Towards Trustworthy AI: Blockchain-based Architecture

Vipul Popat
School of Computing
Dublin City university
Galway, Republic of Ireland
vipul.popat2@mail.dcu.ie, 0000-0002-0511-4563

Vishal Padwal
School of Computing
Dublin City university
Dublin, Republic of Ireland
Vishal.padwal2@mail.dcu.ie

Dr. Irina Tal
Faculty of Engineering and Computing
Dublin City university
Dublin, Republic of Ireland
irina.tal@mail.dcu.ie

I. INTRODUCTION

Trustworthy Artificial intelligence (AI) refer to AI systems that are developed, deployed, and used in a manner that is reliable, transparent, and ethical. It addresses AI from a perspective that assures fairness, safety, and respect for fundamental human values such as privacy, dignity, and autonomy. To promote the development and deployment of trustworthy artificial intelligence, the European Union has been actively involved. As part of its efforts to provide recommendations on the ethical and legal framework for artificial intelligence, the European Commission established the High-Level Expert Group on AI (AI HLEG) in 2018.

A white paper by the European Commission in 2020 outlines the EU's approach to developing trustworthy AI. The paper includes several mandatory requirements for transparency, accountability, and human oversight, which propose a regulatory framework for AI.

Furthermore, the EU has developed ethical guidelines for using artificial intelligence. According to the AI HLEG guidelines published in 2019, AI systems should be designed and developed in a transparent, ethical, and trustworthy manner. Human autonomy, harm prevention, and transparency are among the principles incorporated into these contracts.

Blockchain technology can play a key role in enabling Trustworthy AI by providing a secure and transparent platform for storing and managing data and information related to AI systems and their decision-making processes. By their decentralized nature, blockchains can provide an assurance that data used for training and operating AI systems is secure, accurate, and impervious to tampering. Auditing and verifying the data and processes that underlie their decision-making will help enhance trust in AI systems.

Additionally, smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller written directly into code, may also be employed to ensure that AI systems are in accordance with certain ethical and legal norms. A smart contract could, for instance, be used to ensure that AI systems are not used maliciously or to enforce data privacy policies automatically.

Several methods and frameworks have been proposed in recent years to address the growing need for trustworthy AI.

The aim of various AI methods is to guarantee that AI systems are reliable and trustworthy at various stages throughout their lifecycle. In some cases, AI systems are designed in a manner that provides the basis for laying out reliable requirements and expectations. Among the methods used to ensure fairness, diversity, and security of data is data collection, protection, and pre-processing. In some approaches, the modelling phase of the AI system is focused on providing an explanation and an explanation of how the system works. A second method uses auditing and testing techniques to ensure accountability and reliability during an AI system's implementation and oversight phase.

We make two contributions in this paper. This paper aims to provide a comprehensive background, concepts, and need for a trustworthy AI system. Secondly, we review and organize the existing methods and guidelines that ensure the trustworthiness of AI systems.

II. TECHNICAL BACKGROUND

A. Trustworthy AI Overview

As a matter of fact, trustworthy AI refers to the use of AI technologies and applications that are safe, secure, transparent, and ethically aligned with human values and rights. The AI ethics standard incorporates several principles, processes, and methods designed to ensure that AI systems are developed and operated in a responsible manner that protects the well-being of individuals, society, the environment, and ensures accountability and transparency. Data privacy and security, fairness, transparency, and legal compliance are all key aspects of trusted AI. Developing trustworthy AI requires collaboration across multiple domains, including computer science, social science, ethics, and law.

B. Preliminaries and Definitions

Trustworthy AI is not a monolithic concept but rather a polylithic one [28]. There are several interpretations of different terms in this field. The definition and explanation of these terms are therefore essential before we can use them. There are several key definitions of terms relating to AI in this section.

A field of study known as AI is concerned with making machines think. According to Legg and Hutter [28], AI involves the imitation of human behaviour and decision-

making abilities. As a result, AI is the process of training machines to perform tasks requiring intelligence.

Black-box problem: This refers to a system that is opaque, and it is difficult to track its structure, internal workings, and implementation [28]. It is becoming increasingly difficult to comprehend AI systems as they become more complex [28]. As a result, the trustworthiness of the system is reduced since it is difficult to explain the reasoning behind the output system to different users that it interacts with.

Explainable and interpretable AI refers to the development of models that can be explained and interpreted. According to Miller [28], explainable AI refers to the way an explanatory agent applies reasoning to the decision-making process of itself or another agent. The work of [28] defines explainable AI as a set of algorithmic techniques for generating high-performance, transparent models that humans can readily comprehend and trust. Explainability and interpretability are often used interchangeably by researchers [28]. The terms are also used interchangeably in this article.

Reliability: System reliability refers to ensuring that the system performs as it is intended to, that is, within specified limits and without any failures, producing the same outputs for the same inputs consistently.

Fairness: A fair system ensures that there is no discrimination or favouritism toward individuals or groups based on their inherent or acquired characteristics that are irrelevant to the decision-making process [28].

Trust: Trust is a complicated phenomenon [28]. The concept of trust is defined differently in different disciplines. In sociology, trust is considered an attribute of human relationships [28]. In psychology, trust is considered a cognitive attribute [28]. In economics, trust is viewed as a calculative attribute. Trust is associated with integrity and reliability, according to all these definitions. Based on a philosophical definition, the National Institute of Standards and Technology defines trust as "the confidence that one element has in another, that that second element will behave as expected."

Acceptance: User acceptance of an AI system depends on its willingness to be used in service encounters.

Trustworthy AI: Trustworthy AI refers to a framework which ensures that a system can be trusted based on the evidence provided by its stated requirements. By doing so, it ensures that users' and stakeholders' expectations are met in a verifiable manner [28].

C. Need for Trustworthy AI

AI systems have achieved a level of performance that allows them to be widely used in society today. A number of these technologies are already transforming the lives of people [30]. Even though these AI systems have some utility, this does not imply that they are of sufficient quality and can be trusted. A casual attitude toward these systems is inappropriate when dealing with high-stakes applications in which one wrong decision can have life-threatening consequences. There is a possibility that these systems will be brittle and unfair. This example from Marcus and Davis [8] illustrates the importance of trustworthy AI by providing an example of facial recognition software. The use of less reliable facial recognition software can be justified if it is used for auto-tagging social media pictures. Even so, the same tool is unacceptable if a police officer intends to use it to locate suspects in surveillance photographs. The example provided here illustrates how people adopt AI systems only when there are no life-threatening consequences. AI systems should be controlled and governed ethically to benefit high-risk applications while increasing their adoption [31].

D. Framework of Trustworthy AI

Guidelines articulate a framework for achieving Trustworthy AI based on fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (EU Charter), and in relevant international human rights law. [120] Below, we briefly touch upon Trustworthy AI's three components.

- Lawful AI

There is no lawless world in which AI systems operate. The development, deployment, and use of AI systems today is subject to several legally binding rules at European, national, and international levels.

Positive and negative obligations are included in the law. This means that it should be interpreted not only in terms of what cannot be done, but also in terms of what can and should be done. There are certain actions that are prohibited by law, but there are others that are enabled by law. [23] A significant consideration in this regard is that the EU Charter contains articles on the freedom to conduct business as well as the freedom to study the arts and sciences, along with articles that address issues that are more familiar to us when determining whether AI is trustworthy, such as non-discrimination and data protection.

- Ethical AI

It is imperative to recognize that achieving trustworthy AI requires more than just compliance with the law, which is only one of its three components. The laws may not always be up to date with technological developments, may be out of step with ethical norms, or may simply not be appropriate for dealing with certain issues. Consequently, AI systems should also be ethical in order to ensure alignment with ethical norms in order to be trustworthy. [23]

- Robust AI

It is imperative for individuals and society to be assured that AI systems will not cause any unintended harm, even if an ethical purpose is ensured. There should be safeguards in place to ensure that these systems perform safely, securely, and reliably, and no unintended adverse effects should occur as a result. As a result, it is essential to ensure that AI systems are robust. The development of ethical and robust AI is therefore closely related and complements one another. [23]

E. Implementation and realisation of trustworthy AI

It is the responsibility of different stakeholder groups to ensure that the following requirements are met:

- The developers are responsible for implementing and applying the requirements to the design and development process.
- A deployment should ensure that the systems they use as well as the products and services they provide meet the requirements.
- The end-users and the wider society should be informed of these requirements and should be able to request that they be observed. [32]

F. Requirement to make Trustworthy AI

As a foundation for enabling "responsible competitiveness", a trustworthy approach guarantees that everyone affected by AI systems can trust that their design, development, and use is lawful, ethical, and robust. To promote responsible and sustainable AI innovation in Europe, these Guidelines have been developed.

It is their goal to make ethics a core pillar of developing a distinctive approach to AI that benefits, empowers, and protects both the individual human flourishing and the common good. As a result, we believe Europe will be able to establish itself as a global leader in cutting-edge artificial intelligence, worthy of our individual and collective trust. By ensuring trustworthiness, Europeans will be able to fully benefit from AI systems' benefits, secure in the knowledge that safeguards will be in place to protect them from potential risks [30] [31] .

Listed below are several requirements that are not exhaustive. The concept encompasses systemic, individual, as well as societal factors:

- Human agency and oversight: AI systems should support human autonomy and decision-making, together with human oversight and intervention.
- Technical robustness and safety: AI systems must be resilient, reliable, and secure, and their development must be guided by a focus on preventing and minimizing unintended consequences.
- Data privacy and governance: AI systems should be governed appropriately in terms of data privacy and protection, as well as quality, integrity, and access.

- Transparency: AI systems should be transparent in terms of their data, systems, and business models. When humans interact with AI systems, they must be informed of both their capabilities and limitations. There is a need for AI systems to avoid unfair bias and provide accessibility and universal design to ensure diversity, non-discrimination, and fairness. There should be consideration and involvement of stakeholders who may be affected by AI systems.

Fig. 1. Interrelationship of the seven requirements: all are of equal importance, support each other, and should be implemented and evaluated throughout the AI system's lifecycle, Figure from [23]
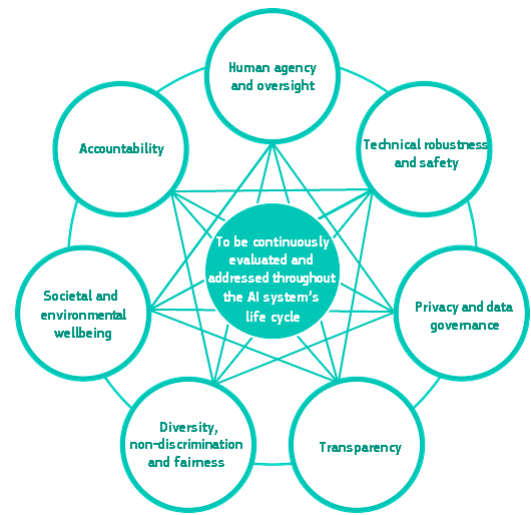
- Social and environmental well-being: AI systems must be environmentally friendly and sustainable, considering the broader community and other sentient beings. It is also necessary to consider the impact on institutions and democracy.
- Accountability: Mechanisms must be implemented to ensure responsibility, accountability, and redress for AI systems and their outcomes. The adverse effects should be identified, assessed, documented, and minimized.[23]

G. Overview of Blockchain

Blockchain is a decentralized digital ledger that enables secure and transparent recording of transactions across multiple computers. Each block of the blockchain contains a record of multiple transactions, and each block is connected to the previous block through cryptography. As the blockchain ledger is decentralized, there is no single point of failure and therefore it is more secure and resilient than centralized systems [21].

Since blockchain technology was developed as the underlying technology for the cryptocurrency Bitcoin, it has been adopted for a wide range of other applications. These

include supply chain management, digital identity, and voting systems [18].

Blockchain technology offers the advantage of maintaining a secure and transparent record of transactions without the need for intermediaries. By utilizing blockchain technology, transactions are made faster, cheaper, and more secure, as well as more transparent and accountable. [19]

Blockchain technology can be classified into three types: public blockchains, private blockchains, and consortium blockchains. A public blockchain can be accessed by anyone, whereas a private blockchain can only be accessed by a select group of participants. In consortium blockchains, a number of organizations collaborate to control the blockchain. They are a hybrid of publicly available and private blockchains.

Overall, blockchain technology is poised to transform a wide variety of industries and has already begun to disrupt traditional business models. In addition, blockchain technology comes with a number of challenges, including scalability, interoperability, and regulatory concerns. [20]

H. Features of blockchain

In order to make blockchain technology unique and valuable for a variety of applications, it has several key characteristics:

- Decentralization: Blockchain is decentralized in the sense that there is no single point of control or central authority. Due to the absence of a single point of failure, the system is more secure and resilient.
- Immutable records: Once a transaction has been recorded on a blockchain, it cannot be altered. As a result, a permanent and unalterable record of transactions is created, which can enhance transparency and accountability.
- Security of transactions: Blockchain technology utilizes cryptography to protect transactions and prevent unauthorized access. As a result, transactions are kept private and secure.
- Transparency: All transactions recorded on the blockchain are visible to all participants, thus making the system transparent. As a result, trust in the system can be enhanced, and fraud and malicious activity may be more easily detected.
- Interoperability: Blockchains are interoperable, which means they can communicate with other systems. By doing so, different blockchain systems are able to exchange data and value.
- Smart contracts: Blockchain technology supports the use of smart contracts, which are self-executing code snippets that enforce a contract's terms. By eliminating intermediaries, agreements can be executed automatically and securely.
- Consensus mechanism: Blockchains use a consensus mechanism in order to ensure that all participants are in agreement with respect to the

ledger's state. The integrity of the system is maintained by preventing disputes.[24][25][26]

A wide variety of use cases can be addressed by blockchain technology, including supply chain management, digital identity, voting systems, and financial services. Blockchain technology is well suited for applications where trust is critical due to its decentralized and secure nature.

III. RELATED WORK

A. Trustworthy AI Frameworks

The principles of trustworthy AI can be enforced through a number of frameworks. The following are some examples:

- A framework for ethical development, deployment, and use of AI developed by the European Commission, based on the seven principles of trustworthy artificial intelligence. [23]
- MIT-IBM Watson AI Lab's AI Accountability framework, which provides a framework for ensuring AI systems are accountable.
- The Partnership on AI's principles for responsible AI, which outline best practices and guidelines for designing, developing, deploying, and using AI responsibly. [31]
- Algorithm Accountability Act, a proposed piece of legislation in the US that would ensure that AI algorithms will be transparent, explainable, and fair [32].

Providing guidelines and standards for ethical AI design and use is the IEEE Global Initiative for Ethical Considerations in AI and Autonomous Systems.

Frameworks such as these can serve as useful tools for individuals and organizations in the development and implementation of trustworthy AI applications. The actual enforcement of these principles is dependent, however, on the laws and regulations in each jurisdiction [27].

Several frameworks are available to assist in implementing the principles of trustworthy artificial intelligence. Here are a few examples:

- The FAIR (Findable, Accessible, Interoperable, Reusable) Guiding Principles for scientific data management and stewardship can be applied to AI systems to ensure responsible data management. [30]
- The International Organization for Standardization (ISO) standards on AI provide guidelines for the ethical and responsible development and use of AI [30].
- The AI Now Institute's AI Policy and Practice Playbook provides a practical guide to organizations

and policymakers seeking to implement ethical and responsible AI practices [1].

- A strategy for responsible development and use of AI is outlined in the Long-Term AI Strategy of the AI Alignment Forum, based on principles of transparency, accountability, and alignment of value.

These frameworks can assist organizations and individuals in ensuring that AI systems are designed and used in a manner that adheres to the principles of trustworthy artificial intelligence. However, it is important to keep in mind that the specific circumstances and context of each case will determine how these frameworks will be implemented.

A substantial amount of work has been accomplished to develop frameworks to support the technical implementation of Trustworthy AI, but these frameworks are very use case specific and do not always encompass all seven principles.

According to [12], critical decisions in complex AI systems need to be made by a consensus of distributed AI and XAI agents or predictors hosted by trusted oracles, with the assumption that the majority of these agents are trustworthy. The blockchain technology can fulfill to a large extent the trustworthiness requirements for AI that are resistant to biases and adversarial attacks. A number of use cases were presented to illustrate how blockchain SCs combined with decentralized storage can be utilized in order to achieve a trustworthy XAI.

In the age of ubiquitous data collection and computing, [17] proposed a framework for developing trustworthy AI systems. A data-centric level of abstraction is provided for ethical questions posed in the context of AI and Data Science. The focus of this framework was the ethics of data and algorithms, and more specifically, those aspects that can be directly integrated into the design and development of AI systems.

It was the goal of [16] to unify the fragmented, currently available approaches to trustworthy AI by considering the entire lifecycle of AI systems, from data acquisition to model development to system development and deployment, and finally to continuous monitoring and governance. The authors provided concrete action items for practitioners and societal stakeholders (e.g., researchers, engineers, and regulators) to improve AI trustworthiness. Furthermore, they identified key opportunities and challenges for the future development of trustworthy AI systems, in which we identified the need for a paradigm shift in the development of comprehensively trustworthy AI systems.

We are already moving towards the 6G era. AI/ML mechanisms will be incorporated into the system as structural components that operate natively. The mechanisms for ensuring trust in these operations become increasingly important as systems become more complex and intelligent.

According to [15], an AI framework is necessary to ensure the input of AI mechanisms is protected, the operation is explainable, and the outputs are reliable.

An architecture for digital manufacturing platforms has been presented by [14] which combines Industry 4.0 paradigms to provide AI-based decision support while maintaining the trustworthiness and human-centricity elements necessary for Industry 5.0. The proposed architecture assists in balancing the perceived benefits associated with AI-centric digitalization while maintaining the role of humans in key decision-making processes. To move from Industry 4.0 to 5.0, they suggested leveraging technologies that target concepts such as human-centricity, sustainability, and resilience.

The study conducted by [13] suggests that trustworthiness is a central requirement for the acceptance and success of AI that is centered around human needs. To determine whether an AI system is trustworthy, it is crucial to assess its behavior and characteristics against a gold standard of so-called trustworthy AI, which may be a set of guidelines, requirements, or simply expectations.

In order for ethical and human-centered AI to succeed, trustworthy AI systems are one of the greatest challenges. There has been an acknowledgement of this fact both in politics [13] and in academia. To implement trustworthiness principles, we advocate the use of methods and technologies from the software engineering field. There has been a long tradition of principled constructionism in software engineering and a great deal of fundamental work has already been completed.

TABLE I : COMPARISON OF TRUSTWORTHY AI FRAMEORK FOR NEGLECTED PRINCIPLES

Framework Reference	Neglected Principles (Full or Partial)
[12]	- Human agency and oversight - Technical robustness and safety - Privacy and data governance - Diversity, non-discrimination and fairness
[17]	- Privacy and data governance - Technical robustness and safety - Diversity, non-discrimination and fairness - Societal and environmental well-being
[16]	- Human agency and oversight - Privacy and data governance - Diversity, non-discrimination and fairness - Societal and environmental well-being
[15]	- Technical robustness and safety - Diversity, non-discrimination and fairness.

B. How could blockchain enable trustworthy AI

Through blockchain technology, trusted AI can be created by providing a decentralized and tamper-proof ledger for storing data and executing smart contracts. In this way, the data used to train AI models is secure, transparent, and immutable, preventing malicious actors from manipulating it and compromising the accuracy of the models. Further, smart contracts on the blockchain can enforce specific rules and conditions for the use and deployment of AI models, creating an additional layer of accountability and trust.

By implementing blockchain technology, anonymous users are able to conduct transactions without the involvement of a third-party intermediary [22].

Big data and standardization can be incorporated into the future scope of blockchain technology. The use of blockchain technology in conjunction with big data allows the creation of a secure cryptographic layer to protect confidential data and copyright forms.

AI is currently gaining popularity and applicability across a wide range of fields due to the proliferation of big data and the increasing computational power. Critical decision-making systems suffer from a major drawback when it comes to the lack of explanations for the decisions made by AI algorithms of today. AI algorithms that provide explanations for their AI decisions are called explainable AI (XAI) [12].

DApp users' technical trustworthiness is a function of consensus, economic models, and incentives for honesty, explainability, and robustness of predictors. A number of additional infrastructure requirements are also necessary, including security, privacy, reliability, usability, dependability, performance, and governance. Blockchain technology appears to be the most suitable option, if not the only one, to meet these requirements. [3] However, several challenges remain to be overcome, including reducing the presence of humans in the loop when validating explanations, and ensuring accurate timeliness for certain applications.

A combination of blockchain technology and trustworthy AI has the potential to bring new levels of security and transparency to a variety of industries. Blockchains can be used to analyze and process data in real-time using AI algorithms, providing valuable insights and reducing the risk of fraud. In addition, the decentralized nature of blockchain ensures that data is not controlled by a single entity. This reduces the risk of data manipulation and enhances overall trust in the system. Thus, blockchain technology and trustworthy AI can be combined to create a secure and transparent ecosystem that benefits individuals and organizations alike.

IV. CONCLUSION

This area of research has been the subject of a significant amount of research, which is described in the related work section. Numerous frameworks have been proposed in different businesses and domains because of research. The frameworks developed until now have not been able to focus on all the principles of trustworthy artificial intelligence. As a result, these frameworks focused on the principles that were relevant for their application in the relevant industry.

Although many AI frameworks have been developed to guide the development and deployment of AI systems. However, there is often a gap between the principles of trustworthy AI and those covered by these frameworks. The ethical principles of fairness and non-discrimination, for instance, may be neglected in some frameworks, while technical principles such as accuracy and reliability may be prioritized. There may be others who focus on societal principles such as environmental sustainability while overlooking technical principles such as robustness and safety. Thus, AI frameworks should take a comprehensive and integrated approach to the principles of trustworthy AI. This will ensure that AI systems are designed and deployed in a transparent, ethical, and beneficial manner.

The development and deployment of AI technologies must be conducted in a trustworthy and responsible manner, as AI has become an increasingly significant component of modern life. Various organizations and governments have developed their own frameworks, but they often focus on a subset of the principles and may not be applicable to all use cases. Moreover, as technology advances and new ethical challenges arise, it is likely that additional principles will need to be considered. This will make it difficult to develop a framework that applies to all situations.

Regulations today increasingly require the interpretation of AI models and the explanation of individual predictions. The technical trustworthiness of a decision is measured by the honesty, the explainability, and the robustness of the predictors used to make the decision.

[34] argues that it is more appropriate to trust the people who wrote the software than the software itself. Nowadays, however, the AI ecosystem has become much more complex with many more stakeholders: the philosopher, the AI researcher, the data scientist, the data provider, the developer, the library author, the hardware manufacturer, the operating system provider, etc. The problem of building trust relationships with and between all stakeholders is practically impossible, let alone determining liability when things go wrong. Therefore, we define trustworthiness on a technical level in our scope.

In addition to decentralization, determinism, immutability, and data integrity, blockchain technology is also resilient against a variety of security attacks aimed at AI agents and their data. The use of AI may also be orchestrated around centralized computing and data storage infrastructures, and these systems are required to deal with continuously evolving data, resulting in probabilistic and volatile decision-making processes.

Using Blockchain technology, we will propose a framework and architecture that will apply all principles of trustworthy artificial intelligence. Frameworks should address all of the principles to ensure that AI is developed and deployed in a manner that is trustworthy, beneficial, and aligned with society's values and needs

REFERENCES

[1] D. Kaur, S. Uslu, K. J. Rittichier, and A. Durresi, 'Trustworthy Artificial Intelligence: A Review', ACM Computing Surveys, vol. 55, no.2. Association for Computing Machinery, 2023.

[2] S. K. Lo et al., 'Towards Trustworthy AI: Blockchain-based Architecture Design for Accountability and Fairness of Federated Learning Systems', IEEE Internet of Things Journal, 2022.

[3] R. D. Garcia, G. Sankar Ramachandran, R. Jurdak, and J. Ueyama, A Blockchain-based Data Governance with Privacy and Provenance: A case study for e-Prescription. Institute of Electrical and Electronics Engineers Inc., 2022.

[4] YIANNAS FRANK, 'A NEW ERA OF FOOD TRANSPARENCY POWERED BY BLOCKCHAIN', 2019.

[5] M. K. Ahuja et al., 'Opening the Software Engineering Toolbox for the Assessment of Trustworthy AI', 2020.

[6] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, 'A comprehensive survey on blockchain technology', Sustainable Energy Technologies and Assessments, vol. 52, 2022.

[7] Z. Yang, Y. Shi, Y. Zhou, Z. Wang, and K. Yang, 'Trustworthy Federated Learning via Blockchain', IEEE Internet of Things Journal, vol. 10, no. 1, pp. 92–109, 2023.

[8] K. Dey and U. Shekhawat, 'Blockchain for sustainable e-agriculture: Literature review, architecture for data management, and implications', Journal of Cleaner Production, vol. 316, 2021.

[9] S. K. Mangla, Y. Kazancoglu, E. Ekinci, M. Liu, M. Özbiltekin, and M. D. Sezer, 'Using system dynamics to analyze the societal impacts of blockchain technology in milk supply chainsrefer', Transportation Research Part E: Logistics and Transportation Review, vol. 149, 2021.

[10] W. Alshahrani and R. Alshahrani, Assessment of Blockchain technology application in the improvement of pharmaceutical industry. Institute of Electrical and Electronics Engineers Inc., 2021.

[11] R. Tian, L. Kong, X. Min, and Y. Qu, Blockchain for AI: A Disruptive Integration. Institute of Electrical and Electronics Engineers Inc., 2022.

[12] C. Baru, Institute of Electrical and Electronics Engineers, and IEEE Computer Society, 2019 IEEE International Conference on Big Data : proceedings : Dec 9 - Dec 12, 2019, Los Angeles, CA, USA. .

[13] Y. Li, 'Emerging blockchain-based applications and techniques', Service Oriented Computing and Applications, vol. 13, no. 4. Springer, pp. 279–285, Dec-2019.

[14] S. Barmpounakis and P. Demestichas, Framework for Trustworthy AI/ML in B5G/6G. Institute of Electrical and Electronics Engineers Inc., 2022.

[15] U. Wajid, A. Nizamis, and V. Anaya, 'Towards Industry 5.0-A Trustworthy AI Framework for Digital Manufacturing with Humans in Control', 2022.

[16] J. de V. Mohino, J. B. Higuera, J. R. B. Higuera, and J. A. S. Montalvo, 'The application of a new secure software development life cycle (S-SDLC) with agile methodologies', Electronics (Switzerland), vol. 8, no. 11, 2019.

[17] M. D. Wilkinson et al., 'Comment: The FAIR Guiding Principles for scientific data management and stewardship', Scientific Data, vol. 3, 2016.

[18] M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, 'Blockchain for explainable and trustworthy artificial intelligence', Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 10, no. 1, 2020.

[19] M. C. N. Yates JoAnne, 'The International Organization for Standardization (ISO)', 2009.

[20] D. P. Srivasthav, L. P. Maddali, and R. Vigneswaran, Study of Blockchain Forensics and Analytics tools. Institute of Electrical and Electronics Engineers Inc., 2021.

[21] B. Liu, Overview of the Basic Principles of Blockchain. Institute of Electrical and Electronics Engineers Inc., 2021.

[22] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, 'A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities', IEEE Access, vol. 9, pp. 12730–12749, 2021.

[23] High-Level Expert Group on Artificial Intelligence, 'HIGH-LEVEL EXPERT GROUP ON AISET UP BY THE EUROPEAN COMMISSION ETHICS GUIDELINES FOR TRUSTWORTHY AI', 2019

[24] F. Yang, L. Lei, and H. Zhu, Overview of Blockchain and Cloud Service Integration. Institute of Electrical and Electronics Engineers Inc., 2022.

[25] S. Utomo, A. John, A. Rouniyar, H. C. Hsu, and P. A. Hsiung, Federated Trustworthy AI Architecture for Smart Cities. Institute of Electrical and Electronics Engineers Inc., 2022.

[26] S. Ahmadjee, C. Mera-Gómez, R. Bahsoon, and R. Kazman, 'A Study on Blockchain Architecture Design Decisions and Their Security Attacks and Threats', ACM Transactions on Software Engineering and Methodology, vol. 31, no. 2, 2022.

[27] B. Li et al., 'Trustworthy AI: From Principles to Practices', ACM Computing Surveys, vol. 55, no. 9, pp. 1–46, 2023.

[28] R. Xu and J. Joshi, 'Trustworthy and transparent third-party authority', ACM Transactions on Internet Technology, vol. 20, no. 4, Nov. 2020.

[29] D. Murray-Rust, C. Elsden, B. Nissen, E. Tallyn, L. Pschetz, and C. Speed, 'Blockchain and Beyond: Understanding Blockchains Through Prototypes and Public Engagement', ACM Transactions on Computer-Human Interaction, vol. 29, no. 5, 2023.

[30] A. Kumar, T. Braud, S. Tarkoma, and P. Hui, 'Trustworthy AI in the Age of Pervasive Computing and Big Data; Trustworthy AI in the Age of Pervasive Computing and Big Data', 2020.

[31] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, 'Blockchain-Enabled Accountability Mechanism against Information Leakage in Vertical Industry Services', IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1202–1213, 2021.

[32] A. Rustemi, V. Atanasovski, and A. Risteski, Overview of Blockchain Data Storage and Privacy Protection. Institute of Electrical and Electronics Engineers Inc., 2022.

[33] D. Almeida, K. Shmarko, and E. Lomas, 'The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks', AI and Ethics, vol. 2, no. 3, pp. 377–387, 2022.

[34] THOMPSON KEN, 'Reflections on Trusting Trust', 1984.