Published: 26 February 2026
Online AM: 16 January 2026
Accepted: 08 January 2026
Revised: 02 December 2025
Received: 04 December 2024

SURVEY

Integration of IoT and Distributed Ledger Technologies: A Survey, Challenges, and Future Directions

JUSAK JUSAK, James Cook University, Singapore, Singapore City, Singapore

STEVE KERRISON, James Cook University, Singapore, Singapore City, Singapore

Open Access Support provided by:

James Cook University, Singapore

Integration of IoT and Distributed Ledger Technologies: A Survey, Challenges, and Future Directions

JUSAK JUSAK, School of Science and Technology, James Cook University - Singapore Campus, Singapore, Singapore
STEVE KERRISON, School of Science and Technology, James Cook University - Singapore Campus, Singapore, Singapore

IoT data demands are growing, with Distributed Ledger Technologies (DLTs) offering secure data management, provided they can meet scaling and efficiency requirements that are more restrictive than in conventional application environments. This article comprehensively surveys 27 DLTs of varying paradigms and implementation methods, proposes a scoring method for determining DLT-IoT integration suitability, and then applies that method to the surveyed DLTs. Six DLTs were shortlisted as the most promising, which were then subjected to in-depth analysis around three IoT use cases: health-IoT, e-commerce and automotive manufacturing. We discuss the viability of lightweight DLTs and identify crucial future research directions.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Security and privacy** → *Tamper-proof and tamper-resistant designs*; • **Networks** → **Sensor networks**; **Peer-to-peer networks**; • **Computer systems organization** → **Peer-to-peer architectures;**

Additional Key Words and Phrases: Distributed ledger technology, blockchain, directed acyclic graph, integration, internet of things

ACM Reference Format:
Jusak Jusak and Steve Kerrison. 2026. Integration of IoT and Distributed Ledger Technologies: A Survey, Challenges, and Future Directions. *ACM Comput. Surv.* 58, 9, Article 234 (February 2026), 34 pages. https://doi.org/10.1145/3789255

1 Introduction

We are at the centre of the **Internet of Things** (**IoT**) revolution. A growing number of sensors, actuators, and smart devices are becoming ubiquitous in everyday life. These devices collect huge amounts of data that could completely change businesses, make operations better, and even change the way we see the world around us. According to a Statista Inc. report [127], the number of connected devices worldwide was 19.8 billion in 2025 and forecast to be more than 40.6 billion devices by 2034. Smartphones, televisions, tablets, computers, and other electronic devices are among them. Hence, the necessity for data management solutions that are secure, efficient, interoperable, and scalable is critical as the number of connected and automated devices increases.

Authors' Contact Information: Jusak Jusak (corresponding author), School of Science and Technology, James Cook University—Singapore Campus, Singapore, Singapore; e-mail: jusak.jusak@jcu.edu.au; Steve Kerrison, School of Science and Technology, James Cook University—Singapore Campus, Singapore, Singapore; e-mail: steve.kerrison@jcu.edu.au.

ACM 0360-0300/2026/02-ART234
https://doi.org/10.1145/3789255

Recent investigations show that **Distributed Ledger Technologies** (**DLTs**) have evolved as a way to address numerous challenges in the development of IoT systems [46]. For example, by removing central intermediaries, DLTs facilitate faster and more secure transactions and data transfer, reducing operational costs and points of failure inherent in traditional centralised systems [51, 114]. Some of them are intended to facilitate high transaction throughput and feeless transactions, making them perfect for IoT situations in which devices routinely transmit small amounts of information. DLTs also provide a more robust security framework by distributing data across multiple nodes, making it far more difficult for hostile actors to exploit the system [23, 104]. Despite these profound advantages, the integration of DLTs into IoT environments is challenged by the severe resource constraints of many IoT devices.

In a 2025 survey [6], respondents identified that while IoT has a key role to play in DLT adoption, the IoT sector itself benefits from DLT less than a number of other sectors. At the same time, a majority of the respondents identified DLT (or blockchain) adoption as increasing within their industry. As such, IoT and DLT will likely be increasingly interlinked in the coming years.

This review article critically advances the understanding of existing DLT frameworks and their crucial integration within the IoT landscape. While current literature recognises DLT's potential in IoT, particularly with blockchain, a significant gap persists in documenting the specific lightweight characteristics essential for IoT environments and the attendant integration challenges. This article directly addresses this gap, offering a comprehensive analysis of these emerging technologies and presenting illustrative use cases to guide the development of robust DLT-IoT systems.

Through this rigorous analysis and focused study, we make the following contributions:

- Our survey provides a thorough overview of existing DLT-IoT options, encompassing blockchain, **Directed Acyclic Graphs** (**DAGs**), hybrid blockchain-DAG, logical clock-based, and data storing and sharing technologies. This comprehensive coverage aims to facilitate informed decision-making for researchers and practitioners developing future applications.
- By focusing on DLT integration with IoT systems, we emphasise specific opportunities and challenges presented by this sector. This analysis will promote further research and development for lightweight DLTs and their practical application for secure and efficient IoT systems.
- We introduce a set of criteria for selecting suitable DLT platforms for prospective integration into the IoT ecosystem.
- We also introduce a weighted scoring technique to identify the most suitable lightweight DLT platforms for IoT settings. To the best of our knowledge, this is the first study to employ these specific criteria and weighting metrics to select DLT platforms for IoT integration.
- Three use cases, health-IoT, e-commerce and car manufacturing, are then used to study the architectural considerations for DLT integration and performance compatibility, based on the data collected from surveyed sources.
- Finally, we highlight the future developments in lightweight DLTs, aiming contribute to the applicability of DLTs in secure and trustworthy IoT ecosystems, ultimately benefiting communities, application providers, and the entire IoT ecosystem.

The remaining sections of the article are organised in the following sequence: Section 2 outlines previous studies and current challenges facing IoT deployments. In Section 3, we provide a comprehensive overview of DLTs and investigate potential architectural frameworks for DLT integration into IoT environments. Section 4 explores taxonomy of various DLT platforms and presents a curated selection of appropriate lightweight DLT models utilising a weighted scoring methodology. Section 5 takes the top ranked DLTs from the previous section and evaluates them against three case studies to establish a foundational comprehension of potential integration.

We examine the future trajectory of factors that will promote the usability of lightweight DLT platforms in conjunction with IoT systems in Section 6. Finally, conclusions are presented in Section 7.

2 Comparison with Previous Studies

This study commences with a comprehensive review of existing survey articles on the integration of DLTs into IoT systems, specifically encompassing blockchain, DAG, and hybrid DLT schemes. Particular emphasis is placed on identifying and analysing lightweight DLT solutions, crucial for accommodating the inherent resource limitations of IoT devices. Various survey articles were obtained from several prominent databases covering publications from 2018 to 2025 with the following search terms (keywords) on the title and abstract:

—"blockchain", "iot" and "integration",
—"directed acyclic graph" and "iot" and "integration",
—"distributed ledger technology" and "integration",
—"distributed ledger technology" and "lightweight",
—"distributed ledger technology" and "lightweight" and "integration".

Table 1 summarises these existing reviews, outlining various aspects of DLT systems in collation with IoT system development, and their key features. We also highlight the distinct contributions and novel focus of the present study in comparison.

In Table 1 it is evident that the predominant focus of contemporary research surveys in this area focus on the various blockchain architectures and platforms, with a limited number of studies addressing the integration of the lightweight platforms into IoT systems. Blockchain technology, through their prevalent use in cryptocurrencies, has led to them being adopted in other areas such as supply chain, smart city, healthcare, internet of vehicles, and so on. Conversely, DAG architectures have more recently progressed from a mathematical model to practice. For example, one of the pioneers in this area is Tangle, developed in 2015 [9, 103]. Given the potential development in this area, researchers are progressively investigating lightweight models of DLTs as a more appropriate solution for resource-constrained IoT environments [84, 129, 144].

3 Distributed Ledger Technologies (DLT)

This section explores key aspects of DLT, including their core features and common architectural patterns for DLT-IoT integration. We'll examine the two dominant DLT models—blockchain-based and DAG-based systems—which form the foundation for most existing DLT frameworks, alongside the challenges and techniques involved in IoT integration. While both blockchain and DAG models process transactions, this section will also cover decentralised storage frameworks such as the **InterPlanetary File System** (**IPFS**) and Holochain.

3.1 Main Features of DLTs

DLTs serve as a foundation for secure, decentralised, synchronised, and transparent record-keeping [36, 67, 134]. Unlike traditional centralised systems, a DLT distributes data over a network of digital devices like computers, mobile phones, IoT embedded devices, thereby reducing the need for a singular authority to control and validate data. As a result, this decentralised system offers numerous advantages, establishing DLT as one of the most prominent technologies in a wide range of businesses.

Decentralised implementation offers several benefits for IoT, including:

— Enhanced security: DLTs offer tamper-proof record-keeping. Data stored on the ledger is replicated across the network, making it nearly impossible to change or manipulate without

Table 1. Current Survey Papers on DLT and their Coverage

Paper	Block-chain	DAG	Light-weight	IoT	Main Features and Contributions
[110]	✓	✘	✘	✓✓	Review on various issues in the applications of blockchain-IoT
[130]	✓	✘	✘	✓✓	Survey on current blockchain technology in IoT applications
[24]	✓	✓	✘	✘	Explores graph-based DLTs, limited to Tangle and Hashgraph
[40]	✓✓	✘	✘	✓✓	Survey on blockchain-IoT integration and architecture
[7]	✓✓	✓	✘	✓✓	Survey on a variety of integration schemes and security
[147]	✘	✘	✘	✓✓	Review on various applications of DLTs to the IoT system
[80]	✓✓	✘	✘	✓✓	Overview on various architectures of blockchain-IoT systems
[21]	✓✓	✘	✘	✓✓	Blockchain models for IoT systems
[126]	✓✓	✘	✘	✓✓	A literature review to capture BC-IoT integration emphasising on 10 archetypes of BC-IoT systems
[50]	✓	✓	✘	✘	Comprehensive review on blockchain for healthcare
[12]	✓✓	✓	✘	✘	Blockchain-based classification in terms of protocol and network, scalability, and interoperability
[111]	✓✓	✘	✘	✓	IoT-Blockchain architecture on the dew computing
[94]	✓✓	✘	✘	✓✓	Key implementation challenges and technical choices for Blockchain and IoT integration
[9]	✓✓	✓	✓	✓	Comparison on blockchain and IOTA performance and security
[143]	✓✓	✘	✘	✓✓	Explores integration challenges and alternative solutions
[10]	✓✓	✘	✘	✓✓	Explores existing integration, security, and privacy challenges
[118]	✓✓	✓	✓✓	✘	Definition on the concept of lightweight blockchain
[73]	✓✓	✘	✘	✓	A Comprehensive review on blockchain-IoT for Smart cities
[1]	✓✓	✘	✘	✓	Proposes a blockchain taxonomy for IoT applications
[44]	✓✓	✘	✘	✓	Integration of blockchain and IoT networks in Industry 4.0
[90]	✓✓	✘	✘	✓	Utilisation blockchain for various IoT applications
[52]	✓✓	✘	✘	✓	Combining IoT, AI, edge cloud, fog cloud, and blockchain
[5]	✓✓	✘	✘	✓	A blockchain framework for Electronics Health Record (EHR)
[109]	✓✓	✓	✘	✓	Scalability issues in the IoT and blockchain
[128]	✘	✓✓	✘	✘	Evaluation of the DAG-based systems through the lenses of structure, consensus, property, security, and performance
[64]	✓✓	✘	✘	✓✓	Evaluation on the application of blockchain model and IoT in the healthcare industry
[91]	✓✓	✘	✓✓	✘	Identification of lightweight blockchains based on their architecture, consensus algorithm, cryptography model, device authentication, and storage method
[75]	✓✓	✘	✘	✓✓	Blockchain-IoT aspects including scalability, energy use, security, regulatory compliance, and integration complexity
[112]	✓	✓	✘	✓	Survey on DLT features, cloud computing integration, and hybrid architecture for secure and scalable computing
[57]	✓✓	✘	✘	✓✓	Benefits, drawbacks, and opportunities in blockchain-IoT
Self	✓✓	✓✓	✓✓	✓✓	Explore various DLT platforms and potential architectural frameworks for DLTs-IoT integration, introduce the weighted scoring method for appropriate selection of lightweight DLTs, and assess the selected DLTs against real use cases.

✓: limited coverage; ✓✓: comprehensive coverage; ✘: no coverage.

informing all participants. This intrinsic immutability bolsters the security of IoT ecosystems, reducing the danger of cyberattacks and data breaches [78].

— Transparency and traceability: Every network participant can see each individual transaction or event that is stored in the DLTs and hence, it can be traced easily to foster transparency and accountability. This empowers stakeholders to track the provenance of data, identify potential issues, and build trust in the overall system [101].

— Improved efficiency: By minimising the centralised intermediaries, DLTs can streamline data exchange and automate administrative tasks within the IoT network. This leads to increased efficiency, reducing operational costs and enabling faster response times [96].
— Enhanced automation: DLTs pave the way for smart contracts, self-executing agreements coded onto the ledger that trigger actions based on predefined conditions. This enables automatic decision-making and autonomous operation within the IoT network, further optimising efficiency and reducing human intervention [137].

A DLT is typically characterised by three primary features: it uses cryptographic primitives, communicates via peer-to-peer networking, and has a consensus process. Each are explained herein.

3.1.1 Cryptographic Primitives. DLTs are heavily reliant on cryptographic primitives to ensure data security and integrity. The backbone consists of asymmetric cryptography with public and secret keys. The recipient uses a private key for the digital signature of transactions to verify ownership and prevent any tampering. These signatures are verified with public keys to ensure authenticity. In the blockchain system, each ledger block contains a hash of the preceding block, creating a chain in which changing any data invalidates subsequent hashes, revealing any efforts to manipulate the record [22, 33, 43, 83].

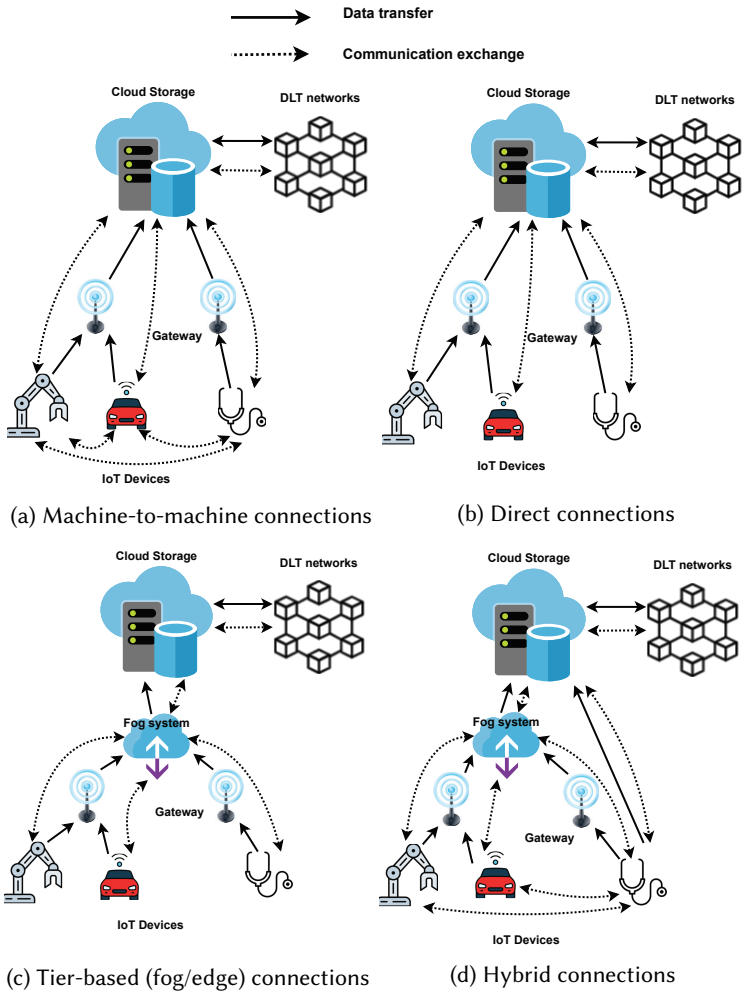
3.1.2 Peer-to-Peer Networking. Aside from the cryptographic primitives, DLT networks rely on **peer-to-peer** (**P2P**) architecture. A complete replica of the ledger is maintained by each network node. New transactions are distributed to the network and independently validated by nodes through the consensus method. This eliminates the necessity for a centralised server, making the system highly resilient to disruptions and tampering.

3.1.3 Consensus Process. A DLT's consensus mechanism is essential for ensuring nodes agree on transaction authenticity and the ledger's state. The primary features of these mechanisms involve balancing security, decentralisation, and resource efficiency. For instance, **Proof-of-Work** (**PoW**) provides high security but is limited by significant energy consumption and scalability constraints [25]. **Proof-of-Stake** (**PoS**) offers improved energy efficiency, though it may introduce centralisation risks if stake becomes overly concentrated. Alternatively, **Practical Byzantine Fault Tolerance** (**PBFT**) focuses on immediate finality and fault tolerance against malicious actors, though its performance often degrades as network size increases due to communication overhead. While these represent widely known examples, numerous other mechanisms exist to optimise the tradeoffs between speed, trust, and resource overhead.

3.2 DLT and IoT System Architecture

Integrating DLT and IoT has attracted significant attention from researchers and practitioners, leading to numerous publications that explore various architectural models [64, 133]. These models, depicted in Figure 1, can be broadly categorised into four types: machine-to-machine connection, direct connection, fog system connection, and hybrid connection. The unique advantages and challenges addressed by each model is discussed below.

3.2.1 Machine-to-Machine (M2M) Connections. This architecture involves IoT devices communicating directly with one another, to share data and perform collaborative tasks. The devices then rely on a gateway or edge device to act as a proxy, connecting them to the DLT network. This model is particularly beneficial for scenarios demanding frequent, real-time interactions among devices, as the gateway minimises network traffic by aggregating data before submission. For instance, this architecture is implemented using the IOTA ledger for health-data sharing, incorporating data from wearable devices and air quality sensors [146].



(a) Machine-to-machine connections

(b) Direct connections

(c) Tier-based (fog/edge) connections

(d) Hybrid connections

Fig. 1. Four models of DLT-IoT integration.

3.2.2 Direct Connections. This architecture simplifies deployment by having each IoT device connect independently to the DLT network via a gateway, with no direct communication between devices. Each device records its own data as separate, immutable transactions. While this guarantees transparency and secure record-keeping, it places a higher demand on the DLT's throughput and increases network traffic due to the volume of individual transactions. Examples of this model are a proof of concept of IoT scenarios utilises Raspberry Pi devices connected to the permissioned network, Hyperledger Fabric [62], applications of DLT on smart cities [147], tracking/tracing on supply chain distribution using IOTA networks [3], and smart farm framework [8].

3.2.3 Tier-Based (fog/edge) Connections. This architecture establishes an intermediary fog/edge layer between resource-constrained IoT devices and the DLT network. Devices send data to the fog/edge layer, which performs initial processing, filtering, and aggregation. This strategy leverages the computational capabilities of the fog/edge to offload heavy workloads from both the DLT network and the IoT devices, significantly minimising latency and improving overall system

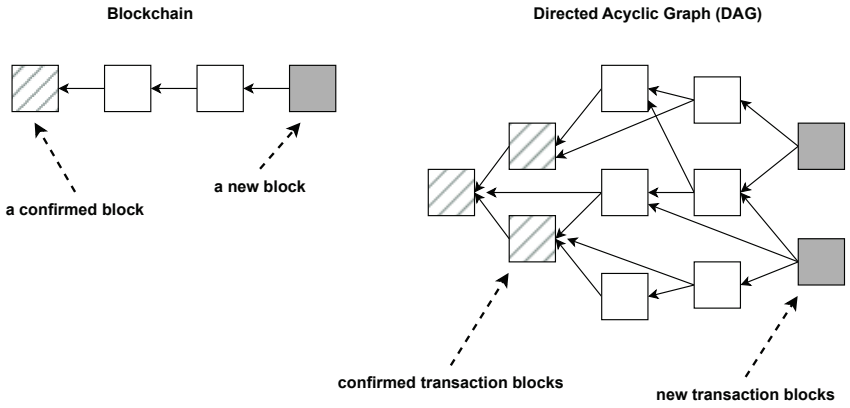


Fig. 2. Blockchain-based and DAG-based DLT blocks structure.

efficiency. This tiered approach is currently the most common model and ideal for applications demanding real-time data processing and decision-making, such as smart cities [73], healthcare monitoring systems [52], and supply chain [13].

3.2.4 Hybrid Connection. This architecture integrates components from the M2M, Direct, and Tier-based models to create a highly versatile and adaptive DLT-IoT framework. IoT devices can interact peer-to-peer, connect directly to the DLT, or utilise the fog/edge layer based on the application's specific requirements. By integrating the strengths of all three designs, the hybrid model delivers a resilient and scalable solution. This makes it ideal for complex ecosystems, such as integrated smart city infrastructures and multi-layered industrial IoT systems, where various devices have distinct connectivity and processing needs [110].

3.3 Blockchain-Based Distributed Ledger

Blockchain's primary goal was initially to leverage on the security and privacy for digital currencies, with Bitcoin serving as the first solution to launch in 2009. The blockchain is an electronic ledger which records transactions and organises them into blocks that are cryptographically interconnected to form an unchangeable chain.

3.3.1 Blockchain-Based Core Structure. The core structure of a blockchain system is fundamentally a decentralised, distributed ledger composed of a continuously growing list of blocks, each cryptographically linked to the previous one as shown in Figure 2. Each block contains a bundle of validated transactions, along with a timestamp, a unique cryptographic hash identifying that block, and crucially, the cryptographic hash of its predecessor block. This chaining of hashes creates an immutable and tamper-resistant record in which any alteration to a past block would change its hash, invalidating all subsequent blocks and immediately being detectable by the network. Multiple copies of this entire chain are maintained and synchronised across numerous independent nodes in a P2P network. Through a consensus mechanism, these nodes collectively agree on the validity of new blocks and the overall state of the ledger, ensuring data integrity, transparency, and resistance to single points of failure [105].

3.3.2 Transaction Validation Process in Blockchain-Based DLTs. Transaction validation in blockchain-based DLTs involves block construction and approval in multiple steps. Initially, a user broadcasts a transaction, which network nodes receive. Before adding the transaction to its

memory pool of unconfirmed transactions, each node checks its syntax, digital signature, nonces, and compliance with predefined consensus rules. The consensus process then selects a node, usually a miner in PoW systems or a validator in PoS systems, to aggregate valid transactions from its pool into a new block. After broadcasting this proposed block to the network, other nodes independently validate its transactions and block (e.g., the PoW solution or validator's stake). The validation process ensures that no double-spending, fraudulent, or unauthorised transactions are added to the ledger, preserving the system's security and trustworthiness. After validation, transactions are grouped into a block, appended to the existing chain, and propagated across the network, ensuring immutability and transparency in a decentralised environment. [105].

3.3.3 Challenges and Techniques for Blockchain-IoT Integration. Blockchain-based DLT's distributed capability could help IoT deployments secure and manage huge networks. However, combining these two technologies is not without challenges. Many IoT devices have resource constraints, which is a major issue. Sensor nodes and wearables have low computational power, memory, and battery life. As a result, traditional blockchain protocols like PoW are too computationally intensive for these low-resource devices. Furthermore, a heterogeneous environment with many sensors, actuators, and intelligent devices has many proprietary communication protocols, operating systems, and processing capabilities, which leads to interoperability issues [12, 17, 90, 143].

Additionally, device heterogeneity is closely linked to security considerations. Systems that are intrinsically heterogeneous can result in vulnerabilities due to varying encryption algorithms and security measures employed by different manufacturers [30, 74]. Taking advantages of these device differences, attackers may exploit weaker links in the chain to destabilise the entire system [138]. Finally, scalability continues to be a significant issue when integrating blockchain into large-scale IoT deployments. Existing public blockchains, with their limited transaction processing capacity, are inadequate for managing the vast data produced by millions of networked devices [69]. While some limitations have significant challenges for blockchain-IoT integration, several promising techniques listed in Table 2 have sought to address these issues.

3.4 DAG-Based Distributed Ledger

DAG-based distributed ledgers offer an alternative architecture to traditional blockchains for recording transactions. Unlike blockchains that rely on a linear or totally-ordered chain of blocks, DAGs utilise a causal-ordered structure. In this structure, transactions are no longer confined to blocks; instead, they exist as nodes within the graph, referencing previous transactions they depend on Ref. [39]. This approach allows for parallel validation, meaning multiple transactions can be verified simultaneously, potentially leading to significant speed improvements.

3.4.1 DAG-Based Core Structure. A DAG-based DLT uses a directed acyclic graph structure. This graph consists of nodes and directed edges as shown in Figure 2. Each node indicates a transaction that holds the transaction data. Directed edges connect nodes within the DAG, indicating a dependency. A new transaction references one or more previous transactions that it validates (parent transactions). This creates a web-like structure where transactions rely on each other for validation, eliminating the need for miners and complex block validation processes [101].

Numerous variations of a DAG-based DLT system are currently available. One is IOTA Tangle, the forerunner of DAG networks we use here as an example. A node in the IOTA Tangle is a network participant that issues, validates, and stores transactions within the ledger. Its core elements include a local ledger copy, a tip pool of unconfirmed transactions, a validator module that selects and approves two previous transactions, and a network communication layer for interacting with other nodes. Nodes also manage consensus processes based on cumulative weight

Table 2. Emerging Techniques for Blockchain-IoT Integration

Techniques	Main Purpose	Relevance to IoT	Examples
Federated Learning [26, 34, 132, 142]	Decentralised AI model training with privacy	No raw data exchange, blockchain secures updates	In an Internet of Vehicles (IoV) network, it enables vehicles to locally train traffic prediction and autonomous driving models while securely recording and verifying model updates without sharing sensor or location data [106].
Sharding [86, 109]	Parallelised by dividing the ledger	Improves scalability, reduces individual load	In smart cities setting, different sectors (transport, utilities, public safety) can be assigned different shards [12].
Sidechaining / Subchaining [116]	Offload to parallel blockchains	Faster, customisable transactions for IoT	In a large supply chain network, a sidechain can be dedicated to managing transactions for a specific product category, while the main chain deals with overall tracking and settlement [75].
Lightweight Consensus [118]	Reduce computational and energy costs	Fast, secure transactions on constrained devices	Proof of Authority (PoA), Delegated PoS (DPoS), Practical Byzantine Fault Tolerance (PBFT)
Off-chain / Layer-2 Solutions [55]	Move transactions off main chain	High-frequency, low-cost IoT interactions	Lightning Network for Bitcoin or the Plasma framework for Ethereum [112].
Edge / Fog Computing [14]	Pre-process IoT data before blockchain upload	Low latency, efficient data filtering	Integrating blockchain and edge computing (IBEC) and Clustered Edge Intelligence (CEI), enhancing resource usage and security [42, 135].
Blockchain Interoperability Protocols [75]	Enable cross-chain IoT data exchange	Integrate various blockchains in a single IoT network	Inter-blockchain communication (IBC) that enables secure and trustless exchange of data between diverse blockchains [109].

and tip selection algorithms, with optional services such as permanodes for long-term data storage. This structure enables scalable, feeless, and decentralised transactions handling ideal for IoT networks [128].

IOTA's consensus mechanism uses tip selection, where an incoming new message must approve two unconfirmed messages, known as tips, before it can be attached to the Tangle. This process ensures the network's growth and validation without traditional miners. In IOTA 2.0, consensus is further strengthened by transaction validators, which are nodes that participate in a leaderless binary voting protocol to confirm the validity of transactions and maintain the integrity of the Tangle. These validators are rewarded with Mana, which is a reputation and resource token that helps with congestion control and anti-spam measures. Nodes also manage a local view of the ledger, contributing to the security and efficiency of the Tangle [3, 9].

3.4.2 Comparison between Blockchain-Based and DAG-Based Architectures. Compared with blockchain networks, DAG-based ledgers offer a lightweight and efficient solution for IoT systems compared with traditional blockchain frameworks [99, 131]. Unlike blockchains, DAGs do not require centralised mining or the addition of a specific block to the chain. Instead, transactions are confirmed via a distributed consensus mechanism, allowing for faster transaction processing and higher scalability. DAGs enable real-time data processing and decision-making with faster transaction confirmation and increased throughput, which makes them ideal for resource-constrained IoT devices. These benefits make DAG-based ledgers a potential technology for scalable and efficient IoT applications. These key differences are summarised in Table 3.

3.4.3 Transaction Validation Process in DAG-Based DLTs. Validation begins when a user submits a transaction, and at this phase, the user initiates a transaction on the network. Based on this request, the transaction information is collected into a node. This node contains transaction data (e.g., sender, receiver, amount), timestamps (which record the transaction's creation and validation

Table 3. Key Architectural Differences between Blockchain and DAG-Based DLT

Features	Blockchain	DAG-based DLT
Structure	Linear or totally-ordered chain	Causal-ordered
Transaction validation	Sequential (one block at a time)	Parallel (multiple concurrent transactions)
Dependency	Each block references previous block	Each transaction references parent transactions
Computational load to reach consensus	Heavier	Lighter
Consensus mechanisms	Proof-of-Work, Practical Byzantine Fault Tolerance, Proof-of-Stake	Tangle, Hashgraph

timestamps), references (parent pointers that link the new node to one or more previously validated parent transactions), and digital signature, which ensures authenticity by signing the node with the transaction's cryptographic key [131]. For example, in IOTA framework, before being attached to the Tangle, the new message actively participates in validating the network by performing a tip selection algorithm, often a Weighted Random Walk, to identify and approve two unconfirmed tips as its direct predecessors, thereby linking itself to the existing graph. Once these references are established and local checks are passed, the new message is propagated across the peer-to-peer network via a gossip protocol. As it spreads, other nodes independently validate its content and, by subsequently attaching their own new messages that also reference it, they collectively contribute to its growing approval weight, leading to its eventual confirmation, with conflicts swiftly resolved through **Fast Probabilistic Consensus** (**FPC**) among transaction validators.

3.4.4 Challenges and Techniques for DAG-IoT Integration. DAG-based DLTs, while promising for IoT due to their scalability and feeless nature, face significant integration challenges. These include the inherent resource constraints of most IoT devices, making direct participation difficult. Mainly, the complexity of achieving robust and fast consensus within a vast, often intermittently connected network, resulting a significant challenge to manage the enormous volume and variety of data generated by IoT devices. Despite security and privacy, other challenges are similar to blockchain-IoT integration to overcome the lack of interoperability and standardisation across the fragmented IoT ecosystem. Table 4 outlines available techniques for addressing DAG-IoT integration issues.

3.5 Specialised Solutions

A smaller number of specialised solutions exist to address particular needs or overcome certain limitations in more widely used methods. They may combine elements from the previous DLT models, or introduce new approaches that can sit alongside them.

3.5.1 Hybrid Blockchain-DAG. Hybrid DLTs like blockDAGs [108], including Spectre and Phantasma's "Phantasm" protocol, combine elements of blockchains and DAG to enhance scalability. Their principal work as DLTs is to enable significantly higher transaction throughput by moving away from a linear, single-chain structure. Transaction validation occurs through blocks referencing multiple previous blocks, forming a graph rather than a sequential chain. This allows for parallel block creation. In Spectre, validation involves a recursive voting mechanism among blocks to resolve conflicts and establish a probabilistic ordering [117]. Phantasma, conversely, employs a blockDAG with two-level colouring and stability thresholds to achieve a more deterministic and stable ordering, leveraging the DAG's parallelism for speed while aiming for robust finality [145].

Table 4. Emerging Techniques for DAG-IoT Integration

Techniques	Main Purpose	Relevance to IoT	Examples
Lightweight clients / nodes [65]	Reduce computational and storage impact on devices	Allows low-power, constrained IoT devices to interact with the DLT	IOTA light nodes, simplified client libraries for embedded systems.
Optimised consensus mechanisms [75]	Achieve scalable, robust, and fast network agreement	Essential for high-throughput, real-time IoT applications with many devices	IOTA's Fast Probabilistic Consensus (FPC).
Improved tip selection algorithms [107]	Ensure consistent confirmation times and network health	Critical for reliable and timely data processing, mitigating orphaned transactions in dynamic IoT environments	Advanced algorithms designed for better network throughput and confirmation stability.
Tiered architectures (Fog / Edge)[129]	Process data closer to the source; reduce network load	Lowers latency, improves scalability for massive device deployments by localising processing	Edge gateways running partial DAG nodes, fog computing for localised consensus.
Data stream management (off-chain) [75]	Efficiently handle high-volume, low-value IoT data	Prevents network congestion from continuous small sensor readings	Local data aggregation, state channels, committing only proofs / summaries to the DAG.
Decentralised Identity (DID) [101]	Provide secure, self-sovereign identities and verifiable data	Enhances device authentication and user-centric identities for IoT interactions	IOTA Identity that is built on W3C DID standard.
Lightweight Cryptography [75]	Enable secure operations with minimal overhead	Allows resource-constrained IoT devices to perform essential cryptographic tasks	Efficient hashing algorithms, optimised elliptic curve cryptography.

3.5.2 Tempo (Radix). Radix's original DLT, Tempo, utilised a unique approach to achieve massive scalability. Its core principle involved each network node maintaining a local logical clock, an increasing integer representing observed events. Transaction validation in Tempo was done using a form of lazy consensus and sharding. Unlike global block-based consensus, Tempo validated transactions (i.e., Atoms) on a per-transaction basis. When a node received an Atom, it performed local validation (e.g., signature checks, double-spend prevention) against its own ledger, associating its current logical clock value. In case of conflicts, nodes would gather these temporal proofs from relevant shards to deterministically establish event order. Cryptographic signatures ensured the integrity of these proofs, enabling efficient, sharded transaction processing without relying on a slow, global consensus mechanism [68].

3.5.3 InterPlanetary File System. The IPFS is a decentralised file storing and sharing technology that fundamentally changes how data is accessed and transmitted over the internet [31]. Unlike standard web systems, which use location-based addressing (URLs pointing to specific servers), IPFS uses content addressing. This means that each file is identifiable by a unique cryptographic hash of its contents, known as a **Content Identifier** (**CID**). When a user requests a file, the IPFS network retrieves it from any node where it is stored, rather than a single centralised server. This design makes IPFS highly resistant to censorship, single points of failure and link failure, as the content is available as long as at least one node on the network keeps it.

IPFS organises its data using a **Merkle Directed Acyclic Graph** (**Merkle DAG**). When a file is added to IPFS, it is divided into smaller chunks, and each chunk is cryptographically hashed, yielding a CID [77]. These CIDs then become nodes within the Merkle DAG, with connections between them illustrating hierarchical relationships, such as a directory's CID linking to the CIDs of its contained files and subdirectories. The Merkle DAG structure assures data integrity because

any change to the content of a file or directory results in a different CID, thus creating a new version rather than modifying the original. It also allows for efficient data deduplication because identical files or chunks throughout the network will share the same CID. To maintain data integrity and security, IPFS uses the SHA-256 cryptographic hash by default.

3.5.4 Holochain. Holochain takes a revolutionary approach to distributed computing, distinguishing itself from both blockchain and classic DAG-based systems by emphasising an agent-centric architecture [79]. Instead of a single, global, continuously replicated ledger that all participants must validate, Holochain allows each user or agent to maintain their own separate, cryptographically secure data chain, also known as a source chain. This local chain stores all of an individual's actions and data related to a specific application. Holochain's primary function is to enable distributed applications (hApps) that are highly scalable, efficient, and respect user autonomy, allowing for real-time interactions and data control without the need for centralised servers or a universal consensus method.

Holochain's structure is based on a **distributed hash table** (**DHT**), similar to BitTorrent, and individual source chains resembling a git repository. Each agent's source chain is a hash chain, which ensures that entries are tamper-proof and sequentially sorted by that agent. Public data from these separate source chains is then gossiped to and validated by a random subset of DHT peers. This peer validation assures data integrity throughout the network without needing each node to keep or validate every transaction. This zero-of-N trust model implies that if even one honest peer evaluates a piece of data against the hApp's rules, its integrity can be verified, leading to high scalability as the network's processing capacity grows with more users. Holochain has a unique security model which relies largely on public-key encryption (particularly, dual-key cryptography) to ensure identification, authenticity, and data integrity. A cryptographic hash is often used to create unique data fingerprints and ensure data immutability on the DHT.

3.6 Comparison among DLT Models

While IPFS and Holochain are sometimes grouped together as decentralised technologies, they differ fundamentally from traditional blockchain, DAG-based, hybrid blockchain-DAG, and logical clock-based DLTs. An inherent characteristic of all of these that they are transactional ledgers, designed to keep an immutable, globally ordered, and cryptographically secure record of events and state changes, making them ideal for smart contract execution. Their goal is to achieve a shared, consistent global state among all participants using a consensus procedure.

In contrast, IPFS and Holochain are not designed as global transactional ledgers. The IPFS functions primarily as a decentralised file storage and sharing protocol, using content-addressing to distribute data rather than maintaining a global transaction history through consensus. Similarly, Holochain is an agent-centric distributed application framework where each user maintains a local data chain, relying on peer validation via a DHT rather than a single, universally replicated ledger or a global consensus mechanism for all transactions. Thus, unlike blockchain and DAGs that focus on immutable transactional records, IPFS prioritises decentralised content delivery, while Holochain emphasises individual autonomy and scalable P2P application functionality.

Table 5 shows a comprehensive comparison of blockchain and DAG against IPFS and Holochain distributed ledger systems in various aspects, thereby facilitating a clear understanding of the differences between the DLT models.

4 DLT Platforms with Potential Integration into IoT Systems

To date, a substantial quantity of DLT-based systems have been documented in academic publications or implemented as real-world platforms for distributed applications. Based on the survey

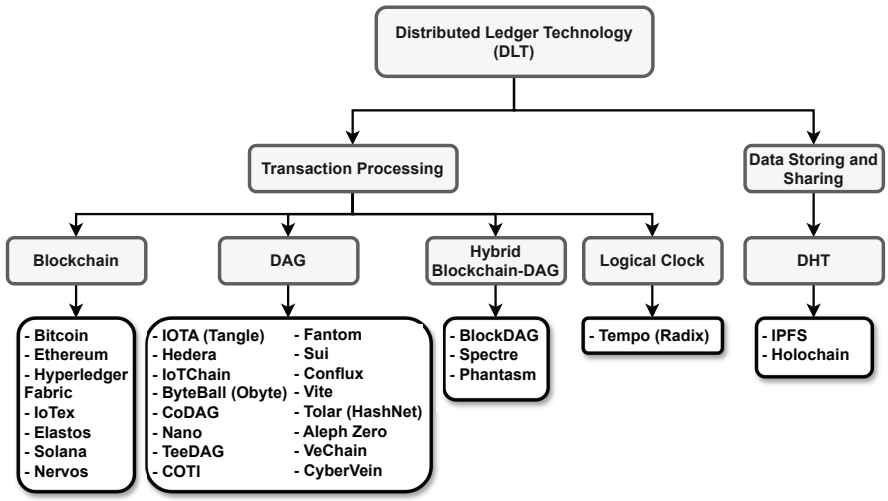


Fig. 3. A taxonomy of DLT appropriate for the IoT context.

Table 5. Comparison between Blockchain/DAG-Based, IPFS, and Holochain Systems

Features	Blockchain / DAG-based	IPFS	Holochain
Primary purpose	Transactional ledgers for value/state transfers	Decentralised file storage and sharing	Agent-centric distributed application framework
Global state	Aim for a single, globally consistent, ordered ledger state	No global transactional state; content-addressing	Local agent chains; no single global ledger
Data Structure	Linear chain of blocks (Blockchain) or interconnected transactions (DAG)	Merkle DAG for file organisation; content-addressed nodes	Agent-specific hash chains; distributed hash table
Consensus Mechanism	Explicit global consensus (PoW, PoS, DAG algorithms)	No transactional consensus; focuses on content integrity	Distributed validation via peer witnessing and DHT
Transaction Immutability	Immutable transactional records on a shared ledger	Content immutability for files; no transactional ledger	Local chain immutability for agents; peer validation on DHT

articles documented in the preceding part, we carefully selected DLT platforms for potential integration into IoT systems. The selection of DLT systems was based on their robust grounding in the literature, as well as their widespread acceptance and practical use in industry. Figure 3 displays a horizontal structural diagram that classifies the current IoT-related DLT platforms into Blockchain-based, DAG-based, hybrid blockchain-DAG-based, logical clock-based, and DHT-based.

The taxonomy of DLTs is mostly determined by the variations in the structure of the DLT platforms. For example, blockchain is a type of DLTs in which data is stored in blocks that are chained together, whereas a DAG is a structure made up of nodes that are connected in such a way that information may only flow from earlier to later nodes, not the other way around. The logical clock-based DLT features a distinct DLT structure, with each node having its own logical clock and transactions being sorted according to their timestamps. Finally, the structures of IPFS and Holochain, both of which use DHT, require special consideration as they inherit different structures. Whereas Blockchain-based, DAG-based, Hybrid Blockchain-DAG-based, and logical clock-based DLTs provide a secure and transparent means for recording transactions,

IPFS and Holochain give a more flexible and efficient approach to storing and sharing data in distributed networks. Additionally, neither IPFS nor Holochain necessitate a global consensus mechanism.

When examining the landscape of DLTs for integration with IoT systems, it is crucial to define the scope of the platforms under consideration. While the term DLT broadly encompasses technologies that share and synchronise digital data across a distributed network, this article focuses specifically on blockchain-based, DAG-based, hybrid-based, and logical clock-based ledgers. Therefore, the IPFS and Holochain systems are intentionally excluded from this analysis. This exclusion is justified because, while both IPFS and Holochain utilise decentralised and distributed principles for data storage and management, they do not operate as traditional transactional ledgers with a sequential block structure in blockchains or a confirmed-by-references DAG structure. Instead, IPFS is primarily a decentralised file storage and sharing protocol, and Holochain is an agent-centric distributed computing framework, both of which serve distinct purposes and rely on different core mechanisms for data integrity and consensus than the transactional DLTs central to this study.

Table 6 presents a comprehensive list of transaction processing DLT platform candidates, encompassing blockchain-based, DAG-based, hybrid blockchain-DAG, and logical clock structures. Each platform is evaluated against six key attributes: throughput in **transactions per second** (**TPS**), **time to finality** (**TTF**) in seconds or milliseconds, consensus mechanism, cryptographic features, and feeless transaction capabilities, along with their existing DLT-IoT integrations. It is important to note that the TPS and TTF values provided for each platform in the tables are approximations rather than precise figures, as these can vary based on specific configurations and network conditions.

We argue that the success of DLT-IoT integration fundamentally depends on aligning the DLT's key attributes and architectural needs. For example, for real-time machine-to-machine connections (Figure 1(a)) or high-volume direct connections (Figure 1(b)), DLTs need to provide high TPS and near-instant TTF, alongside efficient consensus mechanisms and lightweight cryptographic features to accommodate constrained devices. On the other hand, the tiered and hybrid architectures (Figure 1(c) and 1(d)) offer flexibility, with lower-tier components handle local consensus and lighter cryptography, while the core DLT still requires robust TPS, TTF, and security. Feeless transaction capabilities have a substantial impact on the economic sustainability of pervasive IoT deployments across all architectures, removing prohibitive costs of frequent microtransactions. Additionally, proven DLT-IoT integrations provide possible adoption based on the IoT architecture best practices.

While highly relevant, performance attributes incorporating **Artificial Intelligence** (**AI**) into DLT-IoT integration, such as observability, adaptivity quotient, and computational resource equilibrium [45], are not the focus of this survey. These emerging features and their associated metrics are currently in an exploratory development phase, lacking the extensive, formally peer-reviewed literature required for inclusion here.

4.1 Weighted Scoring the Selected Lightweight DLT Platforms

Based on the DLT platforms given in Table 6, we employed a weighted scoring technique to determine the best DLT platforms that embody the lightweight characteristics of the intended DLT frameworks and are most suitable for integration with IoT systems.

First, we define a set of weights, W, for each assessment attribute, a, shown in Table 7, for example the attribute TPS is given a weight of 0.2. We propose that performance metrics (TPS, TTF), feeless transactions and prior work that demonstrates the potential for integration with IoT are a higher priority than the consensus mechanism used or cryptographic features employed.

These attributes are each then scored, utilising a range from 1 to 7 while assigning only odd numbers, based on criteria described in Table 7 to select A_{ad} for a given attribute, a, of a specific

Table 6. Existing DLT platforms as Candidates for Integration with IoT System

DLT Platforms	Through-put (TPS)*	Time to Finality (TTF)*	Consensus Mechanism	Cryptography Features	Fee-less Txn	Existing DLT-IoT Integration
Blockchain-Based						
Bitcoin [19, 93]	7	60 min	Proof of Work (PoW)	ECC (secp256k1) SHA-256	No	No existing studies
Ethereum [71]	15–45	6–7 min	Proof of Stake (PoS)	ECC (secp256k1) Keccak-256	No	Implemented in various IoT systems, e.g. [41, 119]
Hyperledger Fabric [61]	3-20 k	Seconds to min-utes	Varied, i.e., PBFT, Crash Fault Tolerance (CFT), Solo, Kafka and Raft Orderers	ECC (secp256k1) SHA-256	Yes	Implemented in various IoT systems, e.g. [61, 72, 98]
IoTex [122, 123]	2 k	<1 s	Roll-Delegated PoS	ECC (secp256k1) Keccak-256	No	Implemented in several IoT systems, e.g. [100]
IOT-Chain [92]	1024 – 1071	10 s	Verifiable Ran-dom Function (VRF)	Multilevel archi-tecture, Schnorr signatures SHA-256	Yes	Existing stud-ies, e.g. [92]
Elastos [54]	70-80	2 – 10 s	PoW with sidechain	ECC (secp256k1) SHA-256	No	Existing stud-ies, e.g. [2]
Solana [136]	65 k (theo-retical), 3 k (real-world)	10 – 13 s	Proof of History (PoH) and PoS	ECC (Ed25519) SHA-256	No	Existing stud-ies, e.g. [13, 47]
Nervos [120]	1 k	10–13 s	Common Knowledge Base (CKB), PoW	ECC (secp256k1) Blake2b	No	No existing studies
DAG-Based						
IOTA (Tangle) [49]	1.5 k	10–12 s	Tangle weighted random walk (pre Tangle 2.0), Fast Probabilis-tic Consensus (Tangle 2.0)	ECC (Ed25519) Curl-P and SHA-3	Yes	Implemented in various IoT systems, e.g. [3, 48, 115]
Hedera [4, 121]	10 k	3–5 s	Hashgraph: Asynchronous Byzantine Fault Tolerance (BFT)	ECC (Ed25519) SHA-384	No	Implemented in several IoT systems, e.g. [121]
ByteBall (OByte) [37]	Unspec.	Unspec.	Similar to Tan-gle	ECC (secp256k1) SHA-256	No	Existing stud-ies, e.g. [76]
CoDAG [38]	394	Unspec.	PoW	ECC (secp256k1) SHA-256	No	Existing stud-ies, e.g. [32]
Nano [81]	1 k	<1 s	Open Represen-tative Voting (ORV)	ECC (Ed25519) Blake2b	Yes	Existing stud-ies, e.g. [19]

(Continued)

Table 6. Continued

DLT Platforms	Through-put (TPS)*	Time to Finality (TTF)*	Consensus Mechanism	Cryptography Features	Fee-less Txn	Existing DLT-IoT Integration
TeeDAG [88]	750–2.25 k	Unspec.	Trusted Execution Environment (TEE)	ECC (secp256k1) SHA-256	No	New development, existing studies, e.g. [88]
COTI [60]	100 k	1–2 s	Proof-of-Trust (PoT)	ECC SHA-256	No	New development, no existing studies
Fantom [35]	20 k	1–2 s	Asynchronous BFT - Lachesis	ECC SHA-256	No	Existing studies, e.g. [63]
Sui [29]	10.9 k – 297 k	480 ms	Delegated PoS	ECC (Ed25519, Secp256k1, Secp256r1) Blake2b	No	New development, no existing studies
Conflux [82]	3.4 k-6.4 k	23 s	Hybrid PoW and PoS	ECC (secp256k1) SHA-256	No	New development, existing studies, e.g. [59]
Vite [85]	2 k	1 – 2 s	Hierarchical DPoS (HDPoS)	ECC (Ed25519) Blake2b	Yes	No existing studies
Tolar (HashNET) [89]	200 k	1 – 2 s	Improved Redundancy Reduced Gossip	ECC SHA-3	No	No existing studies
Aleph Zero [58]	89 k – 90 k	400 – 500 ms	Asynchronous BFT	Schnorr signatures Blake2b	No	No existing studies
Vechain [53]	165	10 – 20 s	Proof of Authority (PoA)	ECC (secp256k1) Blake2b256, Keccak256	No	Existing studies, e.g. [8, 77, 102]
CyberVein [56]	Unspec.	Unspec.	Hybrid PoW and PoS, Proof of Contribution (PoC)	ECC (secp256k1) SHA-256	No	No existing studies
Blockchain-DAG Hybrid-Based						
BlockDAG [108, 140]	10 k–15 k	3–5 min	PoW	ECC (secp256k1) SHA-256	No	Existing studies, e.g. [139]
Spectre [117]	Unspec.	10 s	BlockDAG, PoW	ECC (secp256k1) SHA-256	No	Existing studies [141]
Phantasm [145]	Unspec.	Unspec.	BlockDAG, adaptive scalable mining	ECC (secp256k1) SHA-256	No	New development, no existing studies
Logical Clock-Based						
Tempo (Radix) [68]	1M (over 1 k nodes)	Unspec.	Tempo (based on logical clocks)	ECC (secp256k1) SHA-256	No	No existing studies

*: an approximate (not precise) value. Unpsec.: the absence of existing evaluation found in the literature.

Table 7. Weights (W) Used for DLTs Assessment

	TPS	TTF	Consensus Mechanism	Cryptography Features	Feeless Transaction	Potential Integration	Total
Weights (W)	0.2	0.2	0.1	0.1	0.2	0.2	1.0

Table 8. The Attributes (A) Scoring Criteria

Score (A)	TPS	TTF	Consensus Mechanism	Cryptography Features	Feeless Transaction	Potential IoT Integration
1	< 50	> 61 s	PoW, Unspecified	RSA-based encryption	No	No existing studies
3	$51 - 500$	$6 - 60$ s	PoS, DPoS, PoT	ECC (secp256k1)	Yes	$\geq$ 1 publication on DLT analysis
5	$501 - 1$ k	$1 - 5$ s	PBFT, ABFT, DBFT, PoV	ECC (Ed25519)	—	$\geq$ 1 publication on DLT implementation
7	> 1 k	< 1 s	PoA, Tangle, Tempo, TEE	Schnorr cryptography	—	—

DLT, *d*. For instance, for the attribute throughput, a low score of 1 is given to a DLT platform that can generate fewer than 50 TPS. Justification for our scoring criteria of each attribute follows.

4.1.1 Throughput in Transactions per Second (TPS). This is a crucial metric utilised to assess the efficiency of a DLT platform. It quantifies the number of transactions that a system can process within a second. High throughput indicates that a system can handle many transactions efficiently and quickly, which is critical for IoT systems scalability as well.

As a result, a high-throughput DLT may scale more effectively, accommodating the growing data traffic from IoT devices. This keeps the system efficient and responsive even as the IoT network grows. To select the most suitable DLT platforms for IoT systems, we will allocate a higher attribute score for the DLTs that possess intrinsic capacity to generate higher throughput as shown in Table 8, and this is why in Table 7 a high weighting (0.2) is given to this attribute.

4.1.2 Time to Finality (TTF). TTF refers to the duration required for a transaction to be confirmed and recorded in the ledger, in other words the transaction is irreversibly confirmed and added to the ledger, ensuring that it cannot be altered. The shorter the TTF, the more effective the method is said to be. This involves the process of reaching consensus among the nodes in the network. In the context of IoT systems, IoT devices frequently operate in real-time contexts and rely on rapid data transmission for optimal functioning.

A DLT with a short TTF can ensure transaction confirmation on time, which is critical for IoT systems to function properly. Hence, we will assign a higher attribute score to DLTs that produces shorter TTF and weight this score with the same importance as TPS.

4.1.3 Consensus Mechanism. This is the mechanism by which all network participants reach an agreement on the validity of transactions. On the one hand, it maintains the integrity and security of data transmitted between IoT devices. Hence, the choice of a consensus mechanism in an IoT system necessitates the careful consideration of both security and energy efficiency.

The evaluation of this attribute, as depicted in Table 8, will focus on the energy consumption level associated with each consensus mechanism [11, 15]. Therefore, we allocate a higher score to a DLT that applies consensus procedure with less energy consumption. However, as a technical enabler rather than a core metric, we give it a lower weighting (0.1) than the previous two attributes.

4.1.4 Cryptographic Features. Of utmost significance are signatures and immutable ledgers. Cryptographic signatures are employed to verify the authenticity of transactions, while the immutable ledger guarantees that a transaction is irrevocable and cannot be altered or deleted once it has been documented. The effectiveness of cryptographic algorithms implemented in DLT system not only impacts the level of security but also the computational speed. For example, although most of DLT platforms shown in Table 8 operate using **Elliptic Curve Cryptography** (**ECC**), studies indicate that the ed25519 elliptic curve is more efficient than secp256k1 [16, 113]. Here, we will assign a higher attribute score to DLT that applies the ed25519 elliptic curve, and the same weighting as the consensus mechanism.

4.1.5 Feeless Transactions. A prominent characteristic of certain DLTs, these allow users to execute transactions without paying any expenses. This is a significant departure from traditional blockchain networks, which typically require users to pay transaction fees to miners or validators to process their transactions. By eliminating transaction fees, IoT devices can operate more cost-effectively, especially for large-scale deployments with numerous devices engaging in regular, small-scale interactions. The key advantage of feeless transactions in this context is that they make micropayments economically viable. Without transaction fees, even the smallest payments can be processed efficiently, enabling new business models and interactions in the IoT ecosystem. For this attribute, we will assign a higher score for the DLTs that provide feeless transactions. As cost is a key deciding factor in many systems, we weight this at 0.2.

4.1.6 Potential Integration with IoT Systems. This refers to the assessment of existing works on the DLTs-IoT integration systems, built upon prior research published in the literature. The existence of proven DLT-IoT applications is a strong indicator of a platform's maturity, suitability, and community support for IoT applications. Therefore, we will assign a higher attribute score to DLTs that have been reported to be used and/or evaluated in the IoT system environment. Similar to the previous attribute, well-evidenced and lower-risk integration is likely to be favoured by adopters, hence it receives the same 0.2 weighting.

4.1.7 Overall Score. Finally, each attribute score is multiplied by its weight and summed with all others to give the DLT's overall score, S_d:

$$S_d = \sum_{a \in \text{attributes}} (W_a \cdot A_{ad}) . \tag{1}$$

Figure 4 and Table 9 rank DLT platforms based on weighted scores from highest to lowest. Table 9 details the top six DLTs—those achieving a score strictly greater than 4.0—with a full DLT listing in Appendix A. DAG-based ledgers, including Nano, IOTA (Tangle), Hedera, and Aleph Zero dominate the top ranks. Their blockless structures enable high throughput, rapid time-to-finality, and reduced computational and storage requirements, making them well-suited for IoT applications. On the other hand, blockchain-based ledgers such as Hyperledger Fabric and IoTex emerge as strong contenders for IoT integration as these platforms offer high transaction throughput, lightweight consensus mechanisms, and well-established structures.

Another feature that makes the top ledgers better than others is the feeless transaction feature. This can improve the scalability of IoT networks, as they reduce the burden on the network and

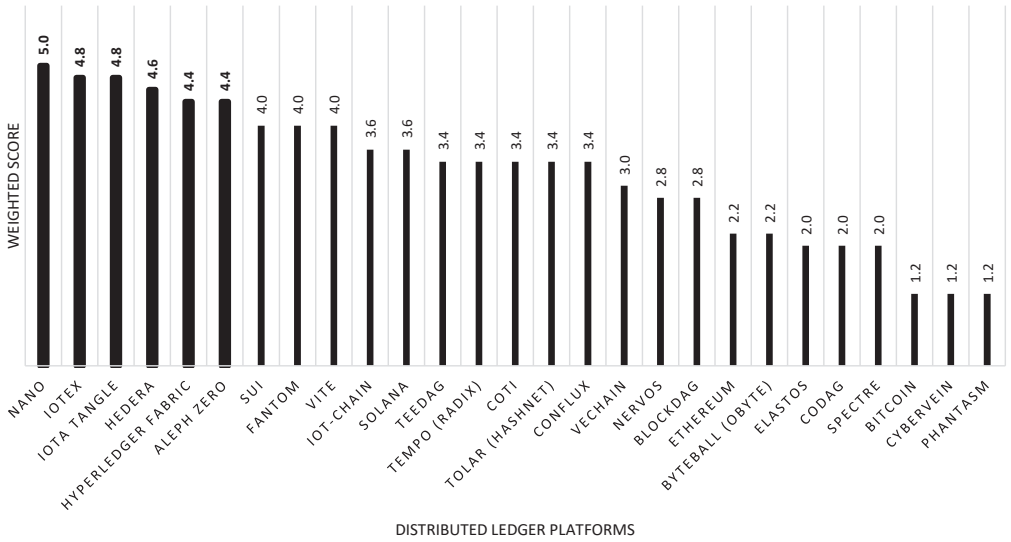


Fig. 4. Weighted Score (S) of the DLT platforms appropriate for IoT environment, thick bars denoting top DLTs that will be examined in detail.

Table 9. Weighted Scores of the Top Six DLTs

DLT platform	TPS	TTF	Consensus Mechanism	Cryptography Features	Feeless Transaction	Potential Integration	Weighted Score
Nano	7	7	5	5	3	3	5
IoTeX	7	7	5	3	1	5	4.8
IOTA Tangle	7	3	7	5	3	5	4.8
Hedera	7	5	5	5	1	5	4.6
Hyperledger Fabric	7	3	5	3	3	5	4.4
Aleph Zero	7	7	5	7	1	1	4.4

A full list of scores for all DLTs is provided in Appendix A.

enable faster transaction processing. It also facilitates integration of IoT devices with DLT networks by removing complexity of managing transaction fees. Widespread adoption of these platforms in IoT integrations further solidifies their position and differentiates them from other DLT models considered in this study. Aleph Zero, while reportedly a highly performant DAG-based DLT, is not feeless and lacks demonstrable IoT integration at the time of writing, so while it equals Hyperledger Fabric's score, it is the lowest ranked of the DAG-based examples.

5 Integration Case Studies

Six DLTs have been identified as the most likely candidates for IoT integration, with some of those having limited existing work on the topic. We analyse three use cases to provide greater insight into the architectural and performance implications of adopting DLTs in these scenarios.

The first scenario is health-IoT, which considers a smartwatch or health-monitoring wristband, samples from which are collected and tracked for the production of health related analysis and recommendations for end-users. This case study represents the need for high TPS from many

devices, but a less strict TTF requirement than other use cases due to batched data and more emphasis on post-collection analysis. The second is transactions in an e-commerce system, where IoT is used for tracking of inventory. While the total volume is high, the DLT only records event-driven transactions (e.g., one sale, one payment). The system scales by user base, not continuous sensor input, however the system must confirm the payment quickly for the user experience. Hence, e-commerce system reflects low TPS and a fast TTF. The third is an automotive manufacturing supply chain, in which a complex combination of components across multiple supplier tiers are tracked through a heavily automated assembly process. In this third scenario, the volume is based on car manufacturing velocity, where all parts must be processed quickly enough to reconcile the ongoing production without blocking subsequent steps.

For each of the use cases, an example of their architecture, their alignment with the models from Figure 1 and key metrics requirements are presented. The metrics are then assessed from the documented performance figures that have been obtained for the six DLTs.

5.1 Health-IoT Case

Smartwatches and other wearables play an increasingly vital role in proactive health management by continuously collecting a wide array of raw health data, such as heart rate, SpO2, sleep patterns, activity levels, and so on. The immediate importance and urgency of this data collection lie in its potential to provide real-time insights into an individual's physiological state, enabling early detection of potential health anomalies or trends [66]. For instance, consistent deviations in heart rate or SpO2 could signal underlying cardiovascular or respiratory issues, prompting timely medical intervention. Furthermore, this rich dataset empowers users to make informed lifestyle choices, track fitness progress, and manage chronic conditions more effectively, shifting healthcare from a reactive to a preventative model. IDC Research reported that in the second quarter of 2024, global smartwatch shipments was 43.7 million units [27].

The smartwatch acquisition architecture, shown in Figure 5, is designed to efficiently and securely collect, process, and store this critical raw health data. At its core, the architecture typically involves the smartwatch itself acting as the primary data source, equipped with various sensors to capture physiological metrics. This raw data is then transmitted wirelessly to a connected device like a smartphone/edge gateway or directly to a fog or cloud-based platform, allowing the direct connection in Figure 1(b) or hybrid connection as in Figure 1(d) utilised.

A crucial component of the architecture is the secure data pipeline, which ensures data integrity and privacy during transmission and storage. The edge gateway passes this prepared and secured data to the DLT connector/adapter, which is specialised to interface with the chosen DLT system. This approach ensures that raw, sensitive health data is efficiently captured, pre-processed at the edge, and then securely prepared for final and immutable blocks on a DLT, forming the foundational input for advanced healthcare applications.

Based on the assumption that batches of health data are recorded every 15 minutes, each smartwatch generates 96 transactions daily (RDD = 96). Given the projected 174.8 million smartwatch units produced in 2024 (UPY), and assuming all this data is transmitted and processed via a DLT system, the system would need to handle 194,222 TPS with daily operational hours, OH = 24, as detailed in Equation (2).

The TTF, which is also a critical metric, must be defined in terms of when the data must be confirmed as recorded immutably in the ledger. In the case of these batched transactions occurring every 15 minutes, a reasonable expectation is that the previous transaction has been finalised before the next one needs to be created. And so a TTF of 15 minutes can be set, assuming that the upload time for the data is significantly less than this.

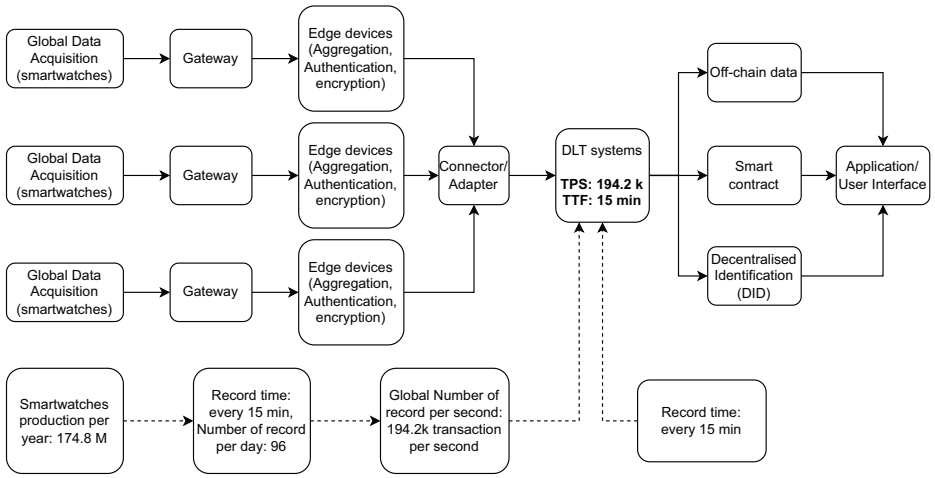


Fig. 5. Example architecture of smartwatches global data acquisition with DLT.

$$\text{TPS} = \frac{\text{RDD} \times \text{UPY}}{\text{OH} \times 3600} = 194,222\,, \tag{2}$$

$$\text{TTF} = \frac{\text{RDD}}{1440} = 15\,\text{minutes}. \tag{3}$$

5.2 E-commerce Case

The rapid growth of e-commerce has become indispensable in our daily lives, offering unparalleled convenience and accessibility. The integration of IoT systems further enhances this experience, as well as offering businesses opportunities for streamlined operations and other efficiencies. These IoT devices enable real-time tracking of goods, automated inventory management, and personalised shopping experiences through data-driven insights. This synergy between e-commerce and IoT creates a seamless and efficient shopping ecosystem, revolutionising how people buy and sell products. The integration of DLTs with this process has been the subject of study [87] and also emphasises the importance of IoT within the supply chain, particularly for product traceability.

The data flow in the e-commerce model in Figure 6 begins with global data acquisition from IoT devices, a user's interactions via app or web browser, and activity within supply chain systems. Subsequently, this requested data flows through an API Gateway to the core Business Logic and Microservices. Critical and immutable transactions, such as order confirmations or supply chain events, are then recorded on the DLT Network, while non-critical or bulk data is stored in off-chain databases. Both DLT and off-chain data are accessible for analytics and reporting, providing insights that can feed back into the e-commerce application front-end for improved user experience. Additionally, payment gateway integrations securely process transactions, with relevant records also committed to the DLT.

To enhance efficiency and responsiveness, a fog computing layer can be strategically introduced at the edge gateway stage. This enables localised processing and analysis of data directly at the network edge, closer to IoT sensors and user interaction points. The integrated e-commerce architecture, which incorporates fog computing and is depicted in Figure 1(c), is ideal for this application. Conversely, Figure 1(b) shows an alternative direct connection architecture that operates without a fog computing layer that can also accommodate this use case.

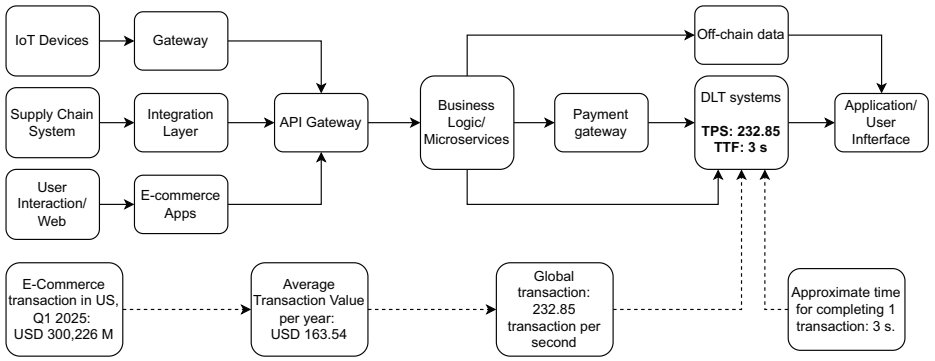


Fig. 6. Example architecture of e-commerce global data acquisition from IoT devices with DLT.

In the USA alone, the amount of **e-commerce transactions (ECT)** in the first quarter of 2025 reach a value of 300,226 Million USD [95] with **average transaction value (ATV)** of 163.54 USD. This information allows us to estimate the TPS, according to Equation (4), of 232.85 TPS by assuming daily operational hours of OH = 24 and number of operational days per year, DY = 365. The time to finality is assumed as the amount of time required for credit card authorisation. The authorisation phase of a credit card transaction is critical for immediate customer feedback, with industry leaders consistently reporting processing times of 1 to 3 seconds [148]. Hence, we define our TTF in this case is 3 seconds by taking the longest acceptable transaction delay.

$$\text{TPS} = \frac{\text{ECT} \times 4}{\text{ATV} \times \text{OH} \times \text{DY} \times 3600} = 232.85\,, \tag{4}$$

$$\text{TTF} = 3 \text{ seconds.} \tag{5}$$

5.3 Automotive Supply Chain Case

Car manufacturing is a heavily automated process that involves a deep supply chain of thousands of parts. Toyota claims that a car comprises more than 30,000 parts, coming both from itself and its suppliers [124], and that a car can be assembled in 22 hours. In 2024, the company reported that it manufactured 10.6 million vehicles [125].

Generally, an automotive supply chain contains multiple tiers of suppliers, from those that turn raw materials into components, through those that create more complex component assemblies, ending with the manufacturer who assembles and integrates the final product [28]. While some factories operate shifts over a 24-hour period, others (including Toyota) do incorporate downtime, resulting in a 16-hour per day duty cycle or similar. For the final product, we can assume a certain amount of concurrency in parts handling is possible, for example installation of front and rear lighting assemblies can happen at the same time with no interdependency.

Using this real-world data, combined with reasonable production assumptions and a supply chain structure, we arrive at Figure 7, which depicts suppliers and a manufacturer and their integration into a DLT-based supply chain. For example, a manufacturer or higher-tier supplier may create an order for a part, then that part may be provided by the lower-tier supplier, and finally that part may be integrated into a larger system.

This structure, which composes multiple independent entities that may have internal M2M communication during production processes, subsequently transacting based on supplied products, closest aligns with the fog system shown in Figure 1(c), although this assumes that each supplier has a similar level of IoT adoption internally.

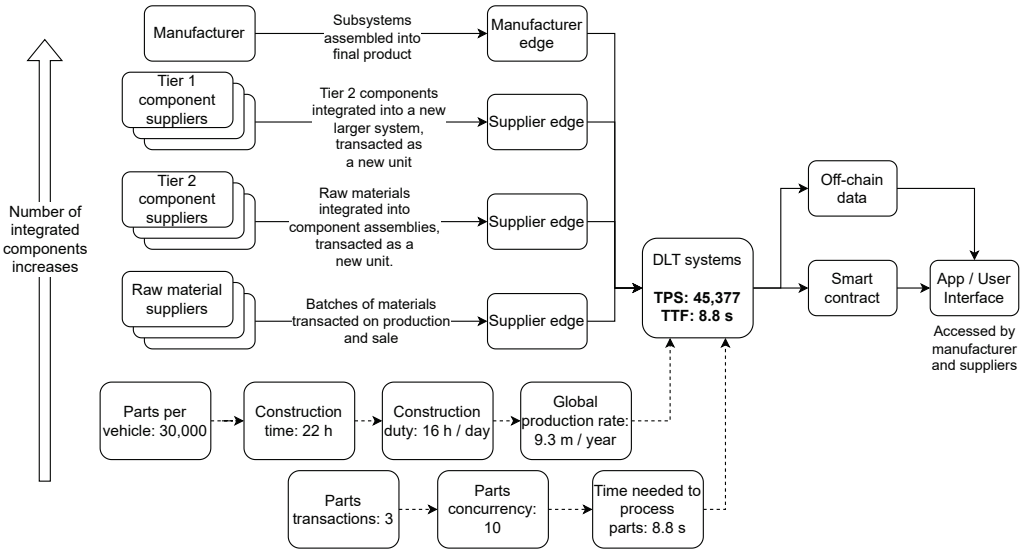


Fig. 7. Example architecture of automotive manufacturing supply chain with DLT.

In Equations (6) and (7), we determine a reasonable TPS and TTF, that would allow global production on the scale previously cited with the target production duration, PD = 22, and daily operational hours, OH = 16. The TPS depends on the parts per unit, PPU = 30, 000, the number of units produced yearly, UPY = 10.6 million, transactions per part, TPP = 3, and the number of operational days per year, DY = 365. TTF assumes the transactions on parts must complete during the time they are handled during assembly and is spread evenly. It uses the number of hours to produce each unit, HPU = 22 and how many parts are handled concurrently, PC = 10, to estimate this.

$$\text{TPS} = \frac{\text{PPU} \times \text{UPY} \times \text{TPP}}{\text{DY} \times \text{OH} \times 3600} = 45,377\,, \tag{6}$$

$$\text{TTF} = \frac{\text{HPU} \times 3600}{\text{PPU} \times \text{TPP}} \times \text{PC} = 8.8 \text{ seconds}. \tag{7}$$

5.4 Analysis and Discussion

The source spreadsheet used to calculate the TPS and TTF requirements for the three cases is contributed as a data publication [70] for future refinement and experimentation. Table 10 summarises the TPS and TTF figures for each of the six shortlisted DLTs alongside the calculated requirements of the three use cases. Given that each case has unique requirements and that some DLTs report ranges of TPS and TTF performance, a means of further analysing this data is proposed.

For both TPS and TTF, we determine whether the stated maximum and minimum stated performance figures would meet the requirement for the case, x, represented as 0 or 1, denoted for example as TTF_{max}. If only one figure is provided then both min and max are the same. Additionally, the DLTs are ranked based on whether their performance metric is within the same order of magnitude as the requirement. This is done for both minimum and maximum, or jointly if a single value is provided, again as a 0 or 1, denoted for example as TPS_{omin}. This allows DLTs that do not meet the requirements, but are close to it, to be ranked more highly than those that are a significant way from meeting the requirements. Finally, each of these metrics — eight in total — are assigned weights, for example $\text{W}_{\text{TTF}_{omin}}$, normalised. This allows for tuning of the requirements, which are

Table 10. Top Six DLTs Versus Case Study Requirements

DLT / Case	TPS	TTF	Weighted Score
Nano	10 K	<1 s	5
IoTeX	2 K	<1 s	4.8
IOTA Tangle	1.5 K	10–12 s	4.8
Hedera	10 K	3–5 s	4.6
Hyperledger Fabric	3–20 K	2–120 s	4.4
Aleph Zero	89–90 K	0.4–0.5 s	4.4
Health IoT	194 K	0.026 s	—
E-commerce	0.2 K	3 s	—
Automotive	45 K	8.8 s	—

Table 11. DLT Scores for Each Case

DLT	Health IoT	E-Commerce	Car Manufacturing
Nano	50 %	100 %	50 %
IoTeX	50 %	100 %	50 %
IOTA Tangle	50 %	50 %	0 %
Hedera	50 %	63 %	63 %
Hyperledger Fabric	50 %	81 %	38 %
Aleph Zero	50 %	100 %	100 %

available in Ref. [70]. The final score for each DLT in each use case is then a percentage representing the sum weights of all criteria, C, that were met:

$$\text{Score} = \sum_{c \in C} (c_x \cdot W_{c_x}),$$
$$C = \{\text{TPS}_{\text{min}}, \text{TPS}_{\text{max}}, \text{TPS}_{\text{omin}}, \text{TPS}_{\text{omax}}, \text{TTF}_{\text{min}}, \text{TTF}_{\text{max}}, \text{TTF}_{\text{omin}}, \text{TTF}_{\text{omax}}\}. \quad (8)$$

From this we produce Table 11, the raw data for which is provided in Ref. [70]. As presented, the health-IoT case cannot be met by any of the shortlisted DLTs without enhancements to the DLTs, or re-architecting or down-scaling of the workload. However, the e-commerce and car manufacturing cases can both be met by one or more DLTs fully, at least in terms of TPS and TTF, with others possibly meeting the requirements with refinements or optimisation.

Re-architecting the health-IoT use case might involve side-chains or sharding to distribute the workload. This would complicate the DLT implementation and poses challenges such as how to assign a user's workload to a particular shard or chain.

A number of other factors are not considered within this assessment, including storage requirements, bandwidth consumption of transactions and the specification/quantity of nodes required to provide the DLT. Nor are the more qualitative measures, such as cryptography features and others covered in Section 4. These can be considered in a separate assessment step when aligning system architecture with DLT solution, or integrated into a more complex criteria scoring system.

For example, in the e-commerce case, Nano, IoTeX, and Aleph Zero can all meet the functional requirements of TPS and TTF. If selecting the winning candidate is done based purely on the weighted scores (Table 9), then Nano would be chosen. However, if there were any additional constraints placed upon the decision, such as key types, fee types, storage requirements or existing use case examples, then the outcome may be different. This makes the case for system architects and decision makers defining their own attribute weights based on our work, rather than directly applying those used here without further consideration.

6 Future Directions

This study identifies a critical challenge in integrating DLTs into IoT systems that lies in effectively managing the enormous volume and diverse variety of data generated by IoT devices. It provides a comprehensive analysis of DLT integration in diverse IoT applications (Section 5) and the evaluation of existing DLTs, selected for their lightweight architectures via a weighted scoring technique (Section 4). Hence, these research findings point to the development of more efficient and readily integrated DLT systems that are specifically intended to meet these criteria, which is critical for their practical application in IoT environments with limited resources.

Innovative research on rapid and robust consensus frameworks is critical for dealing with the massive volume, velocity, and real-time demands of IoT data. This will minimise bottlenecks and assure resilience against attacks and data corruption across large networks. The key future direction is continuum-optimised hybrid consensus, which uses the **Distributed Computing Continuum Systems** (**DCCS**) framework to guide design. This requires deploying lightweight consensus at the edge/fog layer for fast, resource-efficient, localised agreement, and reserving a more rigorous consensus for finality at the cloud layer. This stratified approach maximises performance and scalable trust throughout the computational continuum [45].

Aside from reaching rapid and robust consensus, another critical aspect for integrating DLTs into IoT, particularly for health data use cases, is restructuring the DLT infrastructure to manage data volume and variety effectively. To deal with the overwhelming, constant data streams such as from health-IoT devices, solutions such as adding side chains or sharding become critical for dividing the workload, as does batch processing. Current sharding concepts often involve static partitioning. Future DLT architectures could implement adaptive sharding, where the sharding strategy dynamically reconfigures based on real-time IoT network load, data types, and device density. This could be coupled with dynamic resource allocation for shards, ensuring computational and storage resources are optimally assigned based on the immediate demands of specific IoT data streams, preventing bottlenecks and maximising throughput.

Future DLTs could also implement a tiered architecture that incorporates intelligent edge agents powered by AI that can dynamically learn patterns in IoT data streams. These agents would not just batch, but semantically filter data by identifying and discarding redundant or irrelevant information before it even touches the DLT. This would drastically reduce on-ledger data volume while preserving critical information. To offer an overview of the latest works on the AI-enabled DLT, we listed some of the existing literature that may have significant impact on the future development of the integration of DLT and IoT systems.

— AI-powered consensus mechanisms. Academic research highlights that AI offers promising pathways to optimise consensus mechanism by enhancing efficiency, reducing energy consumption, and improving scalability. Studies specifically demonstrate how integrating AI such as Deep Learning can enable dynamic validator selection and real-time adjustment of consensus difficulty [18].
— AI for network management and congestion mitigation. Literature confirms the application of AI in predicting network congestion within DLT ecosystems, which is essential for ensuring scalability and efficiency [20]. Machine Learning and Deep Learning techniques analyse historical blockchain data to accurately forecast congestion patterns. This allows for proactive measures, such as optimising transaction scheduling and resource allocation before congestion occurs, leading to improved transaction throughput and reduced latency.
— Smart contract optimisation and security. AI can enhance the functionality and performance of smart contracts through automated testing and analysis, reducing risk of exploits and making the underlying platform more reliable and robust for high-speed operation [97].

Finally, we observe that the inherent device heterogeneity, which encompasses various hardware, proprietary protocols and operating systems, poses a substantial hurdle for DLT integration into IoT contexts. This fragmentation complicates device interoperability and DLT interfacing, while also adding to security concerns due to varying processing capabilities and security policy administration. Future DLT solutions could investigate self-configuring DLT adapters that dynamically adjust protocols, or AI-driven interoperability agents embedded at the edge to autonomously translate and normalise data streams for consistent DLT interaction, thereby abstracting and standardising interactions regardless of device differences.

7 Conclusion

The advancement of sensors, actuators, and other intelligent devices is rapidly permeating several sectors, including industry, healthcare, and transportation. These devices transmit vast amounts of data from the field, causing scalability issues for the systems ingesting the data, interoperability problems across devices, and the system security concerns, including safeguarding user privacy. Recent investigations indicate that DLT have advanced as a solution to many issues in the development of IoT systems [75, 112, 134].

This review article has examined the current distributed ledger platforms that could potentially be integrated into the IoT systems. Typically, these ledgers can be classified as blockchain-, DAG-, hybrid- and logical clock-based. We selected lightweight DLTs, utilising a new weighted scoring method to determine the most suitable platforms for potential integration with IoT devices, in which we have utilised various performance indicators encompassing throughput measured in TPS, TTF, consensus mechanism, cryptographic features, feeless transaction capabilities, and current implementation of DLT-IoT integration. Many approaches were identified across 27 DLTs, a number of which have yet to be evaluated in IoT contexts.

Using the proposed scoring system, the top six ranked DLT platforms were identified: IoTex, Hyperledger Fabric, Nano, IOTA (Tangle), Hedera and Aleph Zero, were identified using this system. These were then assessed against three use cases: health-IoT, e-commerce and car manufacturing, each with unique architectural properties, throughput, and delay requirements.

Additional rating was performed based on the numerical criteria of TPS and TTF, identifying varying suitability for each scenario. This assessment method can be used in determining the feasibility of a particular system architecture and workload when seeking a suitable DLT and may also indicate when re-architecting is necessary. For example, the health IoT case was found to not be feasible with any of the shortlisted DLTs in the form it is presented due to throughput limitations. Folding qualitative criteria into this assessment approach is a possible area of future work.

To further improve DLT-IoT integration, this study highlights several key research directions. These include the development of: rapid and robust consensus frameworks for minimising bottlenecks and assuring data integrity, adaptive sharding for dynamic workload management, AI-driven intelligent edge agents for pattern recognition in IoT data, and self-configuring DLT adapters for autonomous data translation and normalisation, ensuring seamless DLT interaction.

Acknowledgment

The authors extend their gratitude to the reviewers of this work for their time and input, as well as to the JCU research support staff for their administrative assistance.

References

[1] Abdelzahir Abdelmaboud, Abdelmuttlib Ibrahim Abdalla Ahmed, Mohammed Abaker, Taiseer Abdalla Elfadil Eisa, Hashim Albasheer, Sara Abdelwahab Ghorashi, and Faten Khalid Karim. 2022. Blockchain for IoT applications:

Taxonomy, platforms, recent advances, challenges and future research directions. *Electronics (Switzerland)* 11, 4 (Feb. 2022). DOI: https://doi.org/10.3390/electronics11040630

[2] Vidushi Agarwal and Sujata Pal. 2020. Blockchain meets IoT: A scalable architecture for security and maintenance. In *Proceedings—-2020 IEEE 17th International Conference on Mobile ad Hoc and Smart Systems, MASS 2020*. Institute of Electrical and Electronics Engineers Inc., 53–61. DOI: https://doi.org/10.1109/MASS50613.2020.00017

[3] Mohd Majid Akhtar, Danish Raza Rizvi, Mohd Abdul Ahad, Salil S. Kanhere, Mohammad Amjad, and Giuseppe Coviello. 2021. Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy. *Sensors* 21 13 (July 2021). DOI: https://doi.org/10.3390/s21134354

[4] Mohammad Alahmad, Imad Alshaikhli, Abdulrahman Alkandari, Abdullah Alshehab, Rabiul Islam, and Meshal Alnasheet. 2022. Influence of hedera hashgraph over blockchain. *Journal of Engineering Science and Technology* 17 5 (2022), 3475–3488.

[5] Shadab Alam, Surbhi Bhatia, Mohammed Shuaib, Mousa Mohammed Khubrani, Fayez Alfayez, Areej A. Malibari, and Sadaf Ahmad. 2023. An overview of blockchain and IoT integration for secure and reliable health records monitoring. *Sustainability (Switzerland)* 15 7 (April 2023). DOI: https://doi.org/10.3390/su15075660

[6] Abbas Ali. 2025. Advancements and transformative applications of blockchain technology. *Journal of Engineering and Computational Intelligence Review* 3, 1 (2025), 36–51. Retrieved from https://jecir.com/index.php/jecir/article/view/8. Accessed: 2026-01-12.

[7] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. 2019. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys and Tutorials* 21 2 (April 2019), 1676–1717. DOI: https://doi.org/10.1109/COMST.2018.2886932

[8] Ahmed Abubakar Aliyu and Jinshuo Liu. 2023. Blockchain-based smart farm security framework for the internet of things. *Sensors* 23 18 (Sept. 2023). DOI: https://doi.org/10.3390/s23187992

[9] Mays Alshaikhli, Tarek Elfouly, Omar Elharrouss, Amr Mohamed, and Najmath Ottakath. 2022. Evolution of internet of things from blockchain to IOTA: A survey. *IEEE Access* 10 (2022), 844–866. DOI: https://doi.org/10.1109/ACCESS.2021.3138353

[10] Yehia Ibrahim Alzoubi, Ahmad Al-Ahmad, Hasan Kahtan, and Ashraf Jaradat. 2022. Internet of things and blockchain integration: Security, privacy, technical, and design challenges. *Future Internet* 14, 7 (July 2022). DOI: https://doi.org/10.3390/fi14070216

[11] Yehia Ibrahim Alzoubi and Alok Mishra. 2023. Green blockchain—A move towards sustainability. *Journal of Cleaner Production* 430 (Dec. 2023). DOI: https://doi.org/10.1016/j.jclepro.2023.139541

[12] Claudia Antal, Tudor Cioara, Ionut Anghel, Marcel Antal, and Ioan Salomie. 2021. Distributed ledger technology review and decentralized applications development guidelines. *Future Internet* 13, 3 (March 2021), 1–32. DOI: https://doi.org/10.3390/fi13030062

[13] Mateen Ashraf and Cathal Heavey. 2022. A prototype of supply chain traceability using solana as blockchain and IoT. In *Procedia Computer Science*, Vol. 217. Elsevier B. V. 948–959. DOI: https://doi.org/10.1016/j.procs.2022.12.292

[14] Prabadevi B., N. Deepa, Quoc-Viet Pham, Dinh C. Nguyen, Praveen Kumar Reddy M., Thippa Reddy G., Pubudu N. Pathirana, and Octavia Dobre. 2021. Toward blockchain for edge-of-things: A new paradigm, opportunities, and future directions. *IEEE Internet of Things Magazine* 4, 2 (April 2021), 102–108. DOI: https://doi.org/10.1109/IOTM.0001.2000191

[15] Abigael Okikijesu Bada, Amalia Damianou, Constantinos Marios Angelopoulos, and Vasilios Katos. 2021. Towards a green blockchain: A review of consensus mechanisms and their energy consumption. In *Proceedings—17th Annual International Conference on Distributed Computing in Sensor Systems, DCOS 2021*. Institute of Electrical and Electronics Engineers Inc., 503–511. DOI: https://doi.org/10.1109/DCOSS52077.2021.00083

[16] Mohammed El baraka, Siham Ezzouak, and Demba Sow. 2024. Exploring alternative elliptic curves for Bitcoin: An efficiency comparison. In *Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security* (New York, NY, USA). ACM, 1–8. DOI: https://doi.org/10.1145/3659677.3659698

[17] Rafael Belchior, Luke Riley, Thomas Hardjono, André Vasconcelos, and Miguel Correia. 2023. Do you need a distributed ledger technology interoperability solution? *Distributed Ledger Technologies: Research and Practice* 2, 1 (Sept. 2023), 1–37. DOI: https://doi.org/10.1145/3564532

[18] Jagger S. Bellagarda and Adnan M. Abu-Mahfouz. 2022. An updated survey on the convergence of distributed ledger technology and artificial intelligence: Current state, major challenges and future direction. *IEEE Access* 10 (2022), 50774–50793. DOI: https://doi.org/10.1109/ACCESS.2022.3173297

[19] Federico Matteo Benčić and Ivana Podnar Žarko. 2018. Distributed ledger technology: Blockchain compared to directed acyclic graph. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. DOI: https://doi.org/10.1109/ICDCS.2018.00171

[20] Dhanasak Bhumichai, Christos Smiliotopoulos, Ryan Benton, Georgios Kambourakis, and Dimitrios Damopoulos. 2024. The convergence of artificial intelligence and blockchain: The state of play and the road ahead. *Information (Switzerland)* 15, 5 (May 2024). DOI: https://doi.org/10.3390/info15050268

[21] Bharat Bhushan, Chinmayee Sahoo, Preeti Sinha, and Aditya Khamparia. 2021. Unification of blockchain and internet of things (BIoT): Requirements, working model, challenges and future directions. *Wireless Networks* 27, 1 (Jan. 2021), 55–90. DOI: https://doi.org/10.1007/s11276-020-02445-6

[22] Anastasios N. Bikos and Sathish A. P. Kumar. 2022. Securing digital ledger technologies-enabled IoT devices: Taxonomy, challenges, and solutions. *IEEE Access* 10 (2022), 46238–46254. DOI: https://doi.org/10.1109/ACCESS.2022.3169141

[23] Blake Bryant and Hossein Saiedian. 2022. Key challenges in security of IoT devices and securing them with the blockchain technology. *SECURITY AND PRIVACY* 5, 5 (Sept. 2022). DOI: https://doi.org/10.1002/spy2.251

[24] Bin Cao, Yixin Li, Lei Zhang, Long Zhang, Shahid Mumtaz, Zhenyu Zhou, and Mugen Peng. 2019. When internet of things meets blockchain challenges in distributed consensus. *IEEE Network* (2019), 133–139. DOI: https://doi.org/10.1109/MNET.2019.1900002

[25] Bin Cao, Zhenghui Zhang, Daquan Feng, Shengli Zhang, Lei Zhang, Mugen Peng, and Yun Li. 2020. Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks* 6, 4 (Nov. 2020), 480–485. DOI: https://doi.org/10.1016/j.dcan.2019.12.001

[26] Mingrui Cao, Long Zhang, and Bin Cao. 2023. Toward on-device federated learning: A direct acyclic graph-based blockchain approach. *IEEE Transactions on Neural Networks and Learning Systems* 34, 4 (April 2023), 2028–2042. DOI: https://doi.org/10.1109/TNNLS.2021.3105810

[27] Miguel Carreon, Maggie Xie, and Sophie Pan. 2024. Global wrist-worn device market ships almost 44 million units in 2Q 2024. *IDC Research* (Sept. 2024). Retrieved from https://my.idc.com/getdoc.jsp?containerId=prCHE52577924. Accessed: 2026-01-12.

[28] Charu Chandra and Ali K. Kamrani. 2004. *Knowledge Management for Consumer-Focused Product Design*. Springer US, Boston, MA, 211–234. DOI: https://doi.org/10.1007/978-1-4419-9015-0_9

[29] Eason Chen, Justa Liang, Bucket Protocol, Ray Huang, Damien Chen, Ashley Hsu, Konstantinos Chalkias, and Stefanos Pleros. 2023. Building Random, Fair, and Verifiable Games on Blockchain. Raffle smart contract designs on Sui Network Pierce Hung Bucket Protocol. DOI: https://doi.org/10.48550/arXiv.2310.12305

[30] Hongsong Chen, Shi Lei, Yiying Zhang, Xintong Han, Yongrui Cao, and Yongpeng Zhang. 2023. Blockchain-based internet of things security architecture and applications. *Journal of Ambient Intelligence and Humanized Computing* 14, 12 (Dec. 2023), 16703–16714. DOI: https://doi.org/10.1007/s12652-023-04675-w

[31] Lu Chen, Xin Zhang, and Zhixin Sun. 2022. Scalable blockchain storage model based on DHT and IPFS. *KSII Transactions on Internet and Information Systems* 16, 7 (July 2022), 2286–2304. DOI: https://doi.org/10.3837/tiis.2022.07.009

[32] Yourong Chen, Yang Zhang, Yubo Zhuang, Kelei Miao, Seyedamin Pouriyeh, and Meng Han. 2024. Efficient and secure blockchain consensus algorithm for heterogeneous industrial internet of things nodes based on double-DAG. *IEEE Transactions on Industrial Informatics* (2024). DOI: https://doi.org/10.1109/TII.2023.3342473

[33] Zhuo Chen, Xiao Chen, and Yun Li. 2023. Performance and security analysis of distributed ledger under the internet of things environments with network instability. *IEEE Internet of Things Journal* 10, 5 (March 2023), 4213–4225. DOI: https://doi.org/10.1109/JIOT.2022.3216586

[34] Bipin Chhetri, Saroj Gopali, Rukayat Olapojoye, Samin Dehbash, and Akbar Siami Namin. 2023. A survey on blockchain-based federated learning and data privacy. *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1311–1318. Retrieved from http://arxiv.org/abs/2306.17338

[35] Sang-Min Choi, Jiho Park, Quan Nguyen, and Andre Cronje. 2018. Fantom: A scalable framework for asynchronous distributed systems. (Oct. 2018). DOI: https://doi.org/10.48550/arXiv.1810.10360

[36] Mohammad Jabed Morshed Chowdhury, Md Sadek Ferdous, Kamanashis Biswas, Niaz Chowdhury, A. S. M. Kayes, Mamoun Alazab, and Paul Watters. 2019. A comparative analysis of distributed ledger technology platforms. *IEEE Access* 7 (2019), 167930–167943. DOI: https://doi.org/10.1109/ACCESS.2019.2953729

[37] Anton Churyumov. 2016. Byteball: A Decentralized System for Storage and Transfer of Value. 49 pages. Retrieved from https://obyte.org/Byteball.pdf. Accessed: 2026-01-12.

[38] Laizhong Cui, Shu Yang, Ziteng Chen, Yi Pan, Mingwei Xu, and Ke Xu. 2020. An efficient and compacted DAG-based blockchain protocol for industrial internet of things. *IEEE Transactions on Industrial Informatics* 16, 6 (June 2020), 4134–4145. DOI: https://doi.org/10.1109/TII.2019.2931157

[39] Andrew Cullen, Pietro Ferraro, Christopher King, and Robert Shorten. 2020. On the resilience of DAG-based distributed ledgers in IoT applications. *IEEE Internet of Things Journal* 7, 8 (Aug. 2020), 7112–7122. DOI: https://doi.org/10.1109/JIOT.2020.2983401

[40] Hong Ning Dai, Zibin Zheng, and Yan Zhang. 2019. Blockchain for internet of things: A survey. *IEEE Internet of Things Journal* 6, 5 (Oct. 2019), 8076–8094. DOI: https://doi.org/10.1109/JIOT.2019.2920987

[41] Mazin Debe, Khaled Salah, Muhammad Habib Ur Rehman, and Davor Svetinovic. 2019. IoT public fog nodes reputation system: A decentralized solution using ethereum blockchain. *IEEE Access* 7 (2019), 178082–178093. DOI: https://doi.org/10.1109/ACCESS.2019.2958355

[42] Chinmaya Kumar Dehury, Satish Narayana Srirama, Praveen Kumar Donta, and Schahram Dustdar. 2024. Securing clustered edge intelligence with blockchain. *IEEE Consumer Electronics Magazine* 13, 1 (Jan. 2024), 22–29. DOI: https://doi.org/10.1109/MCE.2022.3164529

[43] Nathanael Denis, Sophie Chabridon, and Maryline Laurent. 2024. Bringing privacy, security and performance to the Internet of Things using IOTA and usage control. *Annales des Telecommunications/Annals of Telecommunications* (2024). DOI: https://doi.org/10.1007/s12243-023-01005-1

[44] Aarju Dixit, Aditya Trivedi, and W. Wilfred Godfrey. 2022. A survey of cyber attacks on blockchain based IoT systems for industry 4.0. *IET Blockchain* (Nov. 2022). DOI: https://doi.org/10.1049/blc2.12017

[45] Praveen Kumar Donta, Qiyang Zhang, and Schahram Dustdar. 2025. Performance measurements in the AI-centric computing continuum systems. (June 2025). Retrieved from http://arxiv.org/abs/2506.22884

[46] Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. 2019. LSB: A lightweight scalable blockchain for IoT security and anonymity. *J. Parallel and Distrib. Comput.* 134 (Dec. 2019), 180–197. DOI: https://doi.org/10.1016/j.jpdc.2019.08.005

[47] Fintan Duffy, Malika Bendechache, and Irina Tal. 2021. Can solana's high throughput be an enabler for IoT?. In *Proceedings—2021 21st International Conference on Software Quality, Reliability and Security Companion, QRS-C 2021.* Institute of Electrical and Electronics Engineers Inc., 615–621. DOI: https://doi.org/10.1109/QRS-C55045.2021.00094

[48] Atis Elsts, Efstathios Mitskas, and George Oikonomou. 2018. Distributed ledger technology and the internet of things: A feasibility study. In *Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems* (Shenzhen, China). Association for Computing Machinery, 7–12. DOI: https://doi.org/10.1145/3282278.3282280

[49] Caixiang Fan, Sara Ghaemi, Hamzeh Khazaei, Yuxiang Chen, and Petr Musilek. 2021. Performance analysis of the IOTA DAG-based distributed ledger. *ACM Transactions on Modeling and Performance Evaluation of Computing Systems* 6, 3 (Sept. 2021). DOI: https://doi.org/10.1145/3485188

[50] Bahar Farahani, Farshad Firouzi, and Markus Luecking. 2021. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications* 177 (March 2021). DOI: https://doi.org/10.1016/j.jnca.2020.102936

[51] Wen Fei, Hiroyuki Ohno, and Srinivas Sampalli. 2024. A systematic review of IoT security: Research potential, challenges, and future directions. *Comput. Surveys* 56, 5 (May 2024), 1–40. DOI: https://doi.org/10.1145/3625094

[52] Farshad Firouzi, Shiyi Jiang, Krishnendu Chakrabarty, Bahar Farahani, Mahmoud Daneshmand, Jaeseung Song, and Kunal Mankodiya. 2023. Fusion of IoT, AI, edge-fog-cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine. *IEEE Internet of Things Journal* 10, 5 (March 2023), 3686–3705. DOI: https://doi.org/10.1109/JIOT.2022.3191881

[53] Marina Fortunato. 2023. Web3 for Better Whitepaper 3.0. Retrieved from https://files.vechain.org/vechaincontainer/vechain-whitepaper-3-0.pdf. Accessed: 2026-01-12.

[54] Elastos Foundation. 2018. Elastos Whitepaper. (Jan. 2018). Retrieved from https://www.elastos.org/downloads/elastos_whitepaper_en.pdf. Accessed: 2026-01-12.

[55] Ankit Gangwal, Haripriya Ravali Gangavalli, and Apoorva Thirupathi. 2023. A survey of Layer-two blockchain protocols. *Journal of Network and Computer Applications* 209 (Jan. 2023). DOI: https://doi.org/10.1016/j.jnca.2022.103539

[56] Jack Ge, Jerry Ning, and Arthur Yu. 2018. CyberVein A Dataflow Blockchain Platform Whitepaper-Version 1.0. Retrieved from https://chainwhy.com/upload/default/20180623/9cbaef06f578834c1689116be5ec22f9.pdf. Accessed: 2026-01-12.

[57] Mozhgan Gholami, Ali Ghaffari, Nahideh Derakhshanfard, Nadir IbrahimoğLu, and Ali Asghar Pourhaji Kazem. 2025. Blockchain integration in IoT: Applications, opportunities, and challenges. *Computers, Materials and Continua* 83, 2 (2025), 1561–1605. DOI: https://doi.org/10.32604/cmc.2025.063304

[58] Adam Gągol, Damian Leśniak, Damian Straszak, and Michał Świętek. 2019. ALEPH: Efficient atomic broadcast in asynchronous networks with Byzantine nodes. In *AFT 2019—Proceedings of the 1st ACM Conference on Advances in Financial Technologies.* Association for Computing Machinery, Inc, 214–228. DOI: https://doi.org/10.1145/3318041.3355467

[59] Malka N. Halgamuge, Geetha K. Munasinghe, and Moshe Zukerman. 2024. Time estimation for a new block generation in blockchain-enabled internet of things. *IEEE Transactions on Network and Service Management* 21, 1 (Feb. 2024), 535–557. DOI: https://doi.org/10.1109/TNSM.2023.3316394

[60] Nir Haloani, Avishay Yanai, Meital Levy, and Yair Lavi. 2024. COTI V2: Confidential Computing Ethereum Layer 2. Retrieved from https://coti.io/files/coti_v2_whitepaper.pdf. Accessed: 2026-01-12.

[61] Runchao Han, Gary Shapiro, Vincent Gramoli, and Xiwei Xu. 2020. On the performance of distributed ledgers for Internet of Things. *Internet of Things* 10 (2020), 87. DOI: https://doi.org/10.1016/j.iot.2019.100087

[62] Lei Hang and Do Hyeun Kim. 2019. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors (Switzerland)* 19, 10 (May 2019). DOI: https://doi.org/10.3390/s19102228

[63] A. S. M.Touhidul Hasan, Shabnam Sabah, Apubra Daria, and Rakib Ul Haque. 2023. A peer-to-peer blockchain-based architecture for trusted and reliable agricultural product traceability. *Decision Analytics Journal* 9 (Dec. 2023). DOI: https://doi.org/10.1016/j.dajour.2023.100363

[64] Pawan Hegde and Praveen Kumar Reddy Maddikunta. 2023. Amalgamation of blockchain with resource-constrained IoT devices for healthcare applications – State of art, challenges and future directions. *International Journal of Cognitive Computing in Engineering* 4 (June 2023), 220–239. DOI: https://doi.org/10.1016/j.ijcce.2023.06.002

[65] Houssein Hellani, Layth Sliman, Abed Ellatif Samhat, and Ernesto Exposito. 2021. Computing resource allocation scheme for DAG-based IOTA nodes. *Sensors* 21, 14 (July 2021). DOI: https://doi.org/10.3390/s21144703

[66] Mohsen Masoumian Hosseini, Seyedeh Toktam Masoumian Hosseini, Karim Qayumi, Shahriar Hosseinzadeh, and Seyedeh Saba Sajadi Tabar. 2023. Smartwatches in healthcare medicine: Assistance and monitoring; a scoping review. *BMC Medical Informatics and Decision Making* 23, 1 (Dec. 2023). DOI: https://doi.org/10.1186/s12911-023-02350-w

[67] Alen Hrga, Tomislav Capuder, and Ivana Podnar Zarko. 2020. Demystifying distributed ledger technologies: Limits, challenges, and potentials in the energy sector. *IEEE Access* 8 (2020), 126149–126163. DOI: https://doi.org/10.1109/ACCESS.2020.3007935

[68] Dan Hughes. 2017. Radix-Tempo. Retrieved from www.radix.global. Accessed: 2026-01-12.

[69] Amirhossein Adavoudi Jolfaei, Seyed Farhad Aghili, and Dave Singelee. 2021. A survey on blockchain-based IoMT systems: Towards scalability. *IEEE Access* 9 (2021), 148948–148975. DOI: https://doi.org/10.1109/ACCESS.2021.3117662

[70] Jusak Jusak and Steve Kerrison. 2025. IoT DLT Survey Data. Retrieved from https://gitlab.com/jcus-sst/iot-dlt-survey-data. Accessed: 2026-01-12.

[71] Felix Kahmann, Fabian Honecker, Julian Dreyer, Marten Fischer, and Ralf Tönjes. 2023. Performance comparison of directed acyclic graph-based distributed ledgers and blockchain platforms. *Computers* 12, 12 (Dec. 2023). DOI: https://doi.org/10.3390/computers12120257

[72] Steve Kerrison, Jusak Jusak, and Tao Huang. 2023. Blockchain-enabled IoT for rural healthcare: Hybrid-channel communication with digital twinning. *Electronics (Switzerland)* 12, 9 (May 2023). DOI: https://doi.org/10.3390/electronics12092128

[73] Usman Khalil, Owais Ahmed Malik, Mueen Uddin, and Chin Ling Chen. 2022. A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: A comprehensive review, recent advances, and future research directions. *Sensors* 22, 14 (July 2022). DOI: https://doi.org/10.3390/s22145168

[74] Abdullah Ayub Khan, Asif Ali Laghari, Zaffar Ahmed Shaikh, Zdzislawa Dacko-Pikiewicz, and Sebastian Kot. 2022. Internet of things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access* 10 (2022), 122679–122695. DOI: https://doi.org/10.1109/ACCESS.2022.3223370

[75] Imran Khan, Yasar Majib, Rehmat Ullah, and Omer Rana. 2024. Blockchain applications for internet of things – A survey. *Internet of Things (Netherlands)* 27 (Oct. 2024). DOI: https://doi.org/10.1016/j.iot.2024.101254

[76] Misbah Khan, Frank den Hartog, and Jiankun Hu. 2022. A survey and ontology of blockchain consensus algorithms for resource-constrained iot systems. *Sensors* 22, 21 (Nov. 2022). DOI: https://doi.org/10.3390/s22218188

[77] Jing Huey Khor, Michail Sidorov, and Seri Aathira Balqis Zulqarnain. 2023. Scalable lightweight protocol for interoperable public blockchain-based supply chain ownership management. *Sensors* 23, 7 (April 2023). DOI: https://doi.org/10.3390/s23073433

[78] I. D. Kotilevets, I. A. Ivanova, I. O. Romanov, S. G. Magomedov, V. V. Nikonov, and S. A. Pavelev. 2018. Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions. *IFAC-PapersOnLine* 51, 30 693–696. DOI: https://doi.org/10.1016/j.ifacol.2018.11.213

[79] Ajitesh Kumar, Akhilesh Kumar Singh, Ijaz Ahmad, Pradeep Kumar Singh, Anushree, Pawan Kumar Verma, Khalid A. Alissa, Mohit Bajaj, Ateeq Ur Rehman, and Elsayed Tag-Eldin. 2022. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors* 22, 15 (Aug. 2022). DOI: https://doi.org/10.3390/s22155921

[80] Laphou Lao, Zecheng Li, Songlin Hou, Bin Xiao, Songtao Guo, and Yuanyuan Yang. 2020. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *Comput. Surveys* 53, 1 (Jan. 2020). DOI: https://doi.org/10.1145/3372136

[81] Colin Lemahieu. 2018. Nano: A Feeless Distributed Cryptocurrency Network. Retrieved from https://api.semanticscholar.org/CorpusID:52886246

[82] Chenxing Li, Peilun Li, Dong Zhou, Zhe Yang, Ming Wu, Guang Yang, Andrew Chi-Chih Yao, Wei Xu, and Fan Long. 2020. A decentralized blockchain with high throughput and fast confirmation. In *USENIX Annual Technical Conference*. 515–528. Retrieved from https://www.usenix.org/conference/atc20/presentation/li-chenxing. Accessed: 2026-01-12.

[83] Shuzhe Li, Hongwei Xu, Qiong Li, and Qi Han. 2024. Simulation study on the security of consensus algorithms in DAG-based distributed ledger. *Frontiers of Computer Science* 18, 3 (June 2024). DOI: https://doi.org/10.1007/s11704-023-2497-y

[84] Yixin Li, Bin Cao, Mugen Peng, Long Zhang, Lei Zhang, Daquan Feng, and Jihong Yu. 2020. Direct acyclic graph-based ledger for internet of things: Performance and security analysis. *IEEE/ACM Transactions on Networking* 28, 4 (Aug. 2020), 1643–1656. DOI: https://doi.org/10.1109/TNET.2020.2991994

[85] Chunming Liu, Daniel Wang, and Ming Wu. 2018. Vite: A High Performance Asynchronous Decentralized Application Platform. Retrieved from https://chainwhy.com/upload/default/20180808/5f86c200d5b4227d7bed65d308d32538.pdf. Accessed: 2026-01-12.

[86] Yizhong Liu, Jianwei Liu, Marcos Antonio Vaz Salles, Zongyang Zhang, Tong Li, Bin Hu, Fritz Henglein, and Rongxing Lu. 2022. Building blocks of sharding blockchain systems: Concepts, approaches, and open problems. *Computer Science Review* 46 (Nov. 2022). DOI: https://doi.org/10.1016/j.cosrev.2022.100513

[87] Zhiyong Liu and Zipei Li. 2020. A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management* 52 (2020), 102059. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.102059

[88] Xiaofeng Lu and Cheng Jiang. 2023. TEEDAG: A high-throughput distributed ledger based on TEE and directed acyclic graph. *Electronics (Switzerland)* 12, 11 (June 2023). DOI: https://doi.org/10.3390/electronics12112393

[89] J. Maričević, K. Skala, Z. Šojat, J. Mesarić, I. Jerković, V. Bojović, and D. Hofman. 2022. HashNET blockchain consensus for DLT applications. *Current Journal of Applied Science and Technology* (March 2022), 1–12. DOI: https://doi.org/10.9734/cjast/2022/v41i431658

[90] Shikha Mathur, Anshuman Kalla, Gürkan Gür, Manoj Kumar Bohra, and Madhusanka Liyanage. 2023. A survey on role of blockchain for IoT: Applications and technical aspects. *Computer Networks* 227 (May 2023). DOI: https://doi.org/10.1016/j.comnet.2023.109726

[91] Khaleel Mershad and Omar Cheikhrouhou. 2023. Lightweight blockchain solutions: Taxonomy, research progress, and comprehensive review. *Internet of Things (Netherlands)* 24 (Dec. 2023). DOI: https://doi.org/10.1016/j.iot.2023.100984

[92] Dongjun Na and Sejin Park. 2022. IoT-chain and monitoring-chain using multilevel blockchain for IoT security. *Sensors* 22, 21 (Nov. 2022). DOI: https://doi.org/10.3390/s22218271

[93] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf. Accessed: 2026-01-12.

[94] Clement Nartey, Eric Tutu Tchao, James Dzisi Gadze, Eliel Keelson, Griffith Selorm Klogo, Benjamin Kommey, and Kwasi Diawuo. 2021. On blockchain and IoT integration platforms: Current implementation challenges and future perspectives. *Wireless Communications and Mobile Computing* 2021 (2021). DOI: https://doi.org/10.1155/2021/6672482

[95] U.S. Census Bureau News. 2025. *QUARTERLY RETAIL E-COMMERCE SALES 1 st QUARTER 2025*. Technical Report. U.S. Department of Commerce. Retrieved from https://www.census.gov/retail/ecommerce.html. Accessed: 2026-01-12.

[96] Lam Duc Nguyen, Arne Bröring, Massimo Pizzol, and Petar Popovski. 2022. Analysis of distributed ledger technologies for industrial manufacturing. *Scientific Reports* 12, 1 (Dec. 2022). DOI: https://doi.org/10.1038/s41598-022-22612-3

[97] Liwei Ouyang, Wenwen Zhang, and Fei Yue Wang. 2022. Intelligent contracts: Making smart contracts smart for blockchain intelligence. *Computers and Electrical Engineering* 104 (Dec. 2022). DOI: https://doi.org/10.1016/j.compeleceng.2022.108421

[98] Houshyar Honar Pajooh, Mohammad Rashid, Fakhrul Alam, and Serge Demidenko. 2021. Hyperledger fabric blockchain for securing the edge internet of things. *Sensors (Switzerland)* 21, 2 (Jan. 2021), 1–29. DOI: https://doi.org/10.3390/s21020359

[99] Seongjoon Park and Hwangnam Kim. 2019. Dag-based distributed ledger for low-latency smart grid network. *Energies* 12, 18 (Sept. 2019). DOI: https://doi.org/10.3390/en12183570

[100] Alberto Partida, Regino Criado, and Miguel Romance. 2021. Identity and access management resilience against intentional risk for blockchain-based IOT platforms. *Electronics (Switzerland)* 10, 4 (Feb. 2021), 1–26. DOI: https://doi.org/10.3390/electronics10040378

[101] Lorenzo Petrosino, Giordano Pescetelli, Quirino Fieramosca, Stefano Della Valle, Mario Merone, and Luca Vollero. 2023. dRAIN: A distributed reliable architecture for IoT networks. *IEEE Internet of Things Journal* (Jan. 2023). DOI: https://doi.org/10.1109/JIOT.2023.3290822

[102] Alessandra Pieroni, Noemi Scarpato, and Lorenzo Felli. 2020. Blockchain and IoT convergence–a systematic survey on technologies, protocols and security. *Applied Sciences (Switzerland)* 10, 19 (Oct. 2020), 1–23. DOI: https://doi.org/10.3390/app10196749

[103] Serguei Popov. 2015. The Tangle. Retrieved from https://api.semanticscholar.org/CorpusID:4958428

[104] Hossein Pourrahmani, Adel Yavarinasab, Amir Mahdi Hosseini Monazzah, and Jan Van herle. 2023. A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. *Internet of Things (Netherlands)* 23 (Oct. 2023). DOI: https://doi.org/10.1016/j.iot.2023.100888

[105] Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das. 2018. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine* 7, 4 (July 2018), 6–14. DOI: https://doi.org/10.1109/MCE.2018.2816299

[106] Youyang Qu, Md Palash Uddin, Chenquan Gan, Yong Xiang, Longxiang Gao, and John Yearwood. 2022. Blockchain-enabled federated learning: A survey. *Comput. Surveys* 55, 4 (Nov. 2022). DOI: https://doi.org/10.1145/3524104

[107] Heena Rathore, Abhay Samant, and Murtuza Jadliwala. 2021. TangleCV: A distributed ledger technique for secure message sharing in connected vehicles. *ACM Transactions on Cyber-Physical Systems* 5, 1 (Jan. 2021). DOI: https://doi.org/10.1145/3404500

[108] B. Swaroopa Reddy and G. V. V. Sharma. 2020. Scalable Consensus Protocols for PoW based Blockchain and blockDAG. Retrieved from http://arxiv.org/abs/2010.05447

[109] Iraq Ahmad Reshi and Sahil Sholla. 2023. The blockchain conundrum: An in-depth examination of challenges, contributing technologies, and alternatives. *Concurrency and Computation: Practice and Experience* (2023). DOI: https://doi.org/10.1002/cpe.7987

[110] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. 2018. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems* 88 (Nov. 2018), 173–190. DOI: https://doi.org/10.1016/j.future.2018.05.046

[111] Alia Al Sadawi, Mohamed S. Hassan, and Malick Ndiaye. 2021. A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. *IEEE Access* 9 (2021), 54478–54497. DOI: https://doi.org/10.1109/ACCESS.2021.3070555

[112] Shreya Girish Savadatti, Shruthi Krishnamoorthy, and Radhakrishnan Delhibabu. 2025. Survey of distributed ledger technology (DLT) for secure and scalable computing. *IEEE Access* (2025). DOI: https://doi.org/10.1109/ACCESS.2025.3528211

[113] Meryem Cherkaoui Semmouni, Abderrahmane Nitaj, Mostafa Belkasmi, and Mostafa Belkasmi Bitcoin Security. 2019. Bitcoin security with a twisted edwards curve. *Journal of Discrete Mathematical Sciences and Cryptography* 25, 2 (2019), 353–371. DOI: https://doi.org/10.1080/09720529.2019.1681673

[114] Aashima Sharma, Sanmeet Kaur, and Maninder Singh. 2023. A secure blockchain framework for the internet of medical things. *Transactions on Emerging Telecommunications Technologies* (Jan. 2023). DOI: https://doi.org/10.1002/ett.4917

[115] Wellington Fernandes Silvano and Roderval Marcelino. 2020. Iota tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Generation Computer Systems* 112 (Nov. 2020), 307–319. DOI: https://doi.org/10.1016/j.future.2020.05.047

[116] Amritraj Singh, Kelly Click, Reza M. Parizi, Qi Zhang, Ali Dehghantanha, and Kim Kwang Raymond Choo. 2020. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications* 149 (Jan. 2020). DOI: https://doi.org/10.1016/j.jnca.2019.102471

[117] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. 2016. SPECTRE: Serialization of proof-of-work events: Confirming transactions via recursive elections. *Cryptology ePrint Archive* (2016). Issue 1159. Retrieved from https://eprint.iacr.org/2016/1159

[118] Denis Stefanescu, Leticia Montalvillo, Patxi Galan-Garcia, Juanjo Unzilla, and Aitor Urbieta. 2022. A systematic literature review of lightweight blockchain for IoT. *IEEE Access* 10 (2022), 123138–123159. DOI: https://doi.org/10.1109/ACCESS.2022.3224222

[119] Haoli Sun, Song Hua, Ence Zhou, Bingfeng Pi, Jun Sun, and Kazuhiro Yamashita. 2018. Using ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10974 LNCS, 3–17. DOI: https://doi.org/10.1007/978-3-319-94478-4_1

[120] Meng Sun, Yuteng Lu, Yichun Feng, Qi Zhang, and Shaoying Liu. 2021. Modeling and verifying the CKB blockchain consensus protocol. *Mathematics* 9, 22 (Nov. 2021). DOI: https://doi.org/10.3390/math9222954

[121] Yu Tang, Jiawen Yan, Chinmay Chakraborty, and Yi Sun. 2023. Hedera: A permissionless and scalable hybrid blockchain consensus algorithm in multiaccess edge computing for IoT. *IEEE Internet of Things Journal* 10, 24 (Dec. 2023), 21187–21202. DOI: https://doi.org/10.1109/JIOT.2023.3279108

[122] The IoTeX Team. 2018. IoTeX A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain. Retrieved from https://github.com/iotexproject/files/blob/main/publications/IoTeX_Whitepaper_1.5_EN.pdf. Accessed: 2026-01-12.

[123] The IoTeX Team. 2024. IoTeX 2.0-DePIN for Everyone! Retrieved from https://cdn.iotex.io/whitepaper/iotex-2.0-whitepaper.pdf. Accessed: 2026-01-12.

[124] Toyota Motor Corporation. [n. d.]. Toyota Production System. Retrieved from https://global.toyota/en/company/vision-and-philosophy/production-system/. Accessed: 2026-01-12.

[125] Toyota Motor Corporation. 2025. Sales, production, and export results for 2024 (January - December). Retrieved from https://global.toyota/en/company/profile/production-sales-figures/202412.html. Accessed: 2026-01-12.

[126] Nguyen Khoi Tran, M. Ali Babar, and Jonathan Boan. 2021. Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. *Journal of Network and Computer Applications* 173 (Jan. 2021). DOI: https://doi.org/10.1016/j.jnca.2020.102844

[127] Lionel Sujay Vailshery. 2025. Number of IoT connections worldwide 2022-2034. Retrieved from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Accessed: 2026-01-12.

[128] Qin Wang, Jiangshan Yu, Shiping Chen, and Yang Xiang. 2023. SoK: DAG-based blockchain systems. *Comput. Surveys* 55, 12 (March 2023). DOI: https://doi.org/10.1145/3576899

[129] Shangping Wang, Huan Li, Juanjuan Chen, Jifang Wang, and Yingjuan Deng. 2022. DAG blockchain-based lightweight authentication and authorization scheme for IoT devices. *Journal of Information Security and Applications* 66 (May 2022). DOI: https://doi.org/10.1016/j.jisa.2022.103134

[130] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. 2019. Survey on blockchain for internet of things. *Computer Communications* 136 (Feb. 2019), 10–29. DOI: https://doi.org/10.1016/j.comcom.2019.01.006

[131] Huan Yu Wu, Xin Yang, Chentao Yue, Hye Young Paik, and Salil S. Kanhere. 2022. Chain or DAG? underlying data structures, architectures, topologies and consensus in distributed ledger technology: A review, taxonomy and research issues. *Journal of Systems Architecture* 131 (Oct. 2022). DOI: https://doi.org/10.1016/j.sysarc.2022.102720

[132] Feng Xia, Li Kaiye, Wu Songze, and Xin yan. 2023. Enhancing the blockchain interoperability through federated learning with directed acyclic graph. *IET Blockchain* 3, 4 (Dec. 2023), 238–248. DOI: https://doi.org/10.1049/blc2.12033

[133] Kaile Xiao, Zhipeng Gao, Weisong Shi, Xuesong Qiu, Yang Yang, and Lanlan Rui. 2020. EdgeABC: An architecture for task offloading and resource allocation in the Internet of Things. *Future Generation Computer Systems* 107 (June 2020), 498–508. DOI: https://doi.org/10.1016/j.future.2020.02.026

[134] Rongxin Xu, Qiujun Lan, Shiva Raj Pokhrel, and Gang Li. 2023. A knowledge graph-based survey on distributed ledger technology for IoT verticals. *Comput. Surveys* 56, 2 (Sept. 2023). DOI: https://doi.org/10.1145/3609503

[135] He Xue, Dajiang Chen, Ning Zhang, Hong-Ning Dai, and Keping Yu. 2023. Integration of blockchain and edge computing in internet of things: A survey. *Future Generation Computer Systems* 144 (July 2023), 307–326. DOI: https://doi.org/10.1016/j.future.2022.10.029

[136] Anatoly Yakovenko. 2018. Solana: A new architecture for a high performance blockchain v0.8.13. Retrieved from https://api.semanticscholar.org/CorpusID:44155214

[137] Wenli Yang, Erfan Aghasian, Saurabh Garg, David Herbert, Leandro Disiuta, and Byeong Kang. 2019. A survey on blockchain-based internet service architecture: Requirements, challenges, trends, and future. *IEEE Access* 7 (2019), 75845–75872. DOI: https://doi.org/10.1109/ACCESS.2019.2917562

[138] Chong Ye, Wenting Cao, and Shijun Chen. 2021. Security challenges of blockchain in Internet of things: Systematic literature review. *Transactions on Emerging Telecommunications Technologies* 32, 8 (Aug. 2021). DOI: https://doi.org/10.1002/ett.4177

[139] Kimchai Yeow, Abdullah Gani, Raja Wasim Ahmad, Joel J. P. C. Rodrigues, and Kwangman Ko. 2018. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access* 6 (Feb. 2018), 1513–1524. DOI: https://doi.org/10.1109/ACCESS.2017.2779263

[140] Yonatan, Zohar Aviv Lewenberg Yoad, and Sompolinsky. 2015. Inclusive block chain protocols. In *Financial Cryptography and Data Security* (Berlin, Heidelberg), Tatsuaki Böhme Rainer and Okamoto (Eds.). Springer Berlin, 528–547.

[141] Chao Yu, Wenke Yang, Feiyu Xie, and Jianmin He. 2022. Technology and security analysis of cryptocurrency based on blockchain. *Complexity* 2022 (2022). DOI: https://doi.org/10.1155/2022/5835457

[142] Guangsheng Yu, Xu Wang, Caijun Sun, Qin Wang, Ping Yu, Wei Ni, and Ren Ping Liu. 2023. IronForge: An open, secure, fair, decentralized federated learning. *IEEE Transactions on Neural Networks and Learning Systems* (2023), 1–15. DOI: https://doi.org/10.1109/TNNLS.2023.3329249

[143] S. Zafar, K. M. Bhatti, M. Shabbir, F. Hashmat, and A. H. Akbar. 2022. Integration of blockchain and Internet of Things: Challenges and solutions. *Annales des Telecommunications/Annals of Telecommunications* 77, 1-2 (Feb. 2022), 13–32. DOI: https://doi.org/10.1007/s12243-021-00858-8

[144] Xiaodong Zhang, Ru Li, and Hui Zhao. 2023. A parallel consensus mechanism using PBFT based on DAG-lattice structure in the internet of vehicles. *IEEE Internet of Things Journal* 10, 6 (March 2023), 5418–5433. DOI: https://doi.org/10.1109/JIOT.2022.3222217

[145] Zixi Zhang, Mingxia Zhang, Yu Li, Bo Fan, and Li Jiang. 2023. Directed acyclic graph blockchain for secure spectrum sharing and energy trading in power IoT. *China Communications* 20, 5 (May 2023), 182–197. DOI: https://doi.org/10.23919/JCC.2023.00.013

[146] Xiaochen Zheng, Shengjing Sun, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaquín Ordieres-Meré. 2019. Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. *Journal of Medical Internet Research* 21, 6 (June 2019). DOI: https://doi.org/10.2196/13583

[147] Qingyi Zhu, Seng W. Loke, Rolando Trujillo-Rasua, Frank Jiang, and Yong Xiang. 2019. Applications of distributed ledger technologies to the internet of things: A survey. *Comput. Surveys* 52, 6 (Nov. 2019). DOI: https://doi.org/10.1145/3359982

[148] Hakan Şimşek and İrem Güvendiren. 2023. Soft computing based e-commerce website service quality index measurement. *Electronic Commerce Research and Applications* 61 (Sept. 2023). DOI: https://doi.org/10.1016/j.elerap.2023.101303

Appendix

A Full Scoring Data

Table 12. Weighted Scores of All DLT Platforms

DLT platform	TPS	TTF	Consensus Mechanism	Cryptography Features	Feeless Transaction	Potential Integration	Weighted Score
Nano	7	7	5	5	3	3	5
IoTeX	7	7	5	3	1	5	4.8
Iota Tangle	7	3	7	5	3	5	4.8
Hedera	7	5	5	5	1	5	4.6
Hyperledger Fabric	7	3	5	3	3	5	4.4
Aleph Zero	7	7	5	7	1	1	4.4
SUI	7	7	3	5	1	1	4
Fantom	7	5	5	3	1	3	4
Vite	7	5	3	5	3	1	4
IoT-Chain	7	3	5	7	1	1	3.6
Solana	7	3	3	5	1	3	3.6
TeeDAG	7	1	7	3	1	3	3.4
Tempo (Radix)	7	1	7	3	1	3	3.4
COTI	7	5	3	3	1	1	3.4
Tolar (HashNet)	7	5	3	3	1	1	3.4
Conflux	7	3	3	3	1	3	3.4
VeChain	3	3	7	3	1	3	3
Nervos	7	3	1	3	1	1	2.8
BlockDAG	7	1	1	3	1	3	2.8
Ethereum	1	1	3	3	1	5	2.2
Byteball (Obyte)	1	1	7	3	1	3	2.2
Elastos	1	3	1	3	1	3	2
CoDAG	3	1	1	3	1	3	2
Spectre	1	3	1	3	1	3	2
Bitcoin	1	1	1	3	1	1	1.2
CyberVein	1	1	1	3	1	1	1.2
Phantasm	1	1	1	3	1	1	1.2

Received 4 December 2024; revised 2 December 2025; accepted 8 January 2026