

Article

Proposal of a Blockchain-Based Data Management System for Decentralized Artificial Intelligence Devices

Keundug Park ¹ and Heung-Youl Youm ^{2,*}¹ AI & Blockchain Research Center, Seoul University of Foreign Studies, Seoul 60745, Republic of Korea; jacepark926@gmail.com² Department of Information Security Engineering, Soonchunhyang University, Asan 31538, Republic of Korea

* Correspondence: hyyoum@sch.ac.kr

Abstract

A decentralized artificial intelligence (DAI) system is a human-oriented artificial intelligence (AI) system, which performs self-learning and shares its knowledge with other DAI systems like humans. A DAI device is an individual device (e.g., a mobile phone, a personal computer, a robot, a car, etc.) running a DAI system. A DAI device acquires validated knowledge data and raw data from a blockchain system as a trust anchor and improves its knowledge level by self-learning using the validated data. A DAI device using the proposed system reduces unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations), but the proposed system also prevents these malicious DAI devices from acquiring the validated data. This paper proposes a new architecture for a blockchain-based data management system for DAI devices, together with the service scenario and data flow, security threats, and security requirements. It also describes the key features and expected effects of the proposed system. This paper discusses the considerations for developing or operating the proposed system and concludes with future works.

Keywords: blockchain; decentralized artificial intelligence; AI device; data management; knowledge sharing; self-learning; human-oriented AI; trust anchor; responsible AI



Academic Editors: Yang-Im Lee and Peter R. J. Trim

Received: 23 June 2025

Revised: 10 August 2025

Accepted: 11 August 2025

Published: 18 August 2025

Citation: Park, K.; Youm, H.-Y. Proposal of a Blockchain-Based Data Management System for Decentralized Artificial Intelligence Devices. *Big Data Cogn. Comput.* **2025**, *9*, 212. <https://doi.org/10.3390/bdcc9080212>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The existing centralized artificial intelligence (AI) system (e.g., ChatGPT [1], Gemini [2], DeepSeek [3], etc.) has been trained by its developer using raw data such as articles, papers, pictures, videos, audio, and documents. The raw data collected by the developer could include personally identifiable information (PII), false and manipulated information, biased information, and IPR (intellectual property rights) infringement information. The raw data have not been disclosed to any third party, nor have they been validated by any third party. The products generated by AI systems are unreliable and can result in deepfakes, fake news, and hallucinations [4].

The development of AI semiconductors (e.g., neural processing unit (NPU) [5], graphic processing unit (GPU) [6], high bandwidth memory (HBM) [7]), agentic AI [8], physical AI [9], and on-device AI [10] technologies are accelerating the realization of a decentralized artificial intelligence (DAI) system. For example, on-device AI can generate products on a mobile device without connecting to an AI server over the internet. A DAI system runs on an individualized device (e.g., a mobile phone, a personal computer, a robot, a car, etc.) and performs operations, including self-learning, knowledge generation, knowledge

exchange, knowledge initialization, knowledge backup, and knowledge recovery. As the DAI system can perform self-learning with data collected from the device, it is redundant for a developer of a DAI system to continuously train the DAI system and incur huge data costs. A DAI device is an individual device running a DAI system.

A DAI device improves its knowledge level by self-learning internal raw data continuously collected and generated by the individualized device, but the DAI device needs more data to improve the speed and depth of the knowledge level. The DAI device can receive knowledge data and raw data from suppliers and perform self-learning with the data to improve its knowledge level. Knowledge data are the result generated by the learning of DAI devices. Raw data may be the creation of producers. DAI devices should use data validated by third parties for their self-learning to generate reliable products. The integrity of the knowledge data and raw data should be maintained during transfer between DAI devices and suppliers.

This paper proposes a blockchain-based data management system for DAI devices. The proposed system prevents tampering with knowledge data and raw data validated by a third party and provides the validated data to DAI devices for lifelong learning. A malicious DAI device that has generated an unreliable product has limited access to the validated data in the proposed system, which prevents the malicious DAI device from improving its knowledge level by self-learning using the validated data. Identity management for DAI devices should include the credentials and lifecycle of DAI devices and should distinguish between malfunctioning and malicious DAI devices. A supplier who has distributed malicious knowledge data or raw data is restricted from distributing their data to DAI devices using the proposed system, so a producer who has generated the malicious knowledge data or raw data could be restricted from providing their data to the supplier.

The contribution of this paper is as follows. This paper proposes a blockchain-based data management system for DAI devices, including a new architecture for the system, security threats, and security requirements. The proposed system provides a solution for the self-learning of DAI devices with data management among consumers (i.e., DAI devices), producers, suppliers, and validators. It decreases data costs for training DAI compared to existing centralized AI and improves the speed and depth of knowledge level of DAI by using reliable data.

This paper is organized into the following sections: Section 1 introduces DAI and its trends. Section 2 describes the related studies, including problems with existing centralized AI. Section 3 proposes a blockchain-based data management system for DAI devices to solve the problem identified in Section 2. Section 4 identifies security threats to the proposed system and specifies the security requirements mitigating the identified security threats. Section 5 describes the key features and expected effects of the proposed system. Section 6 discusses considerations of the policy, technology, service, and standardization aspects for developing or operating the proposed system and concludes the paper.

2. Problems Statement and Related Studies

This section describes the problem with existing centralized AI systems, and it examines other studies related to the problem.

2.1. Problems with Existing Centralized AI Systems

The existing AI systems work on AI servers that have been trained by developers using raw data such as articles, papers, pictures, videos, audio, and documents. AI clients must connect to AI servers over the internet to perform tasks requested by users. AI clients cannot perform self-learning and rely solely on the knowledge of AI servers to perform the

tasks. However, if the AI client does not connect to the AI server due to internet connection failure and/or the AI server failure, the task cannot be performed in time.

The raw data used to train AI servers are not trustworthy. The raw data collected by the developers of the AI servers could contain personally identifiable information, unreliable information, and illegal information. Since the raw data have not been disclosed to any third party, nor have they been validated by any third party, the products generated by AI servers trained with raw data are unreliable, resulting in deepfakes, fake news, and hallucinations.

2.2. Other Approaches for DAI Systems

This paper refers to studies that address the challenges discussed in Section 2.1 and focuses on analyzing other studies to identify similarities between blockchain-based data management systems for DAI device learning.

A systematization of knowledge (SoK) for blockchain-based DAI solutions and a taxonomy for existing DAI protocols based on the model lifecycle were proposed in [11]. This paper included the functionalities of blockchain for DAI and its contribution to enhance the security, transparency, and trustworthiness of AI processes, including whether it provides incentives for contributors to AI data and models.

A blockchain-based DAI dismissed the central orchestrator in federated learning in [12]. This paper included implementation of a prototype for training AI models on the data contributor side. The prototype demonstrated that AI models are trained on the data contributor side and smart contracts provided the specifications for generating AI models.

Ref. [13] provided a systematic literature review of existing studies in the field of DAI that addresses issues such as digital privacy, ownership, and control. This paper focused on identifying the components of DAI solutions and networks.

A blockchain-AI integrated framework (BAII) was proposed in [14], which enables AI to be trained, verified, and applied on a decentralized blockchain in the construction industry. This paper addressed knowledge about the security vulnerabilities of AI in the construction field and the decentralization of AI using blockchain.

Ref. [15] investigated the contributions of decentralized technologies to DAI's self-sovereignty and potential unstopability and the implications of DAI's unstopability for development of governance frameworks. This paper identified intrinsic characteristics of DAI that challenge traditional oversight, including immutability, global reach, and adaptive survival strategies.

Ref. [16] investigated the fundamentals and consequences of DAI for edge devices in Internet of Things (IoT) networks. This paper demonstrated the balance between model performance and data privacy by combining DAI with federated learning.

Ref. [17] investigated the potential and limitations of decentralized architectures that impact users, markets, and civic participants. This paper included the technological and legal developments needed to enable decentralized machine learning systems to realize their liberating potential.

Ref. [18] investigated technical architectures, consensus mechanisms, token utilities, and fundamental business models by providing a comprehensive review of major AI-token projects. This paper provided emerging developments for the next generation of DAI systems, including blockchain-based federated learning, on-chain verification approaches for AI results, and more robust incentive frameworks.

Ref. [19] analyzed the challenges and opportunities of blockchain technology and potential advantages and difficulties of DAI in cybersecurity. This paper focused on the integration of DAI with blockchain technologies and provided a taxonomy of DAI and blockchain technologies for cybersecurity and the use cases of blockchain-based DAI.

A decentralized artificial intelligence model network (DaiMoN) was proposed in [20]. DaiMon improved the accuracy of machine learning models with peer collaboration. This

paper included a system which keeps a decentralized ledger containing records related to model training and accuracy and the location of newly updated models.

An alternative path for the development of AI based on distributed ledger technology (DLT) was proposed in [21], which included a distributed, decentralized, and democratized market for AI. This paper provided a case study where a system used SingularityNET for coordination between AIs.

A decentralized AI-driven recruitment system was proposed in [22]. This paper evaluated the performance of the system by measuring scalability, latency, accuracy, and user trust. The system enhanced user autonomy, security, and privacy.

DAI Guardians were proposed in [23], a framework that integrates lightweight AI models and blockchain technology to transfer privacy control from corporations to users. This paper provided the core of the framework that embeds AI guardians into blockchain nodes to enable real-time, context-aware decision-making about data access.

Ref. [24] reviewed the research issues, conceptual map, and technical opportunities of DAI and edge intelligence. This paper assessed the areas where decentralized AI and edge intelligence can enable and promote metaverse, Web3, smart blockchain, and decentralized science.

Swarm learning (SL) was proposed to avoid data transfer and monopolistic data governance in [25]. This paper demonstrated that AI models with SL outperform locally trained models and perform on par with models trained on a merged dataset.

A blockchain-based DAI training platform was proposed in [26], which is designed to democratize AI development and alignment through incentive mechanisms. The platform creates an environment where participants can contribute models and computing resources, and it rewards the participants based on their contributions.

The framework of decentralized emergency intelligence was proposed in [27], which protects patient privacy using blockchain-based smart contracts and optimizes the accuracy of machine learning models by balancing minority classes with diagnostic datasets. This paper demonstrated the impact of technologies on healthcare efficiency and patient outcomes.

A blockchain-based DAI data-market framework was proposed in [28], which balances economic security with sub-second finality using a layered hybrid consensus algorithm. This paper includes a token-based incentive model that seeks to discover data value and suppress low-quality data by weighting the data volume, data quality, and staking risk.

A DAI-based platform for the authenticity and protection of digital creation was proposed in [29], which ensures the immutability and transparency of digital assets using blockchain and detects the unauthorized use or replication of registered creative works using AI.

A framework for next-generation edge AI systems was proposed in [30]. This paper included a literature review covering privacy-centric DAI, IoT system scalability, and quantum-enhanced optimization methods, and it argued that combining federated learning with quantum technologies can improve the scalability and effectiveness of edge AI.

DAI for privacy protection with confidential computing was proposed in [31], which protects user data and the parameters of AI models using a hardware-based trusted execution environment that provides isolation for processing sensitive data.

A DAI and blockchain framework for smart cities was proposed in [32], which focuses on enhancing data optimization and data integrity. This paper mentions that blockchain keeps a record of the data generated in smart cities, and AI models use the data to predict trends, optimize service delivery, and improve resource allocation.

A comprehensive survey of the integration of blockchain technologies for securing space-air-ground IoT (SAG-IoT) applications was presented in [33]. This paper discussed the architecture and security threats to SAG-IoT systems and focused on blockchain-based solutions for SAG-IoT security.

A secure and auditable private data sharing (SPDS) scheme in a smart grid was proposed in [34]. This paper presented a blockchain-based framework for trustless personal data computation and data usage tracking, using smart contracts to specify detailed data usage policies.

Based on the research and analyses in other studies, the conclusion was that no previous study exists focusing on a blockchain-based data management system for DAI devices. This paper proposes a new architecture for a blockchain-based data management system for DAI devices, identifies potential security threats to the proposed system, and specifies the security requirements mitigating the identified security threats. As the proposed system focused on data management for DAI device learning compared to SingularityNET [21], which facilitates the development and deployment of AI models. Compared to swam learning [25], which enables collaboration between multiple AI models without sharing raw data, the proposed system demonstrates advantages in device-level autonomy by off-chain learning and data traceability by on-chain hash evidence storage.

3. A Blockchain-Based Data Management System for DAI Devices

This section proposes a new architecture for a blockchain-based data management system for DAI devices and provides a service scenario and data flow to understand the roles of entities that comprise the proposed system.

3.1. System Architecture

A blockchain-based data management system for DAI devices includes consumers (i.e., DAI devices), producers, suppliers, validators, and a blockchain system (i.e., a repository for validated data) acting as a trust anchor [35,36]. The blockchain system consists of a single on-chain and multiple off-chains. A DAI device could be a producer. The producer and supplier could be the same entity.

In Figure 1, the role-based entities of the proposed system are described as follows:

- The consumer is a DAI device. The DAI device is an individual device (e.g., a mobile phone, a personal computer, a robot, a car, etc.) running a DAI system which performs operations including self-learning, knowledge generation, knowledge exchange, knowledge initialization, knowledge backup, and knowledge recovery. The DAI device performs self-learning using the raw data collected and generated by itself (i.e., the owned raw data) and using the validated knowledge data and raw data received from the blockchain system. The DAI device performs tasks such as the generation of products (e.g., images, videos, documents, etc.), interpretation and translation, human-machine dialogue, delivery of food and goods, and autonomous driving based on its knowledge. Knowledge data and raw data could be commercially traded between a consumer and a supplier. For example, a consumer could purchase the knowledge data and raw data related to the travel sector from a supplier.
- The producer generates and creates raw data for training DAI devices. If the producer is a DAI device, the producer generates knowledge data by self-learning. The producer provides the supplier with knowledge data and raw data, which could be commercially traded between the producer and the supplier. For example, if a producer and a supplier are not the same entity, the producer's knowledge data and raw data related to the travel sector could be sold to the supplier.
- The supplier collects knowledge data and raw data from the producer, which could be commercially traded between the supplier and the producer. For example, if a supplier and a producer are not the same entity, a supplier could purchase a producer's knowledge data and raw data related to the travel sector. The supplier stores the knowledge data, information for verifying the integrity of the knowledge data, raw data, and information for verifying the integrity of the raw data in the blockchain

system. The supplier removes unreliable knowledge data and raw data from the blockchain system in accordance with the validation results. The knowledge data and raw data could be commercially traded between a supplier and a consumer (i.e., a DAI device). For example, the knowledge data and raw data related to the travel sector could be sold to a consumer.

- The validator validates knowledge data and raw data received from the blockchain system. The validator inspects and analyzes the raw data to determine whether they contain personally identifiable information (PII), false and manipulated information, biased information, and intellectual property rights (IPR) infringement information. The validator tests and evaluates the knowledge data to determine whether they contain knowledge about privacy, bias, violence, addiction, cruelty, sexuality, and gambling. The testing and evaluation involve conducting a questionnaire survey and reviewing the results of the task using a DAI device that has learned the knowledge data to be validated. The validator stores the validation history and results for the knowledge data and raw data in the blockchain system.
- The blockchain system including a single on-chain and multiple off-chains identifies and authenticates the consumers (i.e., DAI devices), the suppliers, and the validators. The blockchain system prevents the DAI devices that have performed unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations) from accessing knowledge data and raw data. The blockchain system prevents the suppliers that have distributed unreliable knowledge data and raw data from storing their data. The on-chain stores information for verifying the integrity of the knowledge data and information for verifying the integrity of the raw data received from the supplier, and it stores the validation results for the knowledge data and the validation results for raw data received from the validator. The history of knowledge data and raw data processing (e.g., uploading, downloading, and removing) is stored in the on-chain. The off-chain stores knowledge data and raw data received from the supplier, and it stores the validation history for the knowledge data and the validation history for raw data received from the validator. The blockchain system keeps the validated knowledge data and raw data as a trust anchor. The type of on-chain should be public, which allows anyone to access the ledger and can comprise permissioned nodes. The on-chain requires consensus mechanisms (e.g., PoW, PoS, DPoS, BFT, PBFT, PoA, etc.) and smart contracts to process the ledger.

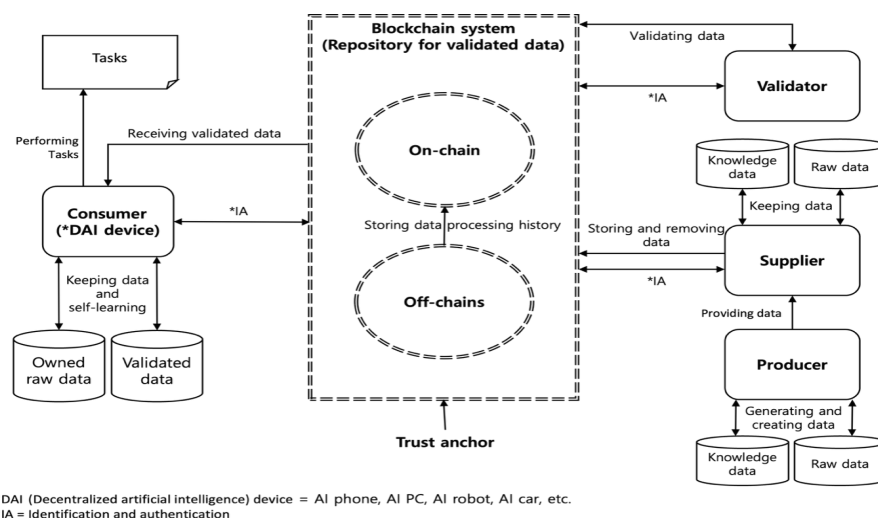


Figure 1. The architecture of a blockchain-based data management system for DAI devices.

3.2. Service Scenario and Data Flow

The service scenario includes knowledge data and raw data management using a blockchain system among consumers (i.e., DAI devices), producers, suppliers, and validators. In Figure 2, the service scenario of data management for DAI devices is described as follows:

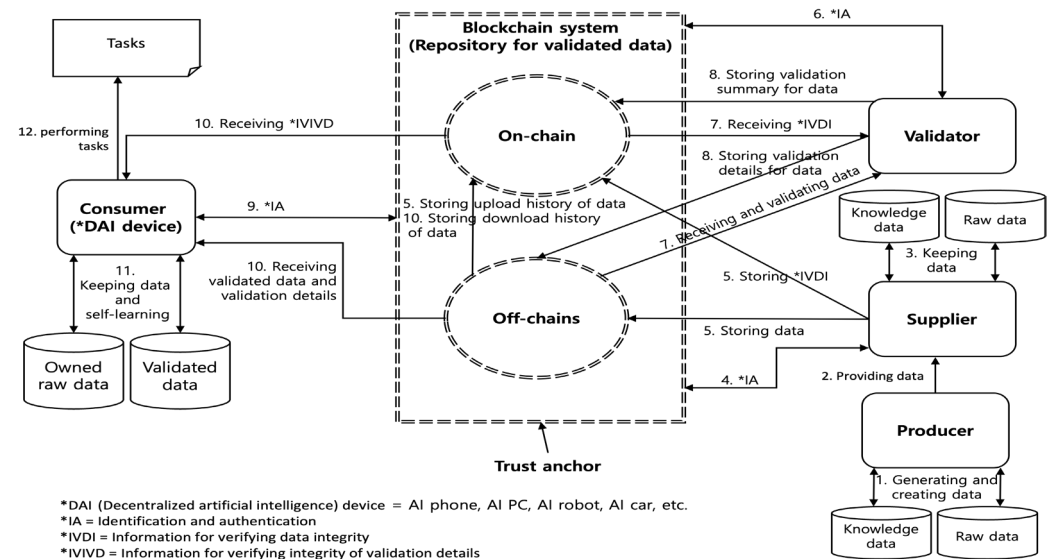


Figure 2. The service scenario of data management for DAI devices.

1. The producer creates raw data. For example, the producer creates pictures, photos, movies, music, papers, and documents on their mobile phones and personal computers. The producer collects data by browsing the internet on their mobile phones and personal computers. The producer collects text message data and voice and video call data on their mobile phones. If the producer is a car or a delivery robot, it collects road data. If the producer is a DAI device, it generates knowledge data on an individualized device (e.g., a mobile phone, a personal computer, a robot, a car, etc.) using self-learning. The producer should remove or de-identify personally identifiable information (PII) within the raw data.
2. The producer provides the supplier with their knowledge data and raw data, which could be commercially traded between the producer and the supplier. For example, if a producer and a supplier are not the same entity, the producer's knowledge data and raw data related to the travel sector could be sold to the supplier. The supplier should encrypt the raw data to prevent the leakage of PII during transmission between the supplier and the producer.
3. The supplier keeps the knowledge data and raw data received from the producer, which could be commercially traded between the supplier and the producer. For example, if a supplier and a producer are not the same entity, a supplier could purchase a producer's knowledge data and raw data related to the travel sector. The supplier should remove or de-identify PII within the raw data.
4. The blockchain system identifies and authenticates the supplier and prevents the supplier that has distributed unreliable knowledge data and raw data from storing their data in accordance with the authentication result.
5. The authorized supplier stores data including their identifier, knowledge data, and raw data in the off-chain and stores information including their identifier, a hash value of the knowledge data, and a hash value of the raw data in the on-chain. The hash value should be generated by secure hash algorithms [37] (e.g., SHA-256, SHA-512, etc.). The off-chain stores the upload history of the knowledge data and raw data,

which includes the identifier of the supplier, the identifier of the knowledge data, and the identifier of the raw data.

6. The blockchain system identifies and authenticates the validator and prevents the unauthorized validator from accessing knowledge data and raw data in the off-chain, in accordance with the authentication result.
7. The authorized validator receives knowledge data and raw data from the off-chain and receives a hash value of the knowledge data and a hash value of the raw data from the on-chain. The validator verifies the integrity of the knowledge data and the raw data using the hash values. If the integrity verification is successful, the validator validates the knowledge data and the raw data. The validator tests and evaluates the knowledge data to determine whether it contains knowledge about privacy, bias, violence, addiction, cruelty, sexuality, and gambling. The testing and evaluation involve conducting a questionnaire survey and reviewing the results of the task using a DAI device that has learned the knowledge data to be validated. The validator inspects and analyzes the raw data to determine whether it contains personally identifiable information (PII), false and manipulated information, biased information, and intellectual property rights (IPR) infringement information. The validator could introduce zero-knowledge proofs or lightweight machine learning (ML) models to automatically detect biased and violent content. The validator generates validation details for the knowledge data and raw data. The validator removes the knowledge data and the raw data after validation is complete.
8. The authorized validator stores data, including their identifier, validation details for knowledge data, and validation details for raw data, in the off-chain and stores information, including their identifier, a hash value of the validation details for the knowledge data, and a hash value of the validation details for the raw data, in the on-chain. The hash value should be generated by secure hash algorithms [37] (e.g., SHA-256, SHA-512, etc.).
9. The blockchain system identifies and authenticates the consumer (i.e., a DAI device) and prevents the DAI device that has performed unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations), from accessing the validated knowledge data and raw data, in accordance with the authentication result.
10. The consumer (i.e., a DAI device) receives the validated knowledge data and raw data from the off-chain and receives hash values of the knowledge data and raw data from the on-chain. The off-chain stores the download history of the validated knowledge data and raw data, which include the identifier of the consumer, the identifier of the validated knowledge data, and the identifier of the validated raw data. The consumer verifies the integrity of the knowledge data and raw data using the hash values. If the integrity verification is successful, the consumer receives validation details for the knowledge data and raw data from the off-chain and receives a hash value of the validation details for the knowledge data and a hash value of the validation details for the raw data from the on-chain. The consumer verifies the integrity of the validation details for the knowledge data and raw data using the hash values. If the integrity verification is successful and the validation result is positive, according to the validation details, the consumer proceeds to the next step.
11. The consumer (i.e., a DAI device) keeps the validated knowledge data and raw data received from the off-chain. The DAI device performs self-learning using the knowledge data and raw data and performs self-learning using the owned raw data. The owned raw data kept in the DAI device represent the data collected and created by the device itself.

12. The consumer (i.e., a DAI device) performs tasks such as the generation of products (e.g., images, videos, documents, etc.), interpretation and translation, human–machine dialogue, delivery of food and goods, and autonomous driving based on their knowledge.

4. Security Threats and Requirements

The potential security threats to the proposed blockchain-based data management system for DAI devices are identified, and the security requirements mitigating the security threats are specified in this section. In Figure 3, entities related to the security threats and requirements of the proposed system are identified.

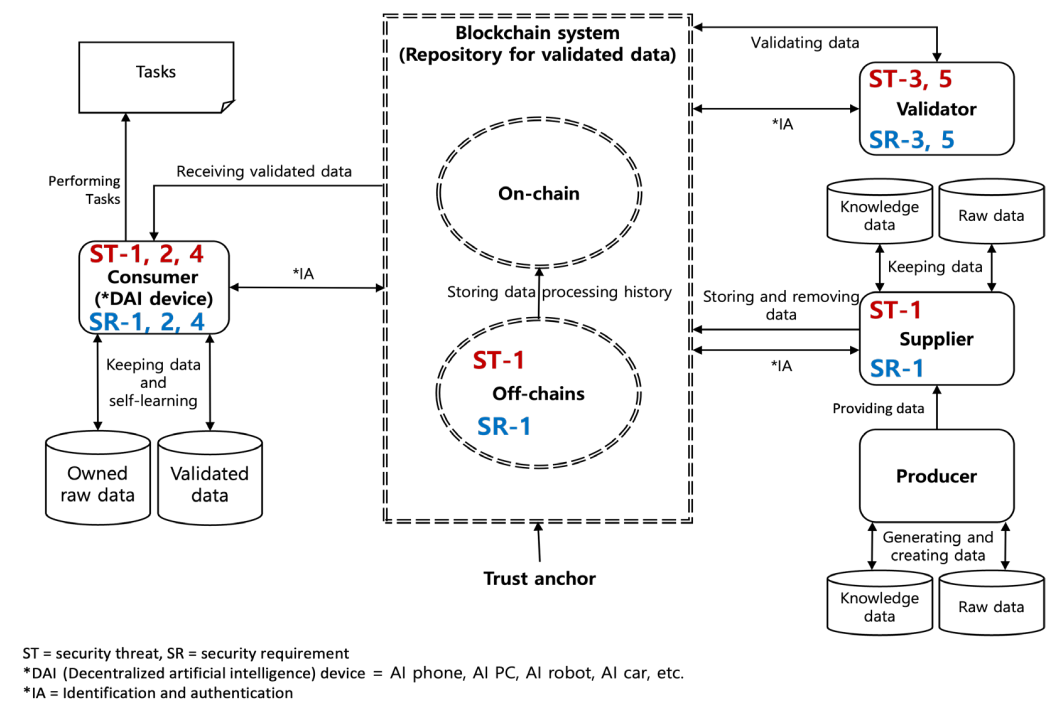


Figure 3. Security threats and requirements of the proposed system.

4.1. Security Threats

The potential security threats (STs) to the proposed blockchain-based data management system for DAI devices are identified as follows:

- Data theft (ST-1): Massive knowledge data and raw data can be stolen from a supplier and a blockchain system and then illegally sold to consumers (i.e., DAI devices). The DAI devices that learned using the stolen and unvalidated knowledge data and raw data from the suppliers can perform unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations). High-quality knowledge data can be stolen from a DAI device and then illegally sold to other consumers.
- Contamination of knowledge data (ST-2): Knowledge data on a DAI device can be contaminated by malware. The DAI device using contaminated knowledge data can malfunction or shut down.
- Abuse of validator authority (ST-3): Collusion between a validator and a supplier can lead to the validator falsely validating knowledge data and raw data on purpose. The falsely validated knowledge data and raw data can be distributed to consumers (i.e., DAI devices) using a blockchain system. The DAI devices that learned using falsely validated knowledge data and raw data can perform unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations).
- Consumer identity theft (ST-4): The identity of a consumer (i.e., a DAI device) can be stolen. A malicious DAI device that has stolen the identity can receive knowledge

data and raw data from a blockchain system and the DAI device that had its identity stolen could pay for the cost of the data.

- Validator identity theft (ST-5): The identity of a validator can be stolen. The malicious entity impersonating the validator can distribute falsely validated knowledge data and raw data to consumers (i.e., DAI devices) using a blockchain system. The DAI devices that learned using falsely validated knowledge data and raw data can perform unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations).

The security threats are specific to the proposed blockchain-based data management system for DAI devices; they are not related to general IT services, including existing AI tools such as chatbots, video generation and editing, image generation, presentations, music generation, voice generation, search engines, etc.

4.2. Security Requirements

The security requirements (SRs) mitigating the security threats identified in Section 4.1 are specified as follows:

- Data encryption (SR-1): Suppliers should encrypt and store knowledge data and raw data using secure encryption algorithms (e.g., AES [38], SEED [38], etc.). Knowledge data and raw data in off-chains should be encrypted and stored using secure encryption algorithms. Consumers (i.e., DAI devices) should encrypt and store knowledge data using secure encryption algorithms. The stolen data that is encrypted cannot be used without decryption. SR-1 mitigates ST-1. Decryption keys for encrypted data in off-chains should be shared with authorized validators and consumers.
- Integrity management for knowledge data (SR-2): The hash value of knowledge data on a DAI device should be generated and stored using secure hash functions (e.g., SHA-256 [39], SHA-512 [39], etc.) to verify the integrity of the knowledge data. The DAI device should use the knowledge data after integrity verification. SR-2 mitigates ST-2.
- Security audit for validators (SR-3): The validation history for knowledge data and raw data should be logged and reviewed regularly (e.g., at least once a month). The validation summary and details for knowledge data and raw data should be reviewed regularly (e.g., at least once a quarter). The auditor should review any problems with the validation procedure and method. In accordance with the audit results, it should prevent malicious validators from accessing the blockchain system that keeps knowledge data and raw data. SR-3 mitigates ST-3. Security audit mechanisms should comply with security regulations or information security management systems (ISMSs) such as the ISO/IEC 27000 series [40–43].
- Identity management for DAI devices (SR-4): Credentials for DAI devices should be issued and managed using a decentralized identity (DID) [44,45]. A DAI device should present its credential to a blockchain system that keeps knowledge data and raw data, and the blockchain system should verify the authenticity of the credential. The DAI device includes a developer, an owner, and an operator. The owner and the operator of the DAI device could be the same entity. A credential for a DAI device should include information about the developer, owners, and operators. The owner and operator of a DAI device could be changed. The credential should include the history of the changes in the owner and operator. The blockchain system should identify the current owner and operator of the DAI device through credential verification. In accordance with the verification results, it should prevent malicious DAI devices from accessing the blockchain system. SR-4 mitigates ST-4.

- Identity management for validators (SR-5): Credentials for validators should be issued and managed using DID. A validator should present their credential to a blockchain system that keeps knowledge data and raw data, and the blockchain system should verify the authenticity of the credential. In accordance with the verification results, it should prevent malicious validators from accessing the blockchain system. SR-5 mitigates ST-5.

5. Key Features and Expected Effects of the Proposed System

Developers and operators of the proposed system can consider the key features and expected effects described in this section.

The key features of the proposed system are as follows:

- Enhancing privacy protection: As DAI devices perform self-learning using internal raw data collected and generated by the individualized devices and using the external knowledge data and raw data validated by third parties, the DAI devices do not share personally identifiable information (PII) with other DAI devices. The validator of the proposed system validates knowledge data and raw data.
- Mitigating bias: As DAI devices improve their knowledge level by self-learning using external knowledge data and raw data validated by third parties, the bias of the DAI devices is mitigated. It supposes that hundreds of millions of DAI mobile phones and DAI PCs (personal computers) around the world exchange their knowledge data and raw data using the proposed system.
- Scalability: As soon as newly released DAI devices are connected to the proposed system, the DAI devices immediately improve their knowledge level by self-learning using the external knowledge data and raw data validated by third parties. As a repository for validated data, blockchain systems facilitate the expansion of nodes across countries or regions.
- Sustainability: As DAI devices continuously perform self-learning using the internal raw data collected and generated by the individualized devices and using the external knowledge data and raw data validated by third parties, the knowledge level of the DAI devices is sustainable leveled upward. On the other hand, as DAI devices that do not use the proposed system perform self-learning using only internal raw data, the knowledge level of the DAI devices declines.

The expected effects of the proposed system are as follows:

- The data costs for training DAI devices could be reduced. As DAI devices could perform self-learning using the internal raw data collected and generated by the individualized devices and using the external knowledge data and raw data validated by third parties, the developers of DAI devices could reduce the data costs for training them. The developers would not need to continuously train DAI devices compared to the existing centralized AI.
- The learning time of DAI devices would be shortened. As DAI devices could perform self-learning using only external knowledge data validated by third parties, DAI devices would not spend time collecting and generating raw data. It is anticipated that the learning time using knowledge data would be shorter than the learning time using raw data.
- The knowledge level of DAI devices could be increased. As DAI devices could perform self-learning using external knowledge data and raw data validated by third parties, the knowledge level of the DAI devices would be higher than that of the existing centralized AI systems. For example, if a DAI device wants to improve its knowledge

level about travel, the device can perform self-learning using external knowledge data and raw data about travel expertise.

- The generation of unreliable products could be reduced. As DAI devices that have generated unreliable products would have limited access to external knowledge data and raw data validated by third parties, this could prevent DAI devices from improving their knowledge level by self-learning using the data. The DAI devices could perform self-learning using only internal raw data, which decreases their knowledge levels. Therefore, even if DAI devices generate unreliable products (e.g., deepfakes, fake news, and hallucinations), the unreliable products will be sloppy and more easily identified.
- Individual raw data could be traded. Raw data collected and generated by individual devices (e.g., mobile phones, personal computers, robots, cars, etc.) could be sold to DAI devices following the validation of the raw data, for example, raw data (e.g., photos, videos, maps, travel records, transportation and accommodation information, etc.) of travel expertise collected and generated by a travel expert's mobile phone. DAI devices could select and purchase raw data for expertise in a specific field.
- Knowledge data of DAI devices could be traded. Knowledge data generated by self-learning performed on a DAI device (e.g., a mobile phone, a personal computer, a robot, a car, etc.) could be sold to other DAI devices following the validation of the knowledge data, for example, knowledge data of travel expertise generated by self-learning performed on a travel expert's DAI device (i.e., a mobile phone). DAI devices could select and purchase knowledge data on expertise in a specific field. Knowledge data could even be exchanged among DAI devices.
- DAI devices could perform lifelong learning without centralized AI servers running on a cloud system. A DAI device could continuously perform self-learning using internal raw data and using external knowledge data and raw data validated by third parties, and it could share its knowledge data with other DAI devices so that DAI devices could improve their knowledge level. This is very similar to the model of human learning.
- The existing centralized AI systems would be decommissioned. High-cost and low-efficiency centralized AI systems would no longer be developed. Developers of centralized AI systems have incurred huge data costs for continuous AI training [46,47]. Operators of centralized AI systems have faced huge costs in increasing AI servers running on cloud systems so that the AI servers can accommodate many AI clients (e.g., AI apps [48] and AI devices [49]). Nevertheless, AI clients cannot perform anything if they cannot connect to the AI servers over the internet. This vulnerability is especially prevalent in the mobility environment.

6. Discussion and Conclusions

DAI devices can improve their knowledge level by self-learning using the internal raw data continuously collected and generated by the individualized devices (e.g., mobile phones, personal computers, robots, cars, etc.), but DAI devices need to improve the speed and depth of knowledge level by using external knowledge data and raw data. The proposed system can provide DAI devices with knowledge data and raw data validated by third parties so that DAI devices improve their knowledge level by self-learning using the knowledge data and raw data on the individualized devices. The proposed system can also restrict the exchange of malicious knowledge data and raw data between DAI devices and suppliers so that DAI devices reduce unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations).

The considerations of policy, technology, service, and standardization aspects for developing or operating the proposed system are as follows:

- Policy aspect: Developers, owners, and operators of DAI devices should consider national or international laws and regulations related to artificial intelligence (AI) [50–54], which should be mandatory to develop secure DAI devices and to securely utilize DAI devices. Developers and operators of the proposed system and developers, owners, and operators of DAI devices should consider the responsible development and use of DAI devices, which can be implemented using international standards on AI management (e.g., ISO/IEC 23894 [55], ISO/IEC 42001 [56], etc.). AI regulators should consider the potential for market monopoly of the proposed system.
- Technology aspect: Developers and operators of the proposed system should consider the identification and authentication of DAI devices, which can be implemented using decentralized identity (DID) [44,45]. Developers and operators of the proposed system should consider the non-repudiation of the behaviors of consumers (i.e., DAI devices), producers, suppliers, and validators, which can be implemented using digital signatures based on the public key infrastructure (PKI) [57,58]. Developers of DAI devices should consider lifelong learning of DAI without degradation in performance, which can be implemented using continual learning [59]. Developers and operators of the proposed system should consider a trust anchor for the validated knowledge data and raw data, which can be implemented using blockchain technology including on-chain and off-chain [60,61].
- Service aspect: Operators of the proposed system should consider the use cases and best practices of DAI devices, which can be key factors in expanding services. The developers and operators of the proposed system should consider the classification and ranking of knowledge data, which can be key factors for building new business models.
- Standardization aspect: Developers of DAI devices and operators of the proposed system should consider the national and international standardization of the architecture and framework, service models, security and privacy, interoperability, use cases, etc., which can be key references to promote the use of DAI devices and the proposed system.

AI watermarking [62] is a cryptographic technique used for accurately identifying AI-generated multimedia content. AI watermarking can be used to detect unreliable products such as deepfake videos and manipulated images. On the other hand, the proposed system can prevent malicious DAI devices from generating unreliable products. Combining the proposed system with AI watermarking can identify and expel unreliable products and malicious generators (i.e., malicious DAI devices).

Future work includes addressing the national and international standardization of the proposed system, studies on the lifecycle management of the credentials for DAI devices and identity management of DAI devices, and studies on validation methodologies for knowledge data and raw data. The proposed system will be developed as an international standard by ISO/TC 307/JWG 4 (security, privacy, and identity for blockchain and DLT). Security and privacy requirements for the proposed system will be developed as a Korean ICT standard by TTA (Telecommunications Technology Association) PG502 (privacy, identity management, and blockchain security). Studies on the lifecycle management of credentials for DAI devices and identity management of DAI devices will enhance the identification and authentication of DAI devices that have performed unreliable tasks, including the generation of unreliable products (e.g., deepfakes, fake news, and hallucinations). Studies on the validation methodologies for knowledge data and raw data will enhance the knowledge level of DAI devices that perform self-learning. Studies comparing the energy efficiency differences in federated learning schemes will quantify the impact of blockchain storage overhead on the resource occupation of DAI devices. Private companies

will be able to implement the proposed system to manage data based on blockchain for the self-learning of DAI devices using technology transfer.

Author Contributions: Conceptualization, K.P.; methodology, K.P.; validation, K.P. and H.-Y.Y.; formal analysis, K.P.; investigation, K.P.; writing—original draft preparation, K.P.; writing—review and editing, K.P. and H.-Y.Y.; supervision, H.-Y.Y.; project administration, H.-Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: This research was implemented as part of the project “Standardization Lab. for Next-generation Cybersecurity” (Project Number: RS-2021-II210112) supported by MSIT (the Ministry of Science and ICT) and IITP (Institute of Information & Communications Technology Planning & Evaluation). This paper was proofread in English by Rachel Choi.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial intelligence
DAI	Decentralized artificial intelligence
DID	Decentralized identity
DLT	Distributed ledger technology
GPU	Graphic processing unit
HBM	High bandwidth memory
IPR	Intellectual property rights
NPU	Neural processing unit
PC	Personal computer
PII	Personally identifiable information
SHA	Secure hash algorithm
SR	Security requirement
ST	Security threat

References

1. ChatGPT. Available online: <https://openai.com/index/chatgpt/> (accessed on 17 June 2025).
2. Gemini. Available online: <https://deepmind.google/models/gemini/> (accessed on 17 June 2025).
3. Deepseek. Available online: <https://www.deepseek.com/en> (accessed on 17 June 2025).
4. Sun, Y.; Sheng, D.; Zhou, Z.; Wu, Y. AI hallucination: Towards a comprehensive classification of distorted information in artificial intelligence-generated content. *Humanit. Soc. Sci. Commun.* **2024**, *11*, 1278. [CrossRef]
5. What is a Neural Processing Unit (NPU)? Available online: <https://www.ibm.com/think/topics/neural-processing-unit> (accessed on 17 June 2025).
6. GPUs for Artificial Intelligence (AI). Available online: <https://www.intel.com/content/www/us/en/learn/gpu-for-ai.html> (accessed on 17 June 2025).
7. Kim, K.; Park, M. Present and Future, Challenges of High Bandwidth Memory (HBM). In Proceedings of the 2024 IEEE International Memory Workshop (IMW), Seoul, Republic of Korea, 12–15 May 2024; pp. 1–4.
8. Acharya, D.B.; Kuppan, K.; Divya, B. Agentic AI: Autonomous Intelligence for Complex Goals—A Comprehensive Survey. *IEEE Access* **2025**, *13*, 18912–18936. [CrossRef]
9. Li, Y.; Duan, Y.; Spulber, A.-B.; Che, H.; Maamar, Z.; Li, Z.; Yang, C.; Lei, Y. Physical Artificial Intelligence: The Concept Expansion of Next-Generation Artificial Intelligence. *arXiv* **2021**. [CrossRef]

10. Wang, X.; Tang, Z.; Guo, J.; Meng, T.; Wang, C.; Wang, T.; Jia, W. Empowering Edge Intelligence: A Comprehensive Survey on On-Device AI Models. *ACM Comput. Surv.* **2025**, *57*, 1–39. [\[CrossRef\]](#)
11. Wang, Z.; Sun, R.; Lui, E.; Shah, V.; Xiong, X.; Sun, J.; Crapis, D.; Knottenbelt, W. SoK: Decentralized AI (DeAI). *arXiv* **2024**. [\[CrossRef\]](#)
12. Masurkar, A.S.; Sun, X.; Dai, J. Using Blockchain for Decentralized Artificial Intelligence with Data Privacy. In Proceedings of the 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 20–22 February 2023; pp. 195–201.
13. Kersic, V.; Turkanovic, M. A Review on Building Blocks of Decentralized Artificial Intelligence. *arXiv* **2024**. [\[CrossRef\]](#)
14. Zheng, C.; Tao, X.; Dong, L.; Zukaib, U.; Tang, J.; Zhou, H.; Cheng, J.C.P.; Cui, X.; Shen, Z. Decentralized artificial intelligence in construction using blockchain. *Autom. Constr.* **2024**, *166*. [\[CrossRef\]](#)
15. Hu, B.A.; Rong, H.; Tay, J. Is Decentralized Artificial Intelligence Governable? Towards Machine Sovereignty and Human Symbiosis. *SSRN* **2025**. [\[CrossRef\]](#)
16. Gouri, M.S.; Nagarajan, M.; Hussain, M.W.; Jayachitra, T.; Jothikumar, R.; Sathya, S. Decentralized AI for Edge Devices with Federated Learning in the Internet of Things. In Proceedings of the 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 14–15 December 2023; pp. 1–5.
17. Shadmy, T.; Ligett, K. Reimagining Decentralized AI. In Proceedings of the CSLAW '24: Symposium on Computer Science and Law, Boston, MA, USA, 12–13 March 2024; pp. 16–23.
18. Mafrur, R. AI-Based Crypto Tokens: The Illusion of Decentralized AI? *IET Blockchain* **2025**, *5*, e70015. [\[CrossRef\]](#)
19. Saleh, A.M.S. Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain Res. Appl.* **2024**, *5*, 100193. [\[CrossRef\]](#)
20. Teerapittayanon, S.; Kung, H.T. DaiMoN: A Decentralized Artificial Intelligence Model Network. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 132–139.
21. Montes, G.A.; Goertzel, B. Distributed, decentralized, and democratized artificial intelligence. *Technol. Forecast. Soc. Change* **2019**, *141*, 354–358. [\[CrossRef\]](#)
22. Hernández-Alvarez, M.; Torres-Hernández, E. Decentralized Systems and AI: Exploring the Intersection of Web3, Blockchain, and Predictive Machine Learning. *Commun. Comput. Inf. Sci.* **2025**, *2529*, 304–311. [\[CrossRef\]](#)
23. Garg, M. Decentralized AI Guardians to Improve Data Privacy and Security for the Users Using Blockchain. *Int. J. Res. Innov. Appl. Sci. (IJRIAS)* **2025**, *10*, 227–238. [\[CrossRef\]](#)
24. Cao, L. Decentralized AI: Edge intelligence and smart blockchain, metaverse, Web3, and DeSci. *IEEE Intell. Syst.* **2022**, *37*, 6–19. [\[CrossRef\]](#)
25. Saldanha, O.L.; Quirke, P.; West, N.P.; James, J.A.; Loughrey, M.B.; Grabsch, H.I.; Salto-Tellez, M.; Alwers, E.; Cifci, D.; Laleh, N.G.; et al. Swarm learning for decentralized artificial intelligence in cancer histopathology. *Nat. Med.* **2022**, *28*, 1232–1239. [\[CrossRef\]](#)
26. Wang, Z.; Sun, R.; Lui, E.; Zhou, T.; Wen, Y.; Sun, J. AIArena: A Blockchain-Based Decentralized AI Training Platform. In Proceedings of the WWW '25: Companion Proceedings of the ACM on Web Conference 2025, Sydney, NSW, Australia, 28 April–2 May 2025; pp. 1375–1379.
27. Ahamed, S.; Khan, M.; Nirjon, I.H. Decentralized AI for Medical Emergency Response Using Blockchain and Computer Vision. *J. Electr. Syst. (JES)* **2024**, *20*, 3479–3490. [\[CrossRef\]](#)
28. Zhang, T. Constructing a Decentralized AI Data Marketplace Enabled by a Blockchain-Based Incentive Mechanism. *J. Ind. Eng. Appl. Sci. (JIEAS)* **2025**, *3*, 42–46. [\[CrossRef\]](#)
29. Kushwaha, M.; Baghwar, J. The Decentralized AI-Powered Platform for Authenticity and Protection of Digital Creation. *Int. J. Res. Publ. Rev. (IJRPR)* **2025**, *6*, 16472–16477.
30. Kiran, S.; Kumar, A.; Chukkala, S. Decentralized AI at the Edge: Federated Learning, Quantum Optimization and IoT Scalability. *Int. J. Sci. Res. Arch.* **2025**, *14*, 256–263. [\[CrossRef\]](#)
31. Lee, D.; Antonio, J.; Khan, H. Privacy-Preserving Decentralized AI with Confidential Computing. *arXiv* **2024**. [\[CrossRef\]](#)
32. Kaha, R. Decentralized AI and Blockchain for Smart Cities: A Framework for Data Integrity and Optimization. *Int. J. Holist. Manag. Perspect. (IJHMP)* **2023**, *4*. Available online: <https://injm.com/index.php/IJHMP/article/view/101> (accessed on 17 June 2025).
33. Wang, Y.; Su, Z.; Ni, J.; Zhang, N.; Shen, X. Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 160–209. [\[CrossRef\]](#)
34. Wang, Y.; Su, Z.; Zhang, N.; Chen, J.; Sun, X.; Ye, Z.; Zhou, Z. SPDS: A Secure and Auditable Private Data Sharing Scheme for Smart Grid Based on Blockchain. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7688–7699. [\[CrossRef\]](#)
35. Shi, P.; Wang, H.; Yang, S.; Chen, C.; Yang, W. Blockchain-based trusted data sharing among trusted stakeholders in IoT. *Softw. Pract. Exp.* **2021**, *51*, 2051–2064. [\[CrossRef\]](#)
36. ISO/TR 23644:2023(en); Blockchain and Distributed Ledger Technologies (DLTs)—Overview of Trust Anchors for DLT-Based Identity Management. International Organization for Standardization: Geneva, Switzerland, 2023. Available online: <https://www.iso.org/obp/ui/es/#iso:std:iso:tr:23644:ed-1:v1:en> (accessed on 20 June 2025).

37. US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF). Available online: <https://datatracker.ietf.org/doc/html/rfc6234> (accessed on 20 June 2025).
38. ISO/IEC 18033-3:2010; Information Technology—Security Techniques—Encryption Algorithms Part 3: Block Ciphers. International Organization for Standardization: Geneva, Switzerland, 2010. Available online: <https://www.iso.org/standard/54531.html> (accessed on 20 June 2025).
39. ISO/IEC 10118-3:2018; IT Security Techniques—Hash-Functions Part 3: Dedicated Hash-Functions. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/standard/67116.html> (accessed on 20 June 2025).
40. ISO/IEC 27000:2018; Information technology — Security techniques — Information security management systems — Overview and vocabulary. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/standard/73906.html> (accessed on 16 August 2025).
41. ISO/IEC 27001:2022; Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: <https://www.iso.org/standard/27001> (accessed on 16 August 2025).
42. ISO/IEC 27002:2022; Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: <https://www.iso.org/standard/75652.html> (accessed on 16 August 2025).
43. ISO/IEC 27005:2022; Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: <https://www.iso.org/standard/80585.html> (accessed on 16 August 2025).
44. Decentralized Identifiers (DIDs) v1.0 Core Architecture, Data Model, and Representations. Available online: <https://www.w3.org/TR/did-core/> (accessed on 20 June 2025).
45. Verifiable Credentials Data Model v2.0. Available online: <https://www.w3.org/TR/vc-data-model-2.0/> (accessed on 20 June 2025).
46. Cottier, B.; Rahman, R.; Fattorini, L.; Maslej, N.; Owen, D. The rising costs of training frontier AI models. *arXiv* **2024**. [CrossRef]
47. The Extreme Cost of Training AI Models. Available online: <https://www.forbes.com/sites/katharinabuchholz/2024/08/23/the-extreme-cost-of-training-ai-models/> (accessed on 20 June 2025).
48. Top 10: AI Applications. Available online: <https://aimagazine.com/top10/top-10-ai-applications> (accessed on 20 June 2025).
49. What We Know About OpenAI's First Consumer Devices. Available online: <https://ia.acs.org.au/article/2025/what-we-know-about-openais-first-consumer-devices.html> (accessed on 20 June 2025).
50. EU AI Act: First Regulation on Artificial Intelligence. Available online: <https://www.europarl.europa.eu/topics/en/article/2023/06/01STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> (accessed on 20 June 2025).
51. Recent U.S. Efforts on AI Policy. Available online: <https://www.cisa.gov/ai/recent-efforts> (accessed on 20 June 2025).
52. Artificial Intelligence 2025 Legislation. Available online: <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation> (accessed on 20 June 2025).
53. A New Chapter in the Age of AI: Basic Act on AI Passed at the National Assembly's Plenary Session. Available online: <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1071&searchOpt=ALL&searchTxt=> (accessed on 20 June 2025).
54. MSIT Announced 'Strategy to Realize Trustworthy Artificial Intelligence'. Available online: <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=509&searchOpt=ALL&searchTxt=> (accessed on 20 June 2025).
55. ISO/IEC 23894:2023; Information Technology—Artificial Intelligence—Guidance on Risk Management. International Organization for Standardization: Geneva, Switzerland, 2023. Available online: <https://www.iso.org/standard/77304.html> (accessed on 20 June 2025).
56. ISO/IEC 42001:2023; Information Technology—Artificial Intelligence—Management System. International Organization for Standardization: Geneva, Switzerland, 2023. Available online: <https://www.iso.org/standard/81230.html> (accessed on 20 June 2025).
57. Albarqi, A.; Alzaid, E.; Alghamdi, F.; Asiri, S.; Kar, J. Public Key Infrastructure: A Survey. *J. Inf. Secur.* **2015**, *6*, 31–37. [CrossRef]
58. ITU-T, X. 509 (10/2019) Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks. Available online: <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509> (accessed on 20 June 2025).
59. Wang, L.; Zhang, X.; Su, H.; Zhu, J. A Comprehensive Survey of Continual Learning: Theory, Method and Application. *arXiv* **2024**. [CrossRef]
60. Thakkar, D.; Sabale, S.; Waghmare, A. Exploring the Efficiency of Off-Chain vs. On-Chain Transactions in Blockchain Network. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2024**, *10*, 40–44. [CrossRef]

61. Onchain vs Offchain. Available online: <https://docs.attest.org/docs/core{-}{-}concepts/onchain-vs-offchain> (accessed on 20 June 2025).
62. AI Watermarking: A Watershed for Multimedia Authenticity. Available online: <https://www.itu.int/hub/2024/05/ai-watermarking-a-watershed-for-multimedia-authenticity/> (accessed on 25 July 2025).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.