anonymization attacks and preserve bitcoin network privacy. Kim et al perform a privacy preserving[79] DML framework (Distributed Machine Learning) for the permissioned blockchain network [80]. An error-based aggregation rule is a new aggregation approach based on errors that was presented to compute global weights. The authors used a permissioned blockchain to make it feasible (Hyperledger Fabric). The proposed model has three phases: simulation, ordering, and execution. Each participant in the network simulates and computes each local gradient under the current global weight on their own local datasets. After that, the local gradient is broadcasted to the manager node with the authority which build the block at each learning iteration after reaching the consensus from the network. Participants thereafter commit a block in the network, which the authority node broadcasts. However, this study only focused on private blockchain networks.

Kumar et al proposed the framework TP2CDF to secure the blockchain network, their solution is based on two layer based privacy preserving [81]; they applied an enhanced type of consensus mechanism (ePoW) as a first layer of privacy, then the PCA technique is deployed to reduce the dimensionality of data to prevent the blockchain form cyber security attacks, which is accomplished through feature mapping, feature selection, feature normalization and feature transformation. However, this solution lacks scalability when the number of IoT nodes increases.

To achieve the same purpose, authors in [72] deployed the federated Machine Learning technique [82] in order to preserve the blockchain privacy by reducing the amount of data to be shared or centralized. Chen et al implemented the LearningChain framework to preserve the privacy of Ethereum blockchain, they demonstrate its efficiency and effectiveness through many training iterations [83]. They also developed a decentralized Stochastic Gradient Descent (SGD) algorithm to build a prediction model on the blockchain. They suggest a l-nearest aggregation technique to safeguard the system from potential Byzantine attacks and offer differential privacy- based techniques to safeguard each party's data privacy.

Other approaches adopted deep learning methods to preserve blockchain privacy; the authors in [84] developed the framework DeepChain that guarantees data privacy for each participant and provides auditability for the whole training process within the blockchain network. DeepChain is a collaborative training system with an incentive mechanism that encourages participants to engage in deep learning model training together and share the resulting local gradients. This protects the anonymity of local gradients while also ensuring the training process's traceability. Thus, the participants are driven to be honest by using incentive mechanisms and transactions.

In other contributions, it is noted that malicious packets establish fraudulent consensus in the blockchain network, G.Betarte et al deployed a firewall framework so that the packets fulfill the basic security criteria, however, as a result of many unrecognizable patterns outstripping the firewall's capabilities, the attacks became increasingly sophisticated. To avoid this problem, the authors in [85] analyzed packet header in real-time using AI models and historical data, this analysis aids in the detection of new and changing patterns. Also [86] estimates the degree of cyber criminality in a Bitcoin network using probability-based factor model (unsupervised learning), they evaluated the breach to determine whether it has the potential to create a damage.

Furthermore, Kumar et al present a privacy-preserving based framework to secure cooperative intelligent transport systems (CITS), the authors in [112] designed a two levels-based framework. The first level involves implementing a blockchain module to transmit CITS data securely between autonomous vehicles (AV). An enhanced-based proof of work consensus protocol (ePOW) is also used in smart contracts to ensure the integrity of data. On the other hand, the second level consists of a DL module using Long Short-Term Memory-Auto encoder to encode the CITS data. Thereafter, the authors adopt an attention-based recurrent neural network (A-RNN) for malicious events recognition. Using the dataset of CICIDS-2017, the model is trained with truncated Back Propagation Through Time (BPTT) for detecting multi-class attack (such as DOS, DDOS). Due to the size of the trained data, the authors use Inter Planetary File System to encrypt and store the data before sending it to the blockchain.

We prepared table 5 in order to summarize the related work and emphasize its strength points and shortcomings, table 5 categorizes the main contributions that perform AI techniques (Machine learning, deep learning, federated learning) to improve the privacy and security of blockchain

networks, in which we specified the research model, the type of blockchain used, the applied sector, the contribution result, the research design and the analysis technique and the limitations.

Table 5:Sum up of BT-AI integration contributions

AI Field	AI-BT faculties	References	Blockchain Type	Applied Sector	Research Design	Data Collection	Analysis Techniques	Main Contributions & Results	Limitations
Machine Learning	Transactions classification	[70]	public (Bitcoin ecosystem)	Financial Sector	Framework	bitcoin-transaction network-metadata 2011-2013	ML K-means and unsupervised SVM Deep Learning	Anomaly and Fraud detection.	Big analysis not mentioned.
		[75]	Public (Ethereum blockchain)	Industry 4.0	Framework	--	ML classification	Patterns classification	Big analysis not mentioned.
		[77]	public (Bitcoin Blockchain)	--	Framework	Chainanalysis	Supervised Learning classification- Gradient Boosting and Bagging Classifier	prediction of the category of an unidentified clusters in Bitcoin Blockchain . F1-score of 0.75.	Smart environments not mentioned. Privacy issue not deeply covered.
		[63]	public (Bitcoin ecosystem)	--	probabilistic model	Bitcoin dataset (10 million address)	Supervised Learning classification	Employment of gradient boosted . Decision tree algorithm .	No smart environments applied.
	Anomaly detection	[64]	Public	Smart home	Study & Simulation	--	Machine Learning (Classification)	Success rates over 90% in classifying IoT devices.	Security of blockchain not tackeled
		[67]	Public (Ethereum blockchain)	--	Simulation	--	ML Random Forest classification & Reinforcement Learning	Signing transactions automation.	No smart environments applied. Security & Privacy issues not tackled.
		[2]	public (Bitcoin Blockchain)	Cybercriminality	Estimation of cybercriminality	data provider Chainanalysis	Supervised ML classification of cyber-criminal related transactions	Bagging (78.46%). Gradient Boosting (80.76%) .	Dataset features not adaptable to smart environments. Big data analytics not included.
		[66]	Considering public, private and consortium blockchain	--	Conception & study	--	Machine Learning and Algorithmic Game Theory	Suggestion of intelligent agent software for blockchain anomaly. Detection (majority attack case).	No smart environments applied & no practical solution is suggested.
		[68]	--	Smart home	AIBC (AI-enabled Blockchain) framework	From 100 sensors and devices	ML classification	Outliners detection	Blockchain type not covered . Big analysis not mentioned.
		[87]	--	Smart Grid	Framework	From electricity pipelines and meters	ML & Big Data Analysis	Anomaly detection in energy consumption in smart grid	Blockchain type not covered . Security & Privacy issues not tackled.
	Privacy preserving	[65]	Public (Ethereum blockchain)	--	Predictive model	--	ML (Random Forest & Multi-Layer Perceptron (MLP))	Prediction of the confirmation time of an Ethereum transaction.	No smart environments applied.
		[80]	--	Smart Home	Framework	TP2CDF	Supervised learning PCA(Principal Component Analysis)	Privacy preserving implementing PCA technique and ePoW (enhanced Proof of Work).	Privacy of private or consortium blockchain not covered. Big Data Analysis.
	Anomaly detection	[81]	-- deep decentralized networks.		DeepLog Framework	client devices	Federated Learning	Anomaly and Fraud detection	Blockchain not mentioned.

Federated Learning		[71]	Permessioned blockchain	IoT nodes (e.g., desktops, workstations)	Framework	CICIDS2017 dataset	Federated Learning	Anomaly detection and blockchain. transparency enhancement.	Dataset features not adaptable to smart environments. Privacy issue not tackled.
	Privacy preserving	[82]	Public (Ethereum blockchain)	--	Framework	LearninChain	decentralized Stochastic Gradient Descent (SGD)	Preserve users data privacy in the blockchain network.	Smart environments not mentioned. Big Data Analysis.
		[78]	Permessioned blockchain	--	Framework	DML Framework	Distributed Machine Learning	Privacy preserving in a blockchain with PoA Consensus.	Smart environments not mentioned. Big Data Analysis.
Deep Learning	**Privacy preserving**	[76]	--	--	Review	--	--	Apply blockchain in IDS for data sharing and trust management.	AI solution not explained Blockchain type not covered . Security & Privacy issues not tackled.
		[83]	Public	--	Simulation	DeepChain	Deep Learning	Protection of the anonymity of local gradients and promotion of traceability of the blockchain.	Smart environments not mentioned. Privacy of private or consortium blockchain not covered. Big Data Analysis.
	Anomaly detection	[73]	--	--	Simulation	NSL-KDD dataset	Deep Learning	Intrusion Detection	Blockchain and smart environments not mention

3. Block-chain based artificial intelligence values

Some facets of blockchain have evolved as a result of applying AI methods to the blockchain networks; in this section, we will illustrate how artificial intelligence supports decentralized networks. The BT-AI integration values were classified into the following categories: scalability, cyber resilience, security and privacy.

As discussed in the previous section, scalability is a serious challenge in the blockchain networks, regarding the exponential increase of new transactions to be verified and initialized in smart environments, the bottleneck and latency problems represent a major. In order to assess the performance, scalability and integrity of blockchain-based IoT systems, the authors in [88] suggest a deep reinforcement learning (DRL) based method. The suggested approach was pursued in three steps, beginning with a system performance checker that covers scalability, decentralization, and security, then improving network scalability without affecting the security and decentralized aspects of the system. Finally, the DRL module selects and verifies the block size, block interval and the bloc producers.

Aside from the aforementioned values, the deployment of AI in blockchain networks has the greatest influence on smart environment security [115]. As stated by [69], machine learning techniques improved the integrity of data within the blockchain networks by detecting anomalous behavior inside a smart environment. The authors proved the efficiency of supervised learning techniques to detect and block malicious transactions or insincere nodes in the blockchain network.

The privacy of the blockchain networks was announced as a major challenge as well; to solve that, Kim et al proposed a privacy preserving DML framework (Distributed Machine Learning) for the permissioned blockchain network and proved the DML performance in preserving users [80].

Moreover, Machine Learning has also been used to predict potential cyber-crime activities and/or cyber-criminal entities within blockchain; the main goal of Yin et al work was to improve the resilience and security of data in a bitcoin system using machine learning. To do so, they implemented a solution for the estimation of malicious entities and transactions [86]. Jourdan et al contributed to the resilience of a blockchain network and the integrity of its transactions by applying machine learning to perform an automated classification of transactions inside the blockchain network [64].

The contribution of Kim et al focuses on securing the Bitcoin base networking application using unsupervised learning and AE. In order to accurately present the P2P traffic, the authors implemented a framework that sense the blockchain traffic and designed a simulated node to generate malicious events: Abn-DoS for DoS attacks and Abn-1p/Syn for eclipse attacks. They performed unsupervised learning to perform online anomaly detection (DoS and eclipse attacks) and presented an AE-based detection engine; this contribution provides an online anomaly detection that can be applied to different P2P networks such as Ethereum and implements a prototype sensing the blockchain traffic in a periodic manner, which can be used in further anomaly detection systems [89].

4. Research trends and future work

Our findings in the literature have steered our research in the direction of addressing the issues of blockchain networks and investigating current techniques to address these challenges using AI. The findings of the research are various; some approaches use machine learning algorithms to improve blockchain security, some include deep learning, others use federated learning to preserve the privacy of blockchain.

The literature review, on the other hand, revealed a number of tendencies. These trends represent research gaps that have yet to be properly resolved, necessitating a great deal of attention.

- **Research trend 1: Decentralized content provider: Privacy preservation**

The recommendation systems (RS) facilitate the users' browsing by estimating their content preferences and are now prevalent in multiple fields (e.g., social media, banking, e-commerce, retail, telecom) [102]. An accurate recommendation system requires the collection and analysis of data such as users' preferences, social media interactions or historical browsing data. Thus, the privacy issue arises because most of the data collected for recommendation systems contain sensitive and confidential information [104]. In fact, the privacy of a RS can be also included in its trustworthiness which must also be taken into consideration. Most of the related work focus on the precision of the RS but not enough attention is addressed to the security and privacy of the data deployed in the process. Moreover, the privacy preservation is indeed a seminal factor in the RS efficiency. However, the classical recommendation algorithms might induce privacy leakage and the main reason is the centralization of the RS [105]. In fact, the AI model performs the user's recommendation by transferring the data to a central server. Particularly, the training and testing process of the AI model is executed centrally in a third-party framework. Thus, any fraudulent behavior within this third- party is able to create a major privacy violation [103].

The integration of BT-AI manages to preserve the privacy of the users [102] and personalize its content by introducing a pulling-based model that provides related content in a decentralized network and preserve simultaneously the user's privacy. Unlike the classic recommendation systems, the related content to a user is introduced to them automatically within their personal device; the AI model is learning to link related content to each user without transferring the user's data to any external server. To assist this approach, the use of federated learning within a blockchain network might lead to a robust privacy preserving RS; since the training,

analysis and transfer of the data will be done in a secure, collaborative and distributed manner. Particularly, federated learning supports the decentralized architecture of the blockchain networks; the training of the model is performed in each user device avoiding the risk of data disclosure, thereafter the trained model of each user is aggregated to the central server in which the model is updated.

Having stated that, the BT-AI perception will benefit decentralized networks by increasing user security and avoiding any potential privacy leakage. Although it's not yet well exploited due to some engineering challenges (update of each user when needed) which also might lead to scalability challenges in big scale networks, the integration of BT-AI can certainly lead to secure and efficient solutions boosting the performance of recommendation systems.

- **Research trend 2: BT-AI: data-oriented perspective**

The blockchain is an active factor to the development of the AI playing field. According to the contribution in [90], the concept of decentralized AI based BT has emerged to encourage independent developers and autonomous designers; they can practice expense free responsibility for licensed innovation, get remuneration for their work at a market cost fitting their personal preference, keep up with information sway and protection. From another perspective, the adoption of both technologies, Artificial Intelligence and Blockchain, can give a rise to accurate datasets representing distributed ledgers traffic.

To the best of our knowledge, there is a huge lack of datasets especially those designed for anomaly detection; we need labeled, accurate and representative datasets that contain real transaction flow inside. The AI models can then be easily implemented, trained, and evaluated to detect anomalies in decentralized network scenario [91][106]. Moreover, most of the available datasets represent the behavior of permissionless blockchains such as bitcoin and Ethereum, even so, most available datasets don't provide specific insights on the distributed networks and hosting systems, also they don't represent the transaction flow within consortium or private blockchain networks.

Conceptualizing new datasets of real-life transactions is an intriguing research approach to consider. Otherwise, feature engineering can always be performed on existing datasets in order to have the adaptivity with the real data flow within distributed networks. In fact, the features can be adequate to the blockchain systems characteristics (block size, consensus protocol, time stamps, nodes dispatch …). The availability of representative blockchain datasets will enable a deeper understanding of the structure and function of distributed networks. By that, ensuring the blockchain security, privacy and cyber resilience in smart environments using AI will be less complicated. Furthermore, creating accurate and representative datasets won't be a research issue, but rather a powerful motivator to build AI models fitting in decentralized systems. Due to the complexity and interoperability issues surrounding BT-AI integration, this conception is not well discussed, requiring a thorough understanding of how AI is adopted in distributed networks.

- **Research trend 3: Online model conception for cyber resilience**

According to [107], the contribution of blockchain in enhancing cyber resilience can be viewed from multiple perspectives such as quality management, reduction in illegal counterfeiting and reduction in the need for counterparties. Due to the rapid evolution of cybersecurity research, experts are trying to remain up to speed on new attacks that are launched on a daily basis and to devise effective mitigation strategies. Furthermore, artificial intelligence is rapidly evolving to serve the field of cyber security and cyber resilience; AI provides the researchers with a large plethora of techniques enabling the security of distributed systems [109]. However, classic anomalies detection engines are usually based on supervised learning methods which consume time during the training and testing of the model before the detection and make the network more complex. Since different types of cyber-attacks emerge on a daily basis, the trained model can be often outdated and might prone to fault alerts. Thus, such approaches are not practical nor optimized.

For that matter, we believe it is critical to emphasize the importance of an online learning model that can learn in a highly dynamic environment and detect unseen patterns of malicious traffic before affecting the network, thus promoting its resilience. It is stated in [92] that the blockchain based decentralized AI gave rise to new resilient strategies that provide persistent traceability and authenticity records. The online anomaly detection technique used in [93] is based on semi supervised learning methods to detect hidden threats by analyzing valid patterns within Bitcoin traffic data. Thus, the adaptivity of an online learning AI model will surely enhance the cyber resilience of BT systems. Further, the framework of [94] proves that using online learning models inside distributed networks allows all users (nodes) to participate in the training, update and evaluation of the model.

This research path will assist the design of a performant anomaly detection model fitting perfectly in highly dynamic environments.

Moreover, the BT enabled online learning model can be used to generate data for training offline models or providing descriptive analysis of the attack data by blockchain researchers, which complete the previous trend (datasets generation).

Although it has not yet been fully exploited owing to the lack of data and the interoperability issues between blockchain networks and smart environments, the integration of BT-AI must surely achieve cyber resilience within smart ecosystems.

V. Conclusion

Blockchain technology has invaded the industry sector in past years since it provides a unique approach for storing and transmitting data in a traceable and secure manner. In fact, the blockchain plays an active role in securing users' data and maintaining network members' anonymity. However, blockchain presents some security concerns namely DoS, eclipse, and double spending attacks.

For existing challenges to be overcome, advanced anomaly detection and mitigation techniques, more precisely those utilizing AI algorithms, are essential. This paper addressed the incorporation of blockchain technology and artificial intelligence which the main purpose is to provide a secure reliable, efficient blockchain network for smart environments. In this paper we narrowed our research to study how AI can assist blockchain networks; in terms of security improvement and privacy preserving in blockchain based smart environments.

We started by detailing the taxonomy of both technologies AI and BT, we introduced its architecture, protocols and functionalities as well as its areas of deployment (smarts environments). Our proposed framework presented the blockchain security challenges that are categorized based on the attacker's intention namely financial gain, de-anonymization, and isolation attacks. We next present the capabilities of BT-AI integration, which include transaction classification, anomaly detection, and privacy preservation. As for the BT-AI values, we discussed the improvement of scalability and cyber resilience, as well as the enhancement of security and privacy. Last but not least, we discussed some relevant research trends that might lead to interesting research areas such as the decentralized content provider for privacy preservation, the BT-AI for a data-oriented perspective and the online learning model for cyber resilience. As future work, we will focus on the impact of BC-AI on the cyber-resilience. Expressly, we will investigate the cyber-resilience in smart environments when adopting BC-AI driven solution.

REFERENCES

[1] M. Company, "Blockchain technology in the insurance sector," *FACI'17,*, 2017.
[2] H. S. &. V. R. Yin, "A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning," *IEEE International Conference on Big Data (Big Data)* , pp. (pp. 3690-3699), 2017.
[3] F. M. &. Ž. I. P. Benčić, "Distributed ledger technology: Blockchain compared to directed acyclic graph," *International Conference on Distributed Computing Systems (ICDCS)*, pp. pp. 1569-1570, 2018.
[4] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework. Expert Systems with Applications," pp. 168, 114384, 2021.
[5] M. V. M. P. K. D. F. A. a. M. H. M. S. Ali, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Comm. Survey and Tutorials*, p. pp. 1–1, 2018.
[6] D. P. T. J. S. J. N. &. A. Oyinloye, "Blockchain Consensus: An Overview of Alternative Protocols. Symmetry, 1," pp. 3(8), 1363., 2021.
[7] S. C. R. A. G. S. K. N. C. K. K. R. &. Z. A. Y. Aggarwal, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, pp. 144, 13-48, 2019.
[8] K. Davis, " The urbanization of the human population," *The City Reader*, p. pp. 2–11, 2011.
[9] R. D. P. K. a. K. B. K. Peterson, "A blockchainbased approach to health information exchange networks," 2016.
[10] T. C. K.K. R. L. C. Z. &. H. D. McGhin, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and Computer Applications*, pp. 135, 62-75, 2019.
[11] Y. Y. a. F. Y. Wang, "Towards blockchain-based intelligent transportation systems," Rio de Janeiro, Brazil , 2016.
[12] U. T. S. P. K. K. P. T. S. K. N. &. A. M. Bodkhe, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access,*, pp. 8, 79764- 79800., 2020.
[13] Z. X. S. D. H. N. C. W. C. X. W. J. &. I. M. Zheng, " An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, pp. 105, 475-491, 2020.
[14] S. Muggleton, "Alan Turing and the development of Artificial Intelligence.," *AI communications*, pp. 27(1), 3-10., 2014.
[15] Q. Mamun, "Blockchain technology in the future of healthcare," *Smart Health*, pp. 23, 100223., 2022.
[16] R. Prasad, "Alexa Everywhere: AI for Daily Convenience.," *The TwelfthACM International Conference on Web Search and Data Mining.*, pp. (pp. 3-3), 2019.
[17] H. M. S. D. H. N. I. M. &. W. T. Wang, "Blockchain-based data privacy management with nudge theory in open banking.," *Future Generation Computer Systems*, pp. 110, 812-823, 2020.
[18] T. Z. Y. J. W. &. C. M. Y. Zhang, "Collaborative algorithms that combine AI with IoT towards monitoring and control system," *Future Generation Computer Systems*, pp. 125, 677-686, 2021.
[19] I. Y. P. E. R. S. J. S. F. K. &. G. M. Chen, "Ethical Machine Learning in Healthcare.," *Annual Review of Biomedical Data Science*, p. 4, 2020.
[20] A. L. C. V. J. C. X. W. R. R. &. D. S. Tarca, " Machine learning and its applications to biology.," *PLoS computational biology*, pp. 3(6), e116., 2007.
[21] B. Liu, "New technology application in logistics industry based on machine learning and embedded network.," *Microprocessors and Microsystems,*, pp. 80, 103596, 2021.
[22] P. &. P. T. Gogas, "Machine learning in economics and finance.," *Computational Economics*, pp. 57(1).1-4, 2021.
[23] B. McMahan and D. Ramage, " GOOGLE AI Blog," 6 April 2017. [Online]. Available: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.
[24] S. S. S. Y. Y. T. H. T. Y. R. M. P. .. &. I. S. S. Pouyanfar, "A survey on deep learning: Algorithms, techniques, and applications.," *ACM Computing Surveys (CSUR)*, pp. 51(5), 1-36., 2018.
[25] S. K. M. A. M. R. &. K. G. Dargan, "A survey of deep learning and its applications: a new paradigm to machine learning.," *Archives of Computational Methods in Engineering*, , pp. 1-22., 2019.
[26] J. Xie, " A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," *IEEE Commun. Surv.*, pp. vol. 21, no. 3, pp. 2794–2830, 2019.
[27] P. T'Serclaes, "Blockchain could be the missing link in the renewable energy revolution," *World Economic Forum*, p. vol. 21, 2017.
[28] B. T. M. &. K. Podgorelec, "A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection," *Sensors*, pp. 20(1), 147, 2020.
[29] T. P. a. S. Lee, "Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods.," 21 AprI 2021. [Online]. Available: http://arxiv.org/abs/1611.03941..
[30] F. R. Y. T. H. R. X. J. L. a. Y. L. J. Xie, "A survey on the scalability of blockchain systems," *IEEE Network*, pp. pp. 166-173, 2019.
[31] M. S. a. M. S. L. S. Sankar, "Survey of consensus protocols on blockchain applications," *IEEE ICACCS*, pp. pp. 1-5, 2017.
[32] O. Protocol, "Ocean Protocol: A Decentralized Substrate for AI Data & Services-Technical Whitepaper," *nternational Journal of Aerospace Engineering* , 2018.
[33] P. O. L. Y. Y. O. A. B. A. P. P. .. &. Z. A. Mamoshina, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healt," *Oncotarget,*, pp. 9(5), 5665, 2018.
[34] K. D. G. D. K. I. C. &. P. Rantos, "Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem," *ICETE*, pp. pp. 738-743, 2018.
[35] M. U. R. M. H. &. C. J. Hassan, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions.," *Future Generation Computer Systems*, pp. 97, 512-

529, 2019.
[36] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review*, p. 21260., 2008.
[37] r. Analysis Market, "Blockchain Technology Market Size, Share & Trends Analysis Report By Type, By Component, By Application, By Enterprise Size, By End-use, By Region, And Segment Forecasts," Grand View research, 2021.
[38] E. H. Mayer, " security in bitcoin and ethereum: a research survey," 2016.
[39] K. &. T. D. Sai, "Disincentivizing Double Spend Attacks Across Interoperable Blockchains," in *First IEEE International Conference on Trust Privacy and Security in Intelligent Systems and Applications (TPS-ISA) . IEEE.*, 2019.
[40] G. O. A. E. R. M. G. A. &. Č. S. Karame, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security (TISSEC)*, pp. 1-32., 2015.
[41] X. J. P. C. T. L. X. &. W. Q. Li, "A survey on the security of blockchain systems.," *Future Generation Computer Systems*, pp. 107, 841-853., 2020.
[42] Q. H. D. Z. S. K. M. K. &. K. N. Feng, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, pp. 126, 45-58, 2019.
[43] Y. L. Y. T. J. &. L. J. Yu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Communications*, pp. 25(6), 12-18, 2018.
[44] M. K. E. S. L. C. &. R. S. Conti, "A survey on security and privacy of bitcoin," *IEEE Communications Surveys & Tutorials*, pp. 3416-3452, 2018.
[45] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications policy*, pp. 41(10), 1027- 1038, 2017.
[46] A. R. a. M. J. Ken Christensen, "A new analysis of the false positive rate of a bloom filter.," *Information Processing Letters*, p. 944–949, 2010.
[47] K. H. H. G. A. &. R. J. (. J. Qin, "Applying private information retrieval to lightweight bitcoin clients.," *IEEE Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. pp. 60-72, 2019
.
[48] A. B. a. I. Pustogarov, " Bitcoin over Tor isn't a Good Idea," *IEEE*, p. 122–134., 2015.
[49] H. A. S. M. B. Y. &. E. A. Al Jawaheri, "Deanonymizing tor hidden service users through bitcoin transactions analysis.," *Computers & Security*, p. 89, 2020.
[50] S. More, "A newly-described 'blockchain denial of service' attack could convince miners to stop mining," *The block*, 8 December 2020.
[51] K. Raj, "Packt," 11 April 2019. [Online]. Available: https://hub.packtpub.com/what-can-blockchain-developers-learn- from-eclipse-attacks-in-a-bitcoin-network-koshik-raj/.
[52] E. K. A. Z. A. &. G. S. Heilman, "Eclipse attacks on bitcoin's peer- to-peer network," *Security Symposium ({USENIX} Security 15)*, pp. (pp. 129-144)., 2015.
[53] X. J. P. C. T. L. X. &. W. Q. (. Li, " A survey on the security of blockchain systems.," *Future Generation Computer Systems*, pp. 107, 841-853, 2020.
[54] C. L. G. C. H. G. Y. &. F. A. Ye, "Analysis of security in blockchain: Case study in 51%-attack detecting," *5th International Conference on Dependable Systems and Their Applications (DSA)*, pp. (pp. 15-24). IEEE., 2018.
[55] A. T. A. H. S. M. S. M. K. R. T. &. S. A. H. Begum, "Blockchain attacks analysis and a model to solve double spending attack.," *Begum, A., Tareq, A. H., Sultana, M., Sohel, M. K., Rahman, T., & Sarwar, A. H. International Journal of Machine Learning and Computing*, pp. 10(2), 352-357, 2020.
[56] G. G. B. S. C. Z. X. L. K. W. D. S. &. W. H. Xu, " Am I eclipsed? A smart detector of eclipse attacks for Ethereum.," *Computers & Security,*, pp. 88, 101604., 2020.
[57] D. Guegan, "Public blockchain versus private blockhain.," 2017.
[58] R. &. C. D. L. K. Lai, "Blockchain–from public to private.," *In Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2 Academic Press.*, pp. (pp. 145-177), 2018.
[59] H. S. M. K. K. S. K. Y. &. K. J. Lee, "Recipient-oriented transaction for preventing double spending attacks in private blockchain. In," *15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECO)*, 2018.
[60] M. A. A. A. A. A. H. Y. M. &. M. A. Saad, "RouteChain: Towards blockchain-based secure and efficient BGP routing," *IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE.*, pp. (pp. 210-218), 2019.
[61] S. &. K. N. Aggarwal, Attacks on blockchain, Elseiver, 2021.
[62] Y. Y. F. R. L. X. J. H. &. L. Liu, *IEEE Communications Surveys & Tutorials*, pp. 22(2), 1392-1431, 2020.
[63] H. S. &. V. Yin, "A first estimation of the propotion of cyber criminal entities in the bitcoin ecosystem using supervised learning," *IEEE International Conference on Big Data*, pp. pp. 3690-3699, 2017.
[64] M. B. S. W. L. &. D. P. Jourdan, "A probabilistic model of the bitcoin blockchain," *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.*, pp. (pp. 0-0), 2019.
[65] A. R. C. J. R. &. K. S. S. Dorri, "On the activity privacy of blockchain for IoT," *IEEE 44th Conference on Local Computer Networks (LCN) ,* pp. pp. 258-261, 2019.
[66] H. J. &. H. A. S. Singh, " Prediction of transaction confirmation time in Ethereum blockchain using machine learning," *International Congress on Blockchain and Applications* , pp. pp. 126-133, 2019.
[67] S. Dey, " Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work," *10th computer science and electronic engineering (CEEC)* , pp. pp. 7-10, 2018.
[68] B. T. M. &. K. S. Podgorelec, " A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection.," *Sensors*, pp. 20(1), 147., 2020.
[69] M. J. M. &. C. M. (. D. Salimitari, " Ai-enabled blockchain: An outlier-aware consensus protocol for blockchain-based iot networks," *IEEE Global Communications Conference (GLOBECOM).*, pp. pp. 1- 6, 2019.
[70] M. Z. K. L. J. G. H. &. Z. Z. Li, "Blockchain-based SVM in smart grids," *Pattern Recognition Letters*, pp. 138, 476-482, 2020.
[71] T. &. L. S. Pham, "Anomaly detection in bitcoin network using unsupervised learning methods," *arXiv preprint arXiv*, p. 1611.03941., 2016.
[72] D. R. V. T. I. S. J. J. W. &. I.-Z. Preuveneers, "E Chained anomaly detection models for federated learning: An intrusion detection case study.," *Applied Sciences*, pp. 8(12), 2663, 2018.
[73] B. M. E. R. D. H. S. &. y. A. B. A. McMahan, " Communication- efficient learning of deep networks from decentralized data," *Artificial Intelligence and Statistics* , pp. pp. 1273-1282, 2017.
[74] Z. Wang, " Deep learning-based intrusion detection with adversaries.," *IEEE Access*, pp. 6, 38367-38384., 2018.
[75] V. B. A. &. K. V. Chandola, " Anomaly detection: A survey," *ACM computing surveys (CSUR)*, pp. 41(3), 1-58., 2009.
[76] A. Bogner, "Seeing is understanding: anomaly detection in blockchains with visualized features.," *ACM international conjoint conference on pervasive and ubiquitous computing and proceedings of the 2017 ACM international symposium on wearable computers*, pp. pp. 5-8, 2017.
[77] W. T. E. W. W. Q. W. Y. &. H. J. Meng, "When intrusion detection meets blockchain technology: a review," *IEEE Access*, pp. 6, 10179- 10188, 2018.
[78] M. A. S. Y. H. L. K. C. M. R. &. V. R. Harlev, "Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning," *51st Hawaii International Conference*, 2018.
[79] S. R. S. A. O. T. A. &. Y. B. Singh, " A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology.," *Future Generation Computer Systems*, pp. 129, 380-388, 2022.
[80] H. K. S. H. H. J. Y. &. S. C. Kim, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, pp. 7, 136481-136495, 2019.
[81] P. G. G. P. &. T. R. Kumar, "TP2SF: A Trustworthy Privacy- Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning.," *Journal of Systems Architecture*, pp. 115, 101954., 2021.
[82] D. R. Brendan McMahan, "Google AI blog," 6th April 2017. [Online]. Available: https://ai.googleblog.com/2017/04/federated- learning-collaborative.html.
[83] X. J. J. L. C. L. W. &. L. P. Chen, "Chen, X., Ji, J., Luo, C., Liao, W., & Li, P. (2018, December). When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," *IEEE International Conference on Big Data (Big Data)*, pp. pp. 1178-1187, 2018.

[84] J. W. J. Z. J. L. M. Z. Y. &. L. W. Weng, " Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing.*, 2019.

[85] E. G. R. M. a. A. P. G. Betarte, "Improving web application firewalls through anomaly detection," *17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. pp. 779–784,, 2018.

[86] H. S. &. V. R. Yin, "A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning," *IEEE International Conference on Big Data (Big Data)* , pp. pp. 3690-3699), 2017.

[87] M. Z. K. L. J. G. H. &. Z. Z. Li, " Blockchain-based anomaly detection of electricity consumption in smart grids," *Pattern Recognition Letters*, pp. 138, 476-482, 2020.

[88] M. Y. F. R. T. Y. L. V. C. &. S. M. Liu, "Performance optimization for blockchain-enabled industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, pp. 15(6), 3559-3, 2019.

[89] J. N. M. F. W. W. S. Z. X. K. I. &. C. S. Y. Kim, "Anomaly detection based on traffic monitoring for secure blockchain networking," *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* , pp. pp. 1-9, 2021.

[90] G. A. &. G. B. Montes, "Distributed, decentralized, and democratized artificial intelligence," *Technological Forecasting and Social Change*, pp. 141, 354-358, 2019.

[91] X. J. J. L. C. L. W. &. L. P. Chen, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," *IEEE*, pp. (pp. 1178-1187), 2018.

[92] M. &. G. S. N. G. Mylrea, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," *IEEE Resilience Week (RWS)* , pp. (pp. 18-23). IEEE., 2017.

[93] J. N. M. F. W. W. S. Z. X. K. I. &. C. S. Y. Kim, ". Anomaly detection based on traffic monitoring for secure blockchain networking," *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* , 2021.

[94] D. e. H. B. W. JUSTIN, "Decentralized & Collaborative AI on Blockchain," *EEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA*, pp. p. 14-17, 2019.

[95] Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics*, *11*(4), 630.

[96] Ynag, Q., Zhao, Y., Huang, H., & Zheng, Z. (2022). Fusing Blockchain and AI with Metaverse: A Survey. *arXiv preprint arXiv:2201.03201*.

[97] Kaushik, K., & Dahiya, S. (2022). Scope and Challenges of Blockchain Technology. In *Recent Innovations in Computing* (pp. 461-473). Springer, Singapore.

[98] Gadekallu, T. R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q. V., ... & Liyanage, M. (2022). Blockchain for the Metaverse: A Review. *arXiv preprint arXiv:2203.09738*.

[99] Suhail, S., Malik, S. U. R., Jurdak, R., Hussain, R., Matulevičius, R., & Svetinovic, D. (2022). Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins. *Computers in Industry*, *141*, 103699.

[100] Li, D., Han, D., Weng, T. H., Zheng, Z., Li, H., Liu, H., ... & Li, K. C. (2022). Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. Soft Computing, 26(9), 4423-4440.

[101] Zhijie, S. U. N., Han, D., Li, D., Wang, X., Chang, C. C., & Wu, Z. (2022). A Blockchain-based Secure Storage Scheme for Medical Information.

[102] Shinde, R., Patil, S., Kotecha, K., & Ruikar, K. (2021). Blockchain for securing ai applications and open innovations. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(3), 189.

[103] Lisi, A., De Salve, A., Mori, P., Ricci, L., & Fabrizi, S. (2021). Rewarding reviews with tokens: An Ethereum-based approach. *Future Generation Computer Systems*, *120*, 36-54.

[104] Padhy, S. K., Singh, A. K., & Vetrivelan, P. (2022). Item-Based Collaborative Filtering Blockchain for Secure Movie Recommendation System. In *Futuristic Communication and Network Technologies* (pp. 937-948). Springer, Singapore.

[105] Omar, A. A., Bosri, R., Rahman, M. S., Begum, N., & Bhuiyan, M. Z. A. (2019, November). Towards privacy-preserving recommender system with blockchains. In *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications* (pp. 106-118). Springer, Singapore.

[106] Liang, W., Xiao, L., Zhang, K., Tang, M., He, D., & Li, K. C. (2021). Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. *IEEE Internet of Things Journal*.

[107] Cole, R., Stevenson, M., & Aitken, J. (2019). Blockchain technology: implications for operations and supply chain management. *Supply Chain Management: An International Journal*.

[108] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors*, *18*(8), 2575.

[109] 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.

[110] Srivastava, G., Crichigno, J., & Dhar, S. (2019, May). A light and secure healthcare blockchain for iot medical devices. In *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)* (pp. 1-5). IEEE.

[111] Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet of Things Journal*, *6*(5), 7702-7712.

[112] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Kumar, N., & Hassan, M. M. (2021). A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. *IEEE Transactions on Intelligent Transportation Systems*.

[113] Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*.

[114] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Systematic reviews*, *10*(1), 1-11.

[115] Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2021). Blockchain and artificial intelligence for 5G-enabled internet of things: challenges, opportunities, and solutions. *Transactions on Emerging Telecommunications Technologies*, e4329.

Oumaima FADI

Networks and telecommunications engineer graduated in the National School of Applied Sciences of Marrakech in 2020.She has joined the TIC Lab as a PhD student in 2021 in the UIR (International University of Rabat). Her research interests are blockchain, artificial intelligence, security and privacy of networks.

Karim ZKIK

Assistant Professor in cybersecurity at the Faculty of Computer Science and Logistics of the UIR, and member of the TICLab. He obtained his doctorate in computer science from the Mohammed V University of Rabat in 2018. In 2013, he also obtained his engineer degree in network and telecommunications engineering from the National School of Applied Sciences in Safi. He joined the CERADE Lab in the Angevine Higher School of Computer Science and Production as professor researcher in 2021. His Research interests are: Security of Information Systems; Cloud Computing; Cryptography; Networks and Mobile; Software Defined Networks "SDN"; Data analysis and Machine Learning.

Abdellatif EL GHAZI

Assistant Professor at the School of Energy (ECINE) of the UIR since 2012, and member of the TIC Lab. His research interests are: numerical analysis and optimization, cloud computing, computer security, IoT and artificial intelligence.

Mohammed BOULMALF

Professor at the International University of Rabat, and Dean of Computer Science School, and member of TIClab. He graduated as a telecommunications engineer from INPT (Morocco) in 1987. In January 2011, he joined the Canadian University of Dubai as and Associate Professor of Telecommunications and Quality Assurance Advisor to the VPAA. He joined the UIR in 2011 and was appointed Dean there in February 2013. He is the author / co-author of around a hundred articles in peer- reviewed journals and conferences in the fields of networks and wireless communications, wireless sensor networks, mobile computing, RFID technologies and network security