Electrical Power and Energy Systems 173 (2025) 111286

Contents lists available at ScienceDirect

International Journal of Electrical Power and Energy Systems

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

Review

Integrated blockchain and federated learning for the cybersecurity of distributed energy resources

Oluleke O. Babayomi [a], Ikechi Saviour Igboanusi [a], Love Allen Chijioke Ahakonye [a], Dong-Seong Kim [b,c,*]

[a] ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, Republic of Korea
[b] Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, Republic of Korea
[c] NSLab Co. Ltd., Gumi, Republic of Korea

ARTICLE INFO

Keywords:
Blockchain
Cyber security
Federated learning
Distributed energy resources
Distributed learning
Smart grid

ABSTRACT

Blockchain and federated learning have emerged as complementary technologies for decentralized, privacy-preserving intelligent and secure management of sustainable distributed energy resources. This paper reviews the integration of blockchain technology with federated learning as an emerging approach to enhance the resilience of distributed energy resources against evolving cyber threats. First, a foundational four-layer cybersecurity framework is introduced for distributed energy resources' device, firmware, cyber network and management application layers. Second, ten recent integrated blockchain and federated learning architectures are analyzed and categorized according to their functional layers and cyber security lifecycle stages. These architectures are systematically analyzed with respect to the following indices, to facilitate their selection for practical deployment: latency, security, scalability, throughput, energy consumption, complexity, and fault tolerance. Furthermore, critical challenges and emerging future research directions are also identified, such as quantum-safe multi-chain systems and quantum-resilient cryptography. Performance evaluation demonstrates that resource-efficient architectures optimize latency and energy consumption, and security-maximized architectures prioritize data protection at computational trade-offs. This review concludes that integrated blockchain and federated learning is a promising solution for secure, reliable and scalable next-generation smart grids.

Contents

* Corresponding author.
E-mail address: dskim@kumoh.ac.kr (D.-S. Kim).

https://doi.org/10.1016/j.ijepes.2025.111286
Received 23 July 2025; Received in revised form 25 September 2025; Accepted 15 October 2025
Available online 25 November 2025

1. Introduction

As global energy systems transition toward decentralization and decarbonization, distributed energy resources (DERs) are becoming foundational to modern smart grids [1]. DERs, including solar photovoltaics, wind turbines, energy storage systems, electric vehicles, and controllable loads, offer unprecedented flexibility and efficiency but simultaneously introduce complex cybersecurity challenges that threaten grid reliability and stability. Traditional centralized and reactive security approaches prove inadequate for protecting these inherently distributed systems, which operate across heterogeneous networks with diverse ownership structures and varying levels of computational capacity [2,3]. The cybersecurity landscape for DERs is particularly concerning given their critical role in power system operations [4]. Successful attacks can cascade from compromised individual devices to wide-scale system disruptions, potentially resulting in physical damage, service interruptions, financial losses, and even public safety risks [5].

The attack surface spans multiple layers: from hardware-level vulnerabilities in sensors and control units to firmware manipulation, network-level intrusions, and application-layer attacks targeting DER management systems (DERMS) [6]. DERMS is a software platform that centrally manages, monitors, and optimizes distributed energy resource operations through real-time data analytics and automated control algorithms. DERMS represents a critical cybersecurity asset due to its oversight of grid stability and energy market participation. Recent incidents have demonstrated attackers' growing sophistication, using techniques like false data injection, denial of service attacks, spoofing, and adversarial machine learning to compromise DER operations.

In recent times, two emerging technologies that address these challenges have gained significant attention in the research community: blockchain and federated learning (FL). Blockchain technology has emerged as a promising solution for establishing trust in decentralized systems through immutable distributed ledgers and consensus mechanisms [8]. Its ability to provide tamper-proof record-keeping, transparent yet privacy-preserving transactions, and smart contract-based automation aligns well with DER security requirements. Concurrently, FL has revolutionized distributed intelligence by enabling collaborative model training without raw data sharing [10,11], allowing DER devices to collectively develop detection and forecasting models while preserving data privacy [9].

Despite their advantages, blockchain and FL have weaknesses that limit their applications to DER systems. The high energy consumption of popular blockchain consensus techniques make them unsuitable for sustainable energy grids [12]. Also, blockchain's limited transaction throughput rate increases latency in real-time DER applications operating at low sampling intervals of microseconds [13]. Similarly, FL is vulnerable to model poisoning from dishonest clients who can maliciously update incorrect model parameters to compromise the global model [14]. Also, the global model generated by the FL algorithm improves with participation of more clients.

To overcome the challenges associated with these technologies, the integration of blockchain and federated learning, termed BlockFL in this paper, has been proposed in the literature [15]. BlockFL represents a synergistic approach that leverages the strengths of each technology while mitigating their respective weaknesses [16]. For instance, the high energy consumption of proof-of-work blockchain consensus mechanisms, particularly problematic in energy systems designed for efficiency, is reduced by FL's approach of keeping computation off-chain. This enables even small solar installations to participate in collaborative learning without excessive energy overhead. Similarly, blockchain mitigates model poisoning in FL by creating immutable logs of training updates and using consensus mechanisms to filter anomalies. For solar PV forecasting systems, this means weather data and generation predictions from multiple distributed sites can be validated before integration into grid management models, preventing manipulated forecasts that could destabilize energy markets.

Previous related review publications fall into three categories: DER cybersecurity in general, blockchain for smart grid-related applications, and FL for DER and smart grid privacy. Authors in [2,6] explored general cybersecurity topics and challenges in DERMS, such as architectures, communication protocols, and mitigation methods against different cyber attacks. Different blockchain solutions for grid decentralization, energy trading and energy optimization were systematically reviewed in [1,7,8]. The advancements in FL-based smart grids for generation, transmission, distribution and consumer nodes were reviewed in [9]. However, these papers lack a comprehensive review on the applications of integrated blockchain and federated learning to DER cyber security. Also, they neither provide a mapping of these technologies to the appropriate hierarchy and cybersecurity lifecycle of DERs, nor show how they improve cyber-resilience at distinctive DER levels/lifecycles. This research gap, shown in Table 1 motivated the study reported in this paper.

Therefore, this review paper makes several important contributions to the field. First, it synthesizes current knowledge on blockchain and FL applications in DER contexts, providing researchers and practitioners with a consolidated view of the state of the art. Second, it analyzes and categorizes ten promising BlockFL architectural approaches, highlighting their operational features, advantages, and limitations. These architectures were selected from journal and international conference publications indexed on Scopus and Web of Science. Third, the study systematically reviews recent implementations across various DER use cases, evaluating their performance, security benefits, and practical limitations. BlockFL for smart grid DER technologies are covered, including electric vehicles, virtual power plants, energy trading and microgrids, renewable energy systems, and energy internet. It was observed that while the theoretical benefits of BlockFL for DERs are compelling, their practical implementation is still an emerging area, with most current efforts focused on proof-of-concept demonstrations and simulations to validate technical feasibility. Finally, the study identifies persistent challenges and emerging trends that will shape future research directions in this rapidly evolving field.

The remainder of this paper is organized as follows (see Fig. 1): Section 2 introduces fundamental concepts of blockchain and FL for DERs; Section 3 presents a framework for analyzing DER cybersecurity across four architectural layers and five lifecycle stages; Section 4 provides a comprehensive overview of BlockFL architectures identified in the literature; Section 5 examines recent advances in BlockFL implementations for DER cybersecurity with case studies; Section 6 discusses challenges and future research directions and Section 7 summarizes the findings of the paper.

2. State of the art on non-integrated blockchain and distributed learning for DERs

This section introduces fundamental concepts on blockchain and FL which are necessary for comprehension of the rest of the paper. Also, the state of the art on blockchain and distributed learning for DER systems are covered.

Table 1
Contribution of this study relative to related state-of-the-art.

Reference	Year	DER security	DER hierarchies	Blockchain	Federated learning	Security lifecycle	BlockFL resilience
[1]	2020	✓	–	✓	–	–	–
[7]	2021	✓	–	✓	–	–	–
[8]	2023	✓	–	✓	–	–	–
[9]	2024	✓	–	–	✓	–	–
[2]	2025	✓	✓	–	–	–	–
[6]	2025	✓	–	–	–	–	–
This paper	TBD	✓	✓	✓	✓	✓	✓

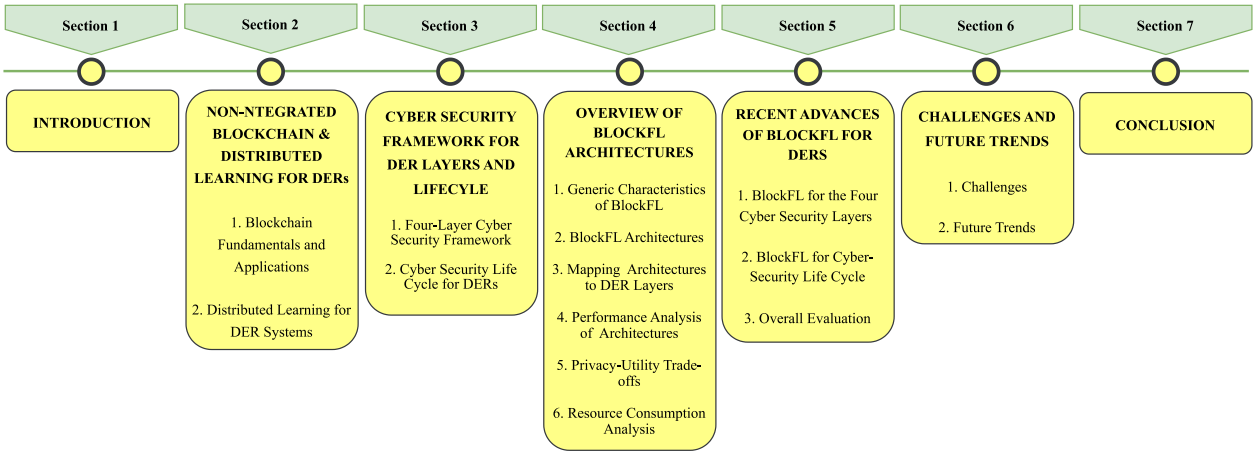

Fig. 1. Organization of the article.

2.1. Article selection methodology

The systematic search employed in this study covered major databases using keywords: "blockchain federated learning", "smart grid", "distributed energy resources", "smart grid security", and "privacy-preserving energy systems". From an initial pool of 150+ papers, the study applied systematic selection criteria to identify the most relevant and technically comprehensive architectures. The selection criteria included relevance to DER applications, focusing on architectures specifically designed for distributed energy resource management, smart grids, or energy trading systems. Recency was prioritized by selecting publications from 2020–2025 to capture the most recent developments in this rapidly evolving field. Technical completeness was ensured by selecting architectures with sufficient detail regarding blockchain integration, federated learning mechanisms, and cybersecurity considerations. This study emphasizes cybersecurity focus by including solutions that explicitly address one or more aspects of the four-layer cybersecurity framework encompassing device, firmware, cyber network, and management application layers. Diversity of approaches was maintained through representative coverage of different integration strategies including blockchain as aggregator, smart contract-controlled training, hierarchical structures, and cross-chain implementations. Finally, the research required performance evaluation capabilities, selecting architectures with available performance metrics or sufficient detail to enable comparative analysis across the evaluation indices. Several architectures were excluded due to limited applicability to DER systems, insufficient technical detail, theoretical proposals without implementation frameworks, redundancy with selected architectures, or publication dates outside the target timeframe.

2.2. Blockchain fundamentals and applications

At its core, a blockchain is a distributed, immutable, and transparent digital ledger. Instead of residing on a single central server, copies of the ledger are maintained across numerous computers (nodes) in a network. Transactions are grouped into blocks, and each new block is cryptographically linked to the previous one, forming a chain. This structure, combined with cryptographic principles, makes altering past records computationally infeasible, ensuring data integrity [17]. Key concepts underpinning blockchain relevant to DERMS include:

2.2.1. Basic principles of blockchain technology

Decentralization. Unlike traditional centralized databases controlled by a single entity, blockchain networks distribute data and control across multiple participants. This eliminates single points of failure and reduces reliance on central intermediaries for validation. In the context of DERMS, this means data related to energy generation, consumption, or grid status can be shared and verified by multiple authorized parties without needing a central utility or aggregator to act as the sole gatekeeper for all information [18,19].

Consensus mechanisms. To ensure all nodes in the distributed network agree on the validity of new transactions and the state of the ledger, blockchains employ consensus mechanisms. These are protocols that nodes follow to reach an agreement. Common mechanisms include (see Table 2):

(i) *Proof-of-Work (PoW):* Used by Bitcoin, PoW requires nodes (miners) to solve complex computational puzzles to validate transactions and add new blocks. While highly secure against certain attacks, it is notoriously energy-intensive and can have low transaction throughput [20].
(ii) *Proof-of-Stake (PoS):* Validators are chosen to create new blocks based on the number of tokens they "stake" or lock up as collateral. PoS is significantly more energy-efficient than PoW and often allows for faster transaction speeds. Various forms of PoS exist, each with different security and performance trade-offs [21].
(iii) *Practical Byzantine Fault Tolerance (PBFT):* A consensus algorithm designed for faster performance in permissioned (non-public) networks. It relies on a specific number of nodes agreeing before a transaction is validated, offering high throughput and

Table 2
Comparison of blockchain consensus mechanisms for DERMS.

Feature	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	PBFT	Suitability for DERMS
Mechanism	Solving puzzles	Validators stake tokens	Voting among validators	Varies based on use case/network type
Energy Consumption	Very High	Low to Moderate	Low	PoS/PBFT preferred for energy context
Transaction Speed	Low	Moderate to High	High	PoS/PBFT better for real-time needs
Scalability	Low	Moderate to High	High (known validators)	PoS/PBFT offer better potential
Security Model	Computational power	Economic incentives (stake)	Tolerates <= 1/3 faulty nodes	All robust, different attack vectors
Permissioning	Typically Public	Public or Permissioned	Typically Permissioned	Permissioned variants often favored

low latency but requiring a known set of participants [22,23]. Other mechanisms like Proof of Authority (PoA) or delegated versions of PoS also exist, often tailored for specific network requirements. The choice of consensus mechanism significantly impacts a blockchain's performance, energy consumption, and security model, making it a critical design decision for DERMS applications.

Smart contracts. These are self-executing contracts with the terms of the agreement directly written into code. They run on the blockchain and automatically execute predefined actions when specific conditions are met, without the need for intermediaries [24]. For DERMS, smart contracts can automate processes like:

(i) Executing peer-to-peer energy trades when generation and consumption data match agreed terms.
(ii) Automatically disbursing payments for grid services provided by DERs.
(iii) Managing access rights for EV charging stations based on payment confirmation.
(iv) Enforcing demand-response agreements automatically when grid signals are received.

2.2.2. Public, private and consortium blockchains

The governance model and accessibility of a blockchain are crucial considerations for its application in the energy sector (see Table 3):

Public blockchains. Anyone can join, view the ledger, and participate in the consensus process (if applicable, like PoW mining) of Bitcoin and Ethereum, for instance. They offer high transparency and censorship resistance but often suffer from lower transaction speeds, higher costs, and potential privacy concerns for sensitive energy data [25]. Their permissionless nature might be unsuitable for critical infrastructure management.

Private blockchains. Access and participation are controlled by a single organization. They offer high speed, scalability, and privacy, as only authorized nodes can validate transactions or view data. Suitable for internal processes within a utility or a single entity managing its DER assets, but lack the inherent trust benefits for multi-stakeholder collaboration [26].

Consortium blockchains. Governed by a pre-selected group of organizations (e.g., multiple utilities, regulators, aggregators). Participants are permissioned, meaning their identities are known. This model strikes a balance between the trust and transparency needs of multi-party systems and the performance and privacy requirements of the energy sector. It allows collaborating entities to share a trusted ledger while maintaining control over who can participate and access specific data [27,28]. Consortium blockchains are often considered the most promising type for complex DERMS implementations involving diverse stakeholders.

2.2.3. Blockchain scalability limitations and solutions

While blockchain technology offers a robust framework for decentralized and secure DER management, its practical implementation is hindered by inherent scalability limitations. The core challenge stems from the blockchain trilemma, which suggests that a network cannot simultaneously optimize for decentralization, security, and scalability [29]. For DER applications, which can involve thousands of high-frequency transactions from devices like solar inverters, smart meters, and electric vehicles, the low transaction throughput (Transactions Per Second, or TPS) and high latency of foundational blockchains present a significant bottleneck. For instance, while Bitcoin and Ethereum can only handle approximately 7 TPS and 15–30 TPS, respectively [30], a large-scale DER system might require a capacity of thousands of TPS for real-time market operations and grid management. This disparity makes many standard blockchain architectures unsuitable for time-sensitive DER control and trading applications.

To address these limitations, several scaling solutions have been proposed, which can be broadly categorized into Layer-2 solutions and other architectural techniques.

(i) *Layer-2 Scaling Solutions:* These are protocols built atop a primary (Layer-1) blockchain. They process the bulk of transactions off-chain, leveraging the main chain primarily for security and final settlement [31].

  (a) State Channels: State channels create a private, off-chain transaction channel between two or more participants [32]. For DERs, a prosumer and a local utility could open a channel, conduct numerous micro-transactions for energy trading off-chain with near-instant finality, and only record the net settlement on the main blockchain when the channel is closed. This drastically reduces the transactional load on the main chain.
  (b) Rollups: Rollups improve scalability by bundling or "rolling up" hundreds of off-chain transactions into a single, compressed transaction that is submitted to the main chain
  [33]. Optimistic Rollups assume the bundled transactions are valid and rely on a dispute resolution period where "fraud proofs" can be submitted. In contrast, Zero-Knowledge (ZK) Rollups use cryptographic validity proofs (such as ZK-SNARKs) to verify every transaction bundle instantly, offering higher security and faster finality [33].

(ii) *Other Scaling Techniques:* Alongside Layer-2 solutions, modifications to the base-layer protocol can also enhance scalability.

  (a) Sharding: This technique partitions a blockchain network into smaller, parallel chains known as "shards". Each shard processes its own set of transactions and smart contracts, allowing the network to handle multiple transactions simultaneously [34]. This parallel processing capability significantly increases the overall network throughput.
  (b) Alternative Consensus Mechanisms: The choice of consensus mechanism critically impacts a blockchain's performance and energy consumption. Moving away from energy-intensive and slow mechanisms like Proof-of-Work (PoW) is a key strategy for DER applications. More efficient alternatives like Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) offer higher transaction speeds, lower latency, and significantly reduced energy

Table 3
Comparison of blockchain types for DERs.

Feature	Public blockchain	Private blockchain	Consortium blockchain	Suitability for DERMS
Access	Permissionless (Anyone can join)	Permissioned (Single organization control)	Permissioned (Governed by a group of organizations)	Consortium or Private generally preferred for control and privacy requirements.
Governance	Decentralized via community or code protocol	Centralized control by the single owning organization	Semi-Decentralized control by the governing group of members	Consortium model aligns well with the multi-stakeholder reality of DERMS.
Speed	Generally Slow transaction throughput	High speed and scalability potential	High speed and scalability potential	Private or Consortium types better suited for performance needs in energy systems.
Privacy	Transparent ledger (Pseudonymous identities)	High privacy via controlled data access	High privacy with configurable access controls amongst members	Private or Consortium offer better data confidentiality for sensitive energy data.
Trust Model	Trust primarily in the underlying code/protocol	Trust placed in the single owning organization	Trust established among the consortium members via governance	Consortium provides a robust framework for inter-organizational trust without a central intermediary.

consumption, making them better suited for the real-time needs of energy systems [35]. Purechain [36,37] used the Proof of Authority and Association (PoA^2) consensus algorithm [38], which is a tuned version of the PoA consensus and pairing it with the Smart Auto Mining (SAM) [39] algorithm to achieve high TPS.

By integrating these advanced scaling solutions, blockchain can better meet the demanding performance requirements of large-scale DER management systems, making it a more viable and efficient platform for the future smart grid.

2.2.4. Blockchain applications and challenges in DERs

The unique characteristics of blockchain enable several promising applications within the DER management system landscape, transforming how energy is traded, managed, and accounted for. Blockchain platforms with smart contracts automate market systems where energy generated by DERs (e.g., solar PV) can be securely traded directly between producers and consumers—within a local distribution network or microgrid [40,41]. They also provide secure auditable ledgers for data sharing in DER systems [42,43]: internet of things (IoT) sensors monitoring grid conditions, smart meters measuring consumption/generation, EV chargers reporting status and energy usage, battery systems indicating state-of-charge, and weather forecasts predicting renewable generation.

Despite these promising features of blockchain to DER management systems, many current blockchain platforms have limited transaction throughput (Transactions Per Second, TPS). For example, Bitcoin handles $\approx$ 7 TPS, while Ethereum handles $\approx$ 15–30 TPS [13]. Real-time energy management and market operations might require handling thousands TPS, especially with large numbers of DERs sending frequent data updates or participating in high-frequency trading. Meanwhile, newer consensus mechanisms (like PoS, PBFT) and Layer-2 scaling solutions (e.g., state channels, sidechains) are being developed to address this. Nonetheless, achieving the required performance for large-scale, real-time DER management systems remains an active research area [18,38,44]. Also, the high energy consumption associated with PoW consensus mechanisms can be a major obstacle to energy-efficient clean energy transition [12]. Other limitations include the poor interoperability of new blockchain platforms with legacy energy systems [45], regulatory uncertainty [46], and high investment cost [47].

2.3. Distributed learning for DER systems

Distributed learning enables the training of machine learning models across multiple devices or nodes, facilitating decentralized data processing and decision-making [48]. In smart energy management, it optimizes energy usage by integrating data from smart meters, sensors, and Internet of Things (IoT) devices [49]. Multi-agent reinforcement learning (MARL) enhances energy coordination in smart communities, optimizing energy use across buildings to reduce costs and balance demand more effectively [50]. Distributed energy resource management systems (DERMS) utilize distributed learning to manage resources such as solar panels, battery storage, and electric vehicles, thereby improving energy distribution and grid reliability. Machine learning algorithms in DERMS enable dynamic scheduling, enhancing energy utilization and minimizing waste by adapting to changes in demand [50,51].

Centralized machine learning, while effective, faces limitations in smart energy management, such as inefficiency in handling large data volumes from smart meters, sensors, and IoT devices [52]. It incurs high data transmission costs and raises privacy concerns due to the need for sharing sensitive data with a central server [52]. Additionally, centralized systems struggle with scalability, as they can be overwhelmed by diverse and distributed data sources from multiple buildings and devices [53]. FL mitigates the limitations of centralized systems by keeping data on local devices and enabling collaborative model training across distributed nodes [54]. This reduces communication overhead, ensures data privacy, and enhances scalability, making it well-suited for applications like DERMS, which require real-time, decentralized decision-making [55].

2.3.1. Decentralized learning

Decentralized learning is becoming an essential tool for managing the complexities of modern energy systems [56]. Several studies have explored its potential in smart energy management [57]. One framework uses reinforcement learning to optimize decentralized energy systems, improving scalability and robustness while balancing supply and demand and reducing reliance on external energy sources [57,58]. Another study introduces the SmartGrid AI platform, which combines deep reinforcement learning and neural networks to optimize energy consumption, predict demand, and enable peer-to-peer energy trading, resulting in reduced energy costs and increased utilization of renewable energy [59]. Additionally, blockchain and FL have been proposed to enhance the security, efficiency, and scalability of decentralized energy management systems [60,61].

The increasing adoption of renewable energy sources and DERs has made power grids more dynamic, rendering traditional centralized control methods less efficient due to scalability, latency, and vulnerabilities [62]. As a result, decentralized learning, particularly multi-agent reinforcement learning (MARL), has emerged as a viable solution for smart energy management [57,63]. In this framework, each DER or group of DERs acts as an autonomous agent that makes decisions

based on local information and interactions with other agents, optimizing the system's overall performance while maximizing individual rewards [63].

Despite its promise, decentralized learning for energy systems faces challenges such as handling limited local observations, sparse rewards, scalability with increasing DERs, and ensuring stability and safety in grid operations [57]. Future work could focus on enhancing communication protocols, improving the robustness of algorithms against grid failures, integrating physical grid models, and exploring hybrid approaches that combine decentralized learning with traditional optimization techniques for better performance [57].

2.3.2. Multi-agent reinforcement learning (MARL) for decentralized DER control

The growing integration of DERs (e.g., solar, wind, and storage) introduces significant uncertainty and variability into power distribution networks, challenging traditional centralized control due to issues related to scalability, latency, and resilience [62]. In response, decentralized approaches, particularly MARL, have gained traction. They enable each DER or group to function as autonomous agents, facilitating localized learning, inter-agent coordination, and adaptive decision-making in dynamic environments [64].

Effective communication and coordination are key for optimizing performance. Additionally, a graph neural network-driven intrinsic reward mechanism for heterogeneous multi-agent cooperation improved coordination and addressed challenges like partial observability and reward sparsity, demonstrating superior performance in cooperative scenarios [64]. Zhang et al. [62] introduced a fully decentralized MARL approach where agents at communication network nodes make decisions based on local observations and messages from their neighbors. They proposed two scalable, decentralized actor-critic algorithms with function approximation to address extensive MARL problems, where agents' joint actions influence the environment's state and rewards [62].

2.3.3. Federated learning for privacy-preserving energy optimization

Federated learning enables privacy-preserving energy management by allowing distributed devices, such as smart meters and sensors, to train machine learning models collaboratively without sharing sensitive data [65]. Each device processes local data and contributes to a global model, enhancing decision-making in energy management systems like DERMS. This decentralized approach ensures privacy by keeping data local while optimizing energy usage, demand forecasting, and efficient distribution across devices. Lee et al. [66] proposed a federated deep reinforcement learning framework for managing shared energy storage systems in smart buildings, ensuring privacy by sharing only portions of the trained neural networks, thereby avoiding the transmission of raw energy consumption data. The joint optimization framework presented by Ju et al. [67] focused on balancing global model accuracy, minimizing total energy consumption, and reducing energy usage disparities across devices, demonstrating the efficiency of federated learning in energy management. To address the non-independent and identically distributed data problem in federated learning, the FedClusAvg algorithm, as utilized by Li et al. [68], enables prosumers to participate in intelligent decision-making while preserving privacy. A resilient FL approach was introduced in [69] for cyber-attack detection and mitigation in electric vehicle demand forecasting. Due to its popularity in academia and industry, FL will be studied in greater detail in subsequent sections of this paper.

2.3.4. Edge artificial intelligence

Edge AI deploys algorithms directly on local devices, such as sensors, controllers, and smart meters, enabling real-time data processing and decision-making without relying on centralized cloud servers [70]. This reduces latency and bandwidth consumption, making it suitable for energy systems that require rapid responses, such as dynamic load balancing and optimization [71]. By enabling autonomous decisions, it enhances microgrid efficiency, optimizes energy storage, supports predictive maintenance, and facilitates the integration of renewable energy. It also improves security and privacy by keeping sensitive data localized, which reduces risks associated with cloud data transmission [72]. In large-scale deployments, it ensures scalability and prevents overloading of the centralized infrastructure. This improves grid stability, optimizes energy flow, and enhances predictive maintenance, contributing to sustainable energy management. A review by authors [73] synthesizes findings from over 200 studies, emphasizing AI's role in improving energy system reliability, resilience, and efficiency, particularly through big data and smart grids.

2.3.5. Swarm learning

Swarm learning enables sensors and smart meters to optimize energy consumption and generation autonomously. It scales effectively with the addition of new devices, enhancing the flexibility and resilience of systems like smart grids and microgrids, and ensures continued operation during device failures [71]. Swarm learning enhances energy efficiency by enabling distributed energy resources to collaborate and balance production and consumption. It facilitates secure data sharing by exchanging model updates instead of raw data, addressing privacy concerns [72]. This approach supports decentralized optimization for energy dispatch, grid management, and integrating renewable energy, providing a scalable, secure, and resilient solution for advanced energy systems. Mongail et al. highlight the role of artificial neural networks and reinforcement learning in predicting energy demand [71]. Another study proposes a Salp swarm-optimized twin support vector machine for predicting smart grid stability and optimizing energy management, demonstrating the effectiveness of swarm learning in renewable energy management [72].

2.3.6. Applications and challenges of distributed learning

Applications of distributed learning techniques span AI-driven energy and load forecasting [73,74], through cyber security intrusion detection [6], to adaptive demand response [75], and real-time optimization of DERs [51]. These applications provide benefits such as scalable management of DER systems [14], real-time decision making at the edge [76], enhanced privacy and security, and improved energy efficiency [51].

There are several challenges associated with the above methods. Managing and integrating data from diverse sources and formats while ensuring consistency and accuracy across distributed nodes requires sophisticated data preprocessing and normalization techniques [76]. Distributed learning methods also require efficient communication protocols to synchronize updates and share information among nodes increasing latency and complexity [14]. Edge devices often have limited computational power and storage capacity, which restricts the complexity of models that can be deployed [51]. While distributed learning enhances privacy, it also introduces new cyber security challenges, such as securing communication channels and protecting against distributed denial-of-service attacks [76,77].

3. Cyber security framework for DER layers and lifecycle

This section introduces the four-layer cyber security framework for DERs, which will be further in the rest of the paper. It also covers the cyber security vulnerabilities across the four layers and then adapts the five stages of the cyber security lifecycle to DER systems.

3.1. Four-layer cyber security framework

Prior studies suggest a three-layer approach to DER cyber security hardening [6]. However, this excludes protection for the edge-based controller collocated at the DER. Meanwhile, this controller, which is present at each DER node is a significant potential entry-point through

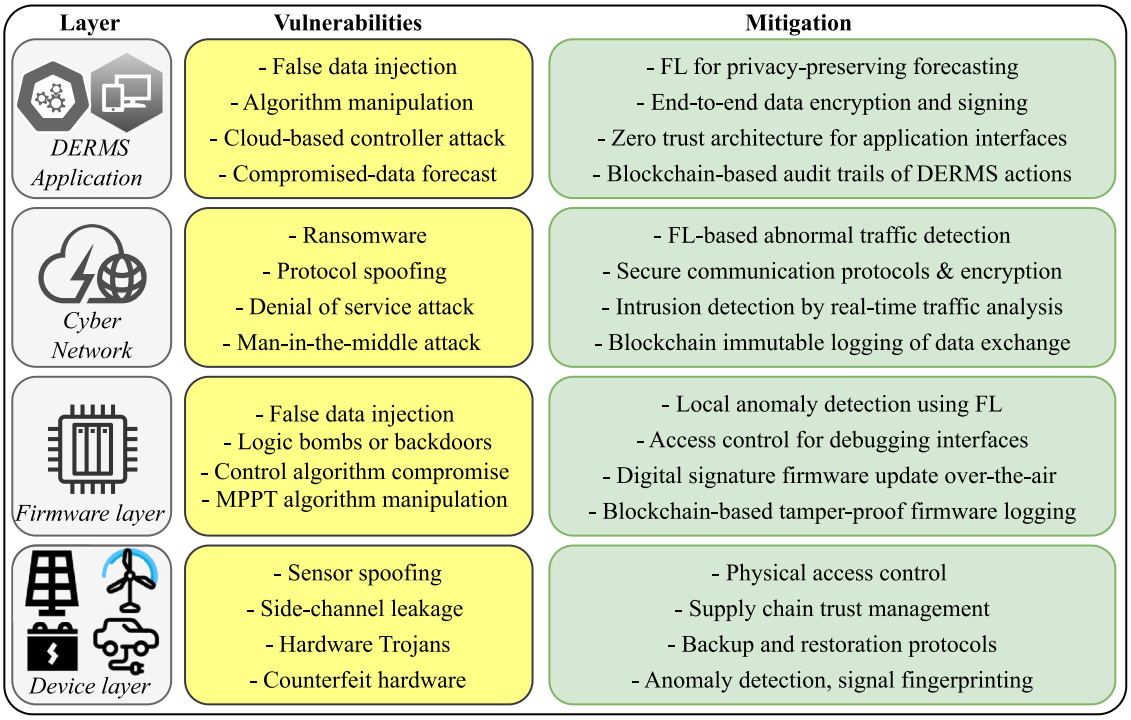

Fig. 2. Cyber security layers, vulnerabilities and mitigation by integrated blockchain-federated learning.

which malware can be introduced into the network-wide DER system. The importance of attack-resilient firmware for DER micro-controllers, digital signal processors and field-programmable gate array integrated circuits is well discussed in several literature [78–80]. However, this layer is not explicitly accounted for in [6].

Therefore, this paper adopts the four-layer cyber security framework shown in Fig. 2. This approach provides a holistic approach to cyber security by organizing attack surfaces, vectors, and mitigation strategies into four tightly coupled layers comprising: device/physical, firmware/control, cyber network, and DERMS/application layers. Each layer is tailored to unique attack modalities while reinforcing adjacent layers for comprehensive resilience.

3.1.1. Device layer

This layer represents the physical components of DERs—sensors, converters, smart meters, and communication modules. Since these are frequently deployed in remote or unsupervised locations [81], they are susceptible to physical tampering, hardware Trojans, and side-channel attacks. Access controls (locks, surveillance, and tamper alarms) deter physical intrusion. Hardware authenticity can be validated by supply chain security through vendor audits and component provenance tracking ensure.

3.1.2. Firmware layer

This layer governs the logic embedded in power electronic converters and smart controllers. It executes real-time algorithms such as maximum power-point tracking, frequency/voltage control, and islanding detection [82]. Firmware vulnerabilities include unauthorized firmware updates and exploitation of legacy control architectures without security patches. This layer can be hardened by securing over-the-air firmware updates with digital signatures, and anomaly detection algorithms.

3.1.3. Cyber network layer

This layer facilitates data exchange (through networking, routing, and communication protocols) between DERs, aggregators, supervisory control and data acquisition (SCADA) systems, and utilities. Attackers can target this layer to disrupt operations or exfiltrate sensitive data. Key vulnerabilities include: man-in-the-middle attacks, denial-of-service attacks on control centers or gateways, ransomware targeting SCADA servers. These weaknesses can be mitigated by end-to-end encryption, mutual authentication, and intrusion detection systems.

3.1.4. DERMS application layer

Distributed energy resource management systems (DERMS), forecasting engines, optimization modules, and energy market interfaces are at the highest layer. These applications orchestrate DER dispatch, demand response, and market participation using AI/ML models, often deployed in the cloud. Key vulnerabilities include: algorithmic manipulation, false data injection, and compromise of cloud-hosted controllers. These vulnerabilities can be mitigated by zero trust architecture and anomaly detection.

3.1.5. Mapping to traditional cybersecurity domains

The proposed four-layer framework inherently addresses traditional cybersecurity classifications across architectural boundaries. Network Security encompasses encrypted communication protocols, mutual authentication, and intrusion detection systems spanning cyber network and application layers. Endpoint Security primarily resides within device and firmware layers through access controls, tamper detection, secure boot processes, and anomaly monitoring at individual DER units. Application Security manifests in the DERMS layer via zero-trust architecture, role-based access controls, and secure API implementations. Data Security operates cross-layer, implementing end-to-end encryption from device sensors through network transmission to application storage, ensuring data integrity, confidentiality, and privacy-preserving analytics throughout the entire DER ecosystem. This integrated approach provides comprehensive coverage while maintaining architectural coherence.

3.2. Cybersecurity vulnerabilities in DERs

DERs face multifaceted cybersecurity threats that exploit vulnerabilities across the four-layer framework (see Fig. 2), necessitating comprehensive defense strategies to maintain grid stability and operational integrity.

3.2.1. Device layer vulnerabilities

Physical DER components deployed in remote locations present significant attack surfaces through hardware manipulation, supply chain compromises, and environmental exploitation. Attackers can install hardware Trojans during manufacturing, conduct physical tampering of sensors and smart meters to inject false readings, or exploit side-channel attacks to extract cryptographic keys from power converters. The distributed nature of DER installations compounds these risks, as many devices operate without continuous monitoring or physical security controls. Electromagnetic interference attacks can disrupt sensor accuracy, while device cloning enables unauthorized network access through legitimate device credentials.

3.2.2. Firmware layer threats

Embedded control systems executing critical real-time algorithms become prime targets for sophisticated adversaries seeking to manipulate power flow or destabilize grid operations. Firmware vulnerabilities manifest through exploitation of unpatched legacy systems, unauthorized over-the-air updates that install malicious code, and reverse engineering of proprietary control algorithms. Attackers can modify maximum power-point tracking algorithms to reduce renewable energy output, compromise islanding detection mechanisms to create dangerous operating conditions, or inject malware that propagates through firmware update channels to multiple DER units simultaneously.

3.2.3. Cyber network layer attacks

Communication infrastructures connecting DERs to control centers face persistent threats from network-based adversaries. Man-in-the-middle attacks intercept and modify control commands between DERMS and field devices, potentially causing equipment damage or grid instability. Distributed denial-of-service attacks overwhelm SCADA systems and communication gateways, disrupting real-time monitoring and control capabilities. Ransomware specifically targeting industrial control systems can encrypt critical operational data, while advanced persistent threats establish covert channels for long-term espionage and sabotage operations.

3.2.4. DERMS application layer risks

Cloud-hosted management systems and AI-driven optimization engines present high-value targets for cyber criminals and nation-state actors. Algorithmic manipulation attacks poison machine learning models used for demand forecasting and dispatch optimization, leading to suboptimal resource allocation and increased operational costs. False data injection attacks compromise market participation algorithms, enabling financial fraud and market manipulation. Cloud infrastructure vulnerabilities expose sensitive customer data and proprietary control strategies, while compromised application programming interfaces enable unauthorized access to critical system functions.

These vulnerabilities necessitate the integrated BlockFL solutions discussed in Section 5, which provide distributed trust mechanisms and privacy-preserving techniques to address threats across all four layers while supporting the comprehensive cyber security lifecycle framework presented in Section 3.3.

3.3. Cyber security life cycle strategy for DERs

The cyber security hardening of DERs in this study is guided by the five key functions defined by the National Institute of Standards and Technology (NIST): prevention, detection, analysis, decision, and recovery [83]. Prevention strategies avoid cyber security incidents by reducing vulnerabilities in the DER system across different layers from the physical layer to the DERMS application layer. Prevention strategies include strong authentication, encrypted communication, secure firmware updates, and role-based access control. For instance, microgrid controllers and DER aggregators must restrict access to authorized users only. Similarly, mitigation mechanisms that prevent cyber intrusions can be triggered by the detection of abnormal activities.

Detection aims to identify cyber-attacks and trigger alarms when they occur. Detection systems monitor real-time network traffic in the DER system, and must be capable of intrusion and anomaly detection. For example, if an unauthorized command is sent to curtail solar output during peak hours, a robust detection mechanism must raise an alarm immediately. This anomaly detection is best done by edge-based analytics embedded on the DER devices which do not rely on centralized cloud servers.

Analysis is necessary to determine the root cause, scope, and potential impact of detected incidents. For instance, a coordinated attack on multiple smart meters may indicate a broader malware campaign. Next, a timely decision must be made to contain or mitigate the threat. DER cyber-security decisions are best implemented by automation, and with minimal latency. Such decisions can include isolating a compromised converter, re-routing power flows, or revoking access credentials of a malicious actor. The recovery stage of the lifecycle restores DER systems to normal operation while preserving data and trust. Recovery mechanisms include firmware rollback, re-synchronization of DER control settings, and restoration from backup configurations. Fig. 6 shows a mapping of BlockFL solutions across these five stages.

4. Overview of BlockFL architectures

This section introduces the generic features of BlockFL architectures, highlighting how BlockFL facilitates the synergistic relationship between both blockchain and FL. Next, ten promising BlockFL architectures in the literature are discussed, their performance analysis based on applicability to the four DER layers, privacy-utility trade-offs and resource-consumption characteristics.

4.1. Generic characteristics of BlockFL

The integration of blockchain and FL creates a powerful framework particularly well-suited for distributed energy resource (DER) management. This synergy addresses critical weaknesses in both technologies, enabling more robust, secure, and efficient energy systems, as shown in Table 4.

FL suffers from vulnerabilities to model poisoning and dishonest clients, a significant concern in energy networks where compromised data could lead to grid instability. Blockchain mitigates this by creating immutable logs of training updates and using consensus mechanisms to filter anomalies. The lack of incentive mechanisms in FL is addressed through blockchain smart contracts that reward honest participation. In wind energy cooperatives, this encourages turbine operators to share accurate performance data, creating more reliable regional wind forecasting models while compensating data providers fairly. Similarly, V2G EV networks benefit from these incentives, motivating EV owners to share battery health and charging pattern data crucial for grid balancing. Trust management between energy storage systems from different vendors and owners becomes possible through blockchain's immutable reputation tracking. This enables neighborhood battery systems to collaborate in demand response programs despite having different manufacturers or owners, as blockchain establishes consistent performance records.

Table 4
Mutual mitigation of blockchain and federated learning (FL) weaknesses in DER systems.

Weakness of blockchain	How FL can help	Weakness of FL	How blockchain can help
High resource and energy usage	FL reduces transaction frequency via selective model updates	Vulnerable to data/model poisoning	Blockchain ensures accountability of updates via smart contracts
Low scalability and high latency	Local FL training avoids global consensus bottlenecks	High communication overhead	Blockchain enables asynchronous, trustless coordination to reduce communication
Limited interoperability with legacy systems	FL adapts to heterogeneous edge devices without protocol changes	Non-IID and imbalanced data issues	Blockchain records data provenance for better model weighting
Smart contract complexity and bugs	FL can limit on-chain logic, shifting ML off-chain	Privacy leakage through model updates	Blockchain provides encrypted, tamper-proof logging for auditability
Decentralization-efficiency tradeoff in consensus	FL reduces blockchain load, enabling simpler consensus protocols	Lack of incentives for participation	Blockchain rewards honest participants using tokens or credits

* IID means independent and identically distributed.

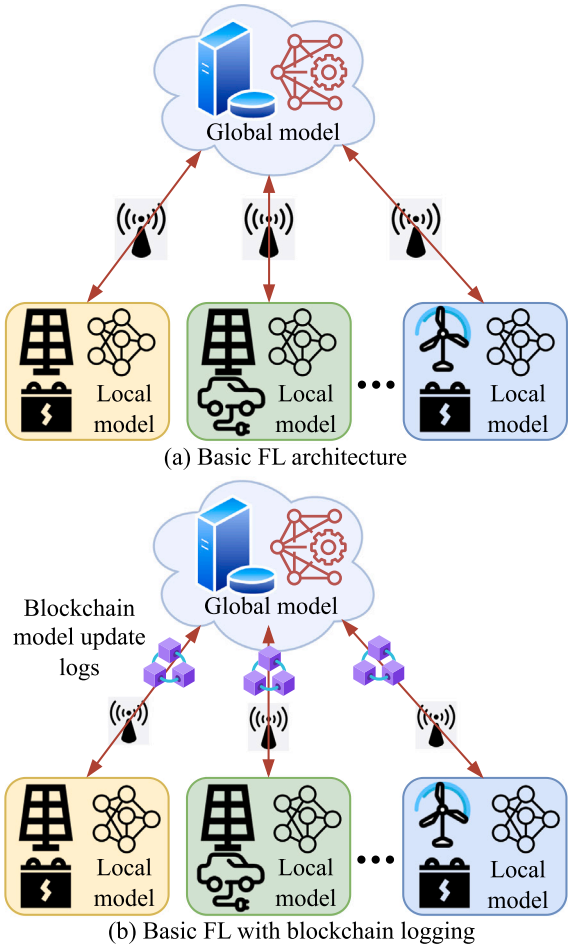

Fig. 3. Classical FL and basic BlockFL architectures.

Conversely, FL addresses blockchain's weaknesses. The high energy consumption of proof-of-work consensus mechanisms is reduced by FL's approach of keeping computation off-chain. FL's inherent privacy preservation keeps sensitive data local, allowing utilities and residential consumers to collaborate on consumption models without exposing individual household patterns. For V2G applications, this means EV charging behaviors can inform grid planning without compromising driver privacy. Finally, FL provides intelligent anomaly detection that blockchain alone lacks. In energy storage systems, this enables adaptive responses to emerging cyber threats or unusual grid conditions, protecting critical infrastructure from novel attack vectors.

4.2. BlockFL architectures

4.2.1. Basic FL with blockchain logging

This is the simplest BlockFL architecture in which blockchain functions primarily as an immutable ledger for logging FL model training (see Fig. 3), as well as model upload and download exchanges between edge devices and the central aggregator [16,84]. It has a low implementation complexity, but is able to preserves FL efficiency while adding transparency of audit trail for all model updates. Nevertheless, its central aggregator remains a single point of failure and has limited protection against poisoning attacks at aggregation stage.

4.2.2. Blockchain as FL model aggregator

This structure (Fig. 4) overcomes the limitations of the basic BlockFL by eliminating the single point of failure in aggregation. The blockchain network directly performs model aggregation with the smart contracts replace central aggregator functionality [85]. Since it is fully decentralized, the edge devices act as miners that execute aggregation algorithms, meanwhile, they also log model updates as transactions to the blockchain. It has high latency, high computational overhead for the blockchain network, and limited scalability with large models or many participants.

4.2.3. FL with smart contract controlled training

In order to overcome the some of the native challenges of FL such as malicious actors intending to poison the centralized model, this architecture uses smart contracts to enforce training rules and protocols [86]. Its transparent reward mechanism incentivizes compliant nodes and penalizes non-compliance or malicious behavior by an automated verification of participant contributions. However, it requires complex rule designs, and smart contract vulnerabilities could compromise system.

4.2.4. Blockchain-imbalanced FL

This highly specialized architecture addresses the unique challenges of rare event detection in renewable energy systems, such as wind turbine blade icing or solar panel failures [54]. The combined blockchain security with class imbalance techniques handles both the security requirements and the statistical challenges of learning from extremely imbalanced datasets where critical events are rare. Despite its improved model performance on minority classes, it could be overfitted to rare events.

4.2.5. Hierarchical BlockFL

This has a multi-level blockchain structure where local blockchains handle regional or domain-specific FL, while global blockchain coordinates across local chains, as shown in Fig. 5. This improved scalability for large-scale systems. Also, there layered model aggregation reduces consensus overhead within local chains. Therefore, this BlockFL is capable of accommodating heterogeneous participant groups, while accommodating domain-specific optimization possible at local levels [87].

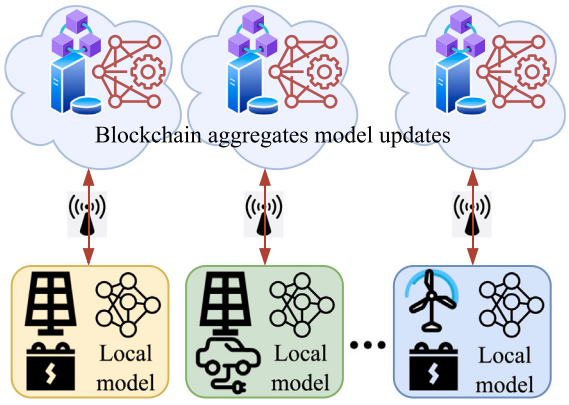

Fig. 4. Blockchain as FL model aggregator BlockFL architecture.

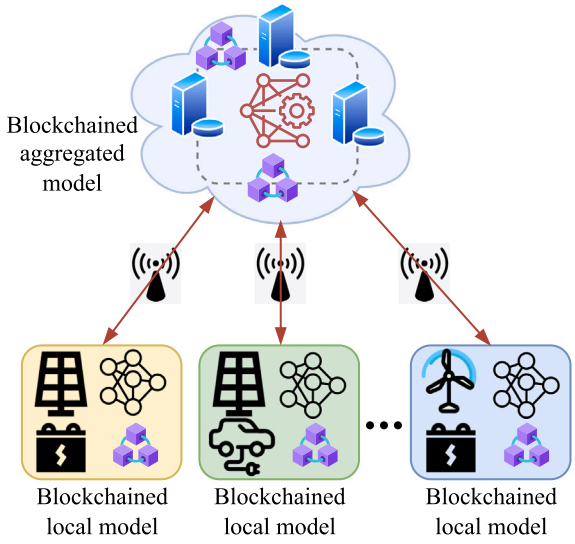

Fig. 5. Hierarchical blockchain-federated learning architecture.

However, it suffers from inter-blockchain synchronization challenges and potential inconsistencies between layers.

4.2.6. Sharded BlockFL

This structure features a horizontal partitioning of the blockchain network with different shards handling distinct subsets of participants. Load balancing across the network is ensured by periodical cross-shard synchronization [88]. Furthermore, the parallel processing of FL model updates significantly improves the throughput capacity. Therefore, the architecture facilitates ease of scale as DER edge devices as the system size increases. Nevertheless, the complex shard structure increase management overhead requirements and introduces cross-shard security vulnerabilities.

4.2.7. Cross-blockchain FL

This architecture utilizes multiple distinct blockchain technologies with cross-chain communication protocols. Different blockchains serve different regional or functional purposes while bridge contracts facilitate interoperability [89]. Therefore, it has the flexibility to leverage strengths of different blockchain platforms across different regions by accommodating heterogeneous participant requirements. It is limited by security vulnerabilities at cross-chain interfaces and can be difficult to debug when challenges arise.

4.2.8. Zero-knowledge proof BlockFL

This architecture is critical for highly sensitive applications where privacy is paramount. Zero-knowledge proof allows verification that models were trained correctly on valid data without ever exposing that data, even to other participants in the federated learning process [90]. It uses cryptographic proofs to verify computational integrity and has strong security guarantees. Despite its resistance to data reconstruction attacks, this structure has increased computational overhead and slower training cycles due to proof generation/verification.

4.2.9. Blockchain-assisted split federated learning

This architecture is particularly suitable for edge computing devices that have limited processing capabilities. The nodes could participate in collaborative learning by computing only the first few layers of a neural network locally, with blockchain securing the transfer of intermediate activations to more powerful servers [91]. The computational load is securely distributed through split learning with blockchain. Despite reducing the client-side computational requirements, training is slowed down due to sequential dependencies.

4.2.10. Energy-efficient lightweight BlockFL

This architecture is essential for applications where energy efficiency is critical, such as battery-powered microgrids [92]. The lightweight blockchain approach enables the constrained devices to participate in federated learning without excessive energy consumption. Therefore, it has higher transaction throughput at lower operating costs. However, it has reduced decentralization due to dependency on trusted validators, and is vulnerable to potential validator collusion.

Summary: Among the reviewed BlockFL architectures (summarized in Table 5), the first five are commonly applied in DER-related literature: Basic FL with blockchain logging, blockchain as aggregator [85], federated learning with smart contract controlled training [54,86], and blockchain-imbalanced FL [54] which is specialized for critical event detection. All the ten discussed architectures selected due to their potential to improve DERs' resilience to malicious attacks.

4.3. Mapping of BlockFL architectures to DER layers

Since each DER layer exhibits distinct attack vectors and computational constraints requiring tailored BlockFL approaches shown in the last column of Table 5. The device layer benefits from energy-efficient lightweight BlockFL due to power constraints in remote deployments. The firmware layer requires split federated learning and smart contract-controlled training to address processing limitations while ensuring secure control logic updates. The cyber network layer leverages zero-knowledge proof BlockFL for privacy-preserving data exchange. The DERMS application layer employs hierarchical and cross-blockchain architectures for scalable multi-domain coordination. This systematic mapping provides engineering guidelines for selecting appropriate BlockFL architectures based on layer-specific security requirements and operational constraints in DER systems.

4.4. Performance analysis of BlockFL architectures

This section compares the BlockFL architectures using metrics including latency, security, scalability, throughput, computational overhead, energy consumption, complexity and fault tolerance, as summarized in Table 6. The table, which considers bitcoin as the baseline pure blockchain (BM2), was created from the authors' interpretation of the reported results in the reviewed literature. These are discussed in the context of their practical suitability to the four layers of DERs earlier introduced in Section 3.1.

Table 5
Features of integrated blockchain-federated learning architectures.

#	Architecture name	Key features	Advantage	Disadvantage	Suitable DER layer
1	Basic FL with Blockchain Logging [16,84]	Blockchain only records the model updates, no direct control over aggregation.	Simple, minimal integration complexity.	Vulnerable if aggregator is compromised.	Device
2	Blockchain as Aggregator [85]	Blockchain miners or smart contracts aggregate FL model updates.	No single-point-of-failure; fully decentralized.	High blockchain transaction overhead; scalability issues.	DERMS
3	Federated Learning with Smart Contract Controlled Training [86]	Smart contracts define and enforce the FL training rules, contribution rewards, and penalties.	Enforces fairness and reduces malicious behavior automatically.	Gas fees (in public blockchains) can become expensive.	Firmware, Cyber Network
4	Blockchain-Imbalanced FL [54]	FL is combined with blockchain and class imbalance correction techniques for rare event detection (e.g., wind blade icing).	Specialized for critical-event detection, robustness against data imbalance.	Requires well-designed imbalance strategies.	Firmware
5	Hierarchical Blockchain-FL [87]	Multiple local FL blockchains connected to a global blockchain; layered model aggregation.	Improves scalability, suits large systems like smart grids.	Design and synchronization complexity.	DERMS Application
6	Sharded Blockchain Federated Learning [88]	Data and model updates are split across multiple shard chains; sharded blockchains synchronize periodically.	Supports high-throughput FL systems, better load balancing.	Complex shard management and security risk across shards.	Cyber Network
7	Cross-Blockchain Federated Learning [89]	Different blockchains handle different regions, and cross-chain communication enables global FL model integration.	Flexibility to support heterogeneous participants.	Cross-chain protocols are immature and risky.	DERMS Application
8	Zero-Knowledge Proof (ZKP) Blockchain FL [90]	Nodes prove correctness of model updates without revealing raw data or model details.	Maximum privacy preservation, data confidentiality.	Heavy computation cost for ZKP generation.	Cyber Network
9	Blockchain-Assisted Split Federated Learning [91]	Split learning across clients and server with blockchain securing intermediate activations.	Reduces device-side computation, strengthens security.	Split learning setups can suffer from latency bottlenecks.	Firmware
10	Energy-Efficient Lightweight Blockchain-FL [92]	Uses Proof-of-Authority or Delegated Proof-of-Stake blockchains to reduce FL transaction overhead.	Energy-efficient and scalable for IoT and microgrids.	Relies on trusted validators; partially centralized trust.	Device

DERMS is distributed energy resource management system, ZKP means zero-knowledge proof.

Table 6
Performance comparison of BlockFL architectures for DER applications.

#	Architecture	Latency	Security	Scalability	Throughput	Computational overhead[†]	Energy consumption[a]	Implementation complexity	Fault tolerance[b]
1	Basic FL with Blockchain Logging	10-60s	Moderate	200-1K nodes	200-1K TPS	20%–40%	15%–35%	Low	10%–25%
2	Blockchain as FL Model Aggregator	10-60 mins	High	<10 nodes	3-50 TPS	100%	100%	High	100%
3	FL with Smart Contract Controlled Training	1-10 mins	High	50-200 nodes	50-200 TPS	40%–80%	35%–70%	High	100%
4	Blockchain-Imbalanced FL	1-10 mins	High	10-50 nodes	50-200 TPS	100%	35%–70%	Moderate	100%
5	Hierarchical BlockFL	1-10 mins	High	>1K nodes	200-1K TPS	40%–80%	35%–70%	High	>100%
6	Sharded BlockFL	10-60s	Moderate	>1K nodes	>1K TPS	40%–80%	35%–70%	Very High	25%–40%
7	Cross-Blockchain FL	10-60 mins	Moderate	200-1K nodes	50-200 TPS	100%	100%	Very High	25%–40%
8	Zero-Knowledge Proof BlockFL	10-60 mins	Very High	10-50 nodes	3-50 TPS	>100%	100%	Very High	100%
9	Blockchain-Assisted Split FL	10-60 mins	High	50-200 nodes	3-50 TPS	20%–40%	15%–35%	Moderate	100%
10	Energy-Efficient Lightweight BlockFL	10-60s	Low	200-1K nodes	>1K TPS	20%–40%	<15%	Low	10%–25%
BM1	Pure FL (no blockchain)	<10s	Low	200-1K nodes	>1K TPS	<20%	<15%	Very Low	10%–25%
BM2	Pure blockchain (no FL)	10-60 mins	Very High	10-50 nodes	3-50 TPS	100%	100%	Moderate	100%

[a] Percentages relative to Pure blockchain/Bitcoin (100%).
[b] Percentage of network nodes that can fail while system remains operational.

4.4.1. Latency

Latency performance varies significantly across BlockFL architectures, with critical implications for DER hierarchical layers. While Pure FL (BM1) achieves very low latency, Basic FL with Blockchain Logging (#1) and Sharded BlockFL (#6) demonstrate low latency suitable for device-layer real-time operations and firmware-level control functions. Energy-Efficient Lightweight BlockFL (#10) achieves minimal latency approaching Pure FL performance, making it appropriate for battery-constrained devices. Moderate latency architectures (#3, #4, #5) are suitable for cyber network coordination and DERMS application-level operations where sub-second response is not critical. High latency systems (#2, #7, #8, #9) approach Pure blockchain (BM2) latency, presenting challenges for time-sensitive DER operations, particularly affecting device-layer responsiveness and firmware execution cycles in grid stabilization scenarios.

4.4.2. Security

Security capabilities demonstrate clear architectural trade-offs across DER implementation layers. Zero-Knowledge Proof BlockFL (#8) provides the highest security through cryptographic verification, essential for DERMS applications handling sensitive grid data, while approaching Pure blockchain (BM2) security levels. Blockchain as FL Model Aggregator (#2), Smart Contract Controlled Training (#3), Blockchain-Imbalanced FL (#4), and Hierarchical BlockFL (#5) offer high security suitable for cyber network protection and cross-layer communication. Moderate security architectures (#1, #6, #7) provide adequate protection for firmware-level operations and device coordination. Energy-Efficient Lightweight BlockFL (#10) exhibits low security similar to Pure FL (BM1) due to trusted validator dependencies, limiting its applicability to less critical device-layer functions where energy efficiency outweighs security requirements.

4.4.3. Scalability

Scalability analysis reveals architecture suitability for different DER deployment scales. Hierarchical BlockFL (#5) and Sharded BlockFL (#6) achieve very high scalability, supporting large-scale DERMS applications and extensive cyber network topologies, matching Pure FL (BM1) scalability. Basic FL with Blockchain Logging (#1), Cross-Blockchain FL (#7), and Energy-Efficient Lightweight BlockFL (#10) provide high scalability for medium-scale deployments across firmware and device layers. Moderate scalability architectures (#3, #9) suit regional DER networks. Low scalability systems (#2, #4, #8) are constrained to small-scale implementations similar to Pure blockchain (BM2), limiting their effectiveness in large-scale DER integration scenarios where thousands of devices require coordination across multiple hierarchical levels.

4.4.4. Throughput

Throughput performance directly impacts DER system responsiveness across operational layers. Sharded BlockFL (#6) and Energy-Efficient Lightweight BlockFL (#10) deliver very high throughput through parallel processing and lightweight operations, approaching Pure FL (BM1) performance levels while supporting high-frequency device-layer communications and firmware updates. Basic FL with Blockchain Logging (#1) and Hierarchical BlockFL (#5) provide high throughput suitable for DERMS applications requiring frequent model updates. Moderate throughput architectures (#3, #4, #7) accommodate standard cyber network operations. Low throughput systems (#2, #8, #9) present significant limitations similar to Pure blockchain (BM2) for real-time DER applications, particularly affecting device-layer performance monitoring and firmware-level control loop execution in dynamic grid conditions.

4.4.5. Computational overhead

Computational overhead analysis reveals critical constraints for resource-limited DER devices. Basic FL with Blockchain Logging (#1), Blockchain-Assisted Split FL (#9), and Energy-Efficient Lightweight BlockFL (#10) exhibit low overhead, enabling deployment on constrained device-layer hardware and embedded firmware systems. Moderate overhead architectures (#3, #5, #6) balance functionality with resource requirements, suitable for cyber network nodes with moderate processing capabilities. High overhead systems (#2, #4, #7) require substantial computational resources, limiting deployment to DERMS application servers. Zero-Knowledge Proof BlockFL (#8) demands very high computational resources, restricting its use to specialized high-security applications where computational cost is justified by security requirements.

4.4.6. Energy consumption

Energy consumption patterns significantly impact DER device sustainability and operational costs. Energy-Efficient Lightweight BlockFL (#10) achieves very low consumption, critical for battery-powered devices and edge-layer deployments. Basic FL with Blockchain Logging (#1) and Blockchain-Assisted Split FL (#9) maintain low energy usage, suitable for resource-constrained firmware implementations. Moderate consumption architectures (#3, #4, #5, #6) balance functionality with energy efficiency for cyber network operations. High consumption systems (#2, #7, #8) require substantial power resources, limiting deployment to grid-connected DERMS applications. The energy profile directly affects device-layer battery life and operational sustainability in distributed DER networks.

4.4.7. Implementation complexity

Implementation complexity varies substantially, affecting deployment feasibility across DER system layers. Basic FL with Blockchain Logging (#1) and Energy-Efficient Lightweight BlockFL (#10) offer low complexity, facilitating rapid deployment in device-layer and firmware applications. Blockchain-Imbalanced FL (#4) and Blockchain-Assisted Split FL (#9) present moderate complexity suitable for specialized cyber network implementations. High complexity architectures (#2, #3, #5, #6) require sophisticated development expertise and extensive testing, appropriate for DERMS application-level deployments. Zero-Knowledge Proof BlockFL (#8) and Cross-Blockchain FL (#7) exhibit very high complexity, demanding specialized cryptographic and multi-chain expertise, limiting their implementation to high-value, security-critical applications.

4.4.8. Fault tolerance

Fault tolerance capabilities determine system resilience across DER operational scenarios. Hierarchical BlockFL (#5) provides very high fault tolerance through multi-layer redundancy, essential for critical DERMS applications and cyber network resilience. High fault tolerance architectures (#2, #3, #4, #8, #9) offer robust protection against component failures, suitable for cyber network coordination and critical device-layer operations. Moderate fault tolerance systems (#6, #7) provide adequate protection for standard DER operations. Low fault tolerance architectures (#1, #10) present vulnerability risks, limiting their deployment to non-critical device-layer functions where simplicity and efficiency outweigh resilience requirements in DER system design.

4.4.9. Summary

The analysis reveals distinct performance trade-offs across BlockFL architectures for DER applications. Energy-Efficient Lightweight BlockFL (#10) and Basic FL with Blockchain Logging (#1) excel in resource-constrained device-layer deployments, offering low latency, minimal computational overhead, and energy efficiency but sacrificing security and fault tolerance. Hierarchical BlockFL (#5) and Sharded BlockFL (#6) demonstrate superior scalability and throughput for large-scale DERMS applications, though with increased implementation

complexity. Zero-Knowledge Proof BlockFL (#8) provides maximum security at the cost of computational resources and latency. The selection depends on specific DER layer requirements, balancing performance metrics against operational constraints across the four hierarchical levels.

4.5. Privacy-utility trade-offs

The deployment of BlockFL architectures in DER systems necessitates careful consideration of the inherent trade-offs between privacy preservation and system utility. The study's comparative analysis reveals three distinct categories of privacy-utility balance among the examined architectures.

4.5.1. High privacy, constrained utility

Zero-Knowledge Proof BlockFL (Architecture 8) exemplifies the maximum privacy preservation approach, enabling cryptographic proof of model update correctness without data disclosure. This architecture achieves very high security ratings but operates with low scalability and throughput performance. The computational complexity of ZKP generation results in high latency and energy consumption, limiting its applicability to scenarios where privacy requirements supersede performance considerations. Similarly, Blockchain as FL Model Aggregator (Architecture 2) eliminates single-point-of-failure vulnerabilities through fully decentralized aggregation, achieving high security at the cost of high blockchain transaction overhead, resulting in reduced scalability and throughput metrics.

4.5.2. Balanced privacy-utility performance

Smart Contract Controlled Training (Architecture 3) and Hierarchical BlockFL (Architecture 5) demonstrate optimal balance between privacy preservation and system performance. Architecture 3 leverages smart contracts to enforce training rules and fairness mechanisms while maintaining moderate performance across latency, scalability, and throughput metrics. Architecture 5 achieves very high scalability through layered model aggregation while preserving high security, though this requires high implementation complexity. Blockchain-Imbalanced FL (Architecture 4) provides specialized capabilities for critical event detection while maintaining high security, demonstrating domain-specific optimization potential.

4.5.3. Utility-optimized approaches

Basic FL with Blockchain Logging (Architecture 1) and Energy-Efficient Lightweight BlockFL (Architecture 10) prioritize system performance over maximum privacy preservation. Architecture 1 achieves high scalability and throughput with minimal integration complexity, accepting moderate security levels and low fault tolerance. Architecture 10 demonstrates that consensus mechanism optimization (using Proof-of-Authority or Delegated Proof-of-Stake) enables very high throughput and very low energy consumption, though this introduces partial centralization that reduces privacy guarantees.

The privacy-utility analysis indicates that DER system designers must evaluate application-specific requirements against available computational resources. Critical infrastructure applications may justify the performance penalties associated with maximum privacy architectures, while high-frequency trading or real-time grid management applications may require utility-optimized solutions with acceptable privacy trade-offs.

4.6. Resource consumption analysis

Resource consumption patterns across BlockFL architectures reveal significant variations in energy efficiency, computational overhead, and scalability characteristics that directly impact deployment feasibility in resource-constrained DER environments.

4.6.1. Energy consumption characteristics

The architectures exhibit distinct energy consumption profiles directly correlated with their consensus mechanisms and cryptographic complexity. Energy-Efficient Lightweight BlockFL demonstrates optimal energy performance through consensus mechanism selection, achieving very low energy consumption suitable for IoT-scale DER devices. Conversely, Zero-Knowledge Proof BlockFL and Cross-Blockchain FL exhibit high energy consumption due to intensive cryptographic operations and inter-chain communication protocols. Blockchain as FL Model Aggregator shows high energy consumption attributable to extensive blockchain transaction processing required for decentralized aggregation.

4.6.2. Computational overhead analysis

Computational resource requirements vary substantially across architectures, creating deployment constraints for resource-limited DER devices. Zero-Knowledge Proof BlockFL imposes very high computational overhead due to cryptographic proof generation, potentially exceeding the processing capabilities of edge devices in distributed energy systems. Blockchain-Imbalanced FL requires high computational resources for class imbalance correction algorithms, limiting its deployment to computationally capable nodes. In contrast, Basic FL with Blockchain Logging and Blockchain-Assisted Split FL maintain low computational overhead through simplified blockchain integration, making them suitable for resource-constrained environments.

4.6.3. Performance-resource trade-off implications

The comparative analysis reveals that optimal BlockFL deployment requires multi-objective optimization considering privacy requirements, performance specifications, and resource constraints. High-throughput applications with moderate privacy requirements benefit from energy-efficient lightweight approaches, while privacy-critical applications may necessitate resource-intensive cryptographic solutions despite performance penalties. The hierarchical and sharded approaches provide intermediate solutions, offering enhanced scalability at increased implementation complexity but manageable energy consumption.

Summary: These findings suggest that practical BlockFL deployment in DER systems requires adaptive architecture selection based on specific operational requirements, available computational resources, and privacy sensitivity levels, rather than adopting a uniform solution across diverse grid applications.

5. Recent advances of BlockFL for DERs

This section presents recent advances of BlockFL for DER cyber security in the literature. The solutions are first analyzed with respect to the four layers of DERs, and then mapped to the five stage of the cyber security life cycle. Finally, the advantages and disadvantages of the techniques are highlighted.

5.1. BlockFL for the four-layer cyber security framework

BlockFL solutions across the four DER cyber security layers are discussed in the following and summarized in Table 7.

5.1.1. Device layer

At the lowest layer, DERs face threats such as sensor tampering, side-channel attacks, hardware Trojans, and unauthorized physical access. These risks are exacerbated in remote, unguarded installations such as off-grid microgrids or residential solar units. Blockchain can provide secure device identities and immutable provenance records for hardware components. By registering unique device IDs and audit trails on-chain [93], operators can trace and verify the origin and authenticity of hardware, thereby reducing the risk of counterfeit devices and tampering. FL offers a privacy-preserving mechanism for

local anomaly detection. For example, lightweight FL models can be deployed on edge devices to detect unusual sensor patterns or hardware behaviors without uploading sensitive raw data. [94] demonstrated this in renewable energy forecasting, showing that FL enables high accuracy while preserving data confidentiality.

5.1.2. Firmware layer

Firmware manipulation or unauthorized updates to the control algorithms in this layer can introduce catastrophic consequences, such as power instability or device failure. Blockchain can be used to ensure the integrity of firmware through tamper-proof version control and update validation. [95] proposed using blockchain to manage secure data exchanges between electric vehicles and central energy dispatch systems, with applications extendable to DER firmware validation. Smart contracts can be programmed to allow only authenticated and authorized updates to control software. FL can monitor firmware behavior across multiple DERs and learn patterns of firmware manipulation or misconfiguration. [95,96] both applied FL to detect model anomalies and predict system performance in a privacy-preserving manner. FL can thus help distinguish between genuine firmware malfunctions and coordinated attacks, enabling secure model sharing without centralized data exposure.

5.1.3. Cyber network layer

Communication vulnerabilities, such as DoS, man-in-the-middle attacks, and ransomware infiltration into SCADA, pose serious threats to DER coordination and grid stability. Blockchain enhances communication integrity and resilience by securing peer-to-peer communications with time-stamped transactions and immutable logs, any unauthorized modifications or delays can be traced and audited [96–98]. Hierarchical or dew-based blockchain architectures, such as those implemented by [97], can also reduce latency and improve the reliability of communications between distributed nodes. FL can be used to build collaborative intrusion detection systems across DER sites. [85,94] applied FL for distributed prediction and forecasting, achieving high accuracy while mitigating data privacy risks. These same methods can be adapted to detect anomalies in traffic patterns, unauthorized signal injection, or abnormal device behavior in the network, making real-time detection scalable and adaptive.

5.1.4. DERMS application layer

The DERMS layer manages energy scheduling, market bidding, grid services, and coordination of multiple DER units. It is vulnerable to higher-level attacks such as adversarial machine learning poisoning, false data injection, or economic manipulation (e.g., false bidding or dispatch signals). Blockchain smart contracts and consensus mechanisms ensure transparency and enforce correct behavior in DERMS logic. [97] used dew-computing blockchain with federated trading logic to ensure privacy and profitability in peer-to-peer markets. [86] employed a proof-of-state-of-charge consensus for validating EV trading, enhancing trust and reducing transaction fraud. At the DERMS layer, FL allows for decentralized, privacy-preserving model training across DERs while maintaining global accuracy. [98] proposed a hierarchical FL model using convolutional neural network-based bidirectional long short-term memory attention with CKKS homomorphic encryption (CKKS (Cheon-Kim-Kim-Song) allows computation on encrypted data without decryption) to predict EV charging behavior, showing strong privacy and low latency. [84] developed FL scheme for qualified local model selection that achieved robust predictions with 35% fewer transactions, enhancing both cyber security and scalability. A key limitation of these approaches is that bidirectional long short-term memory and CKKS introduce computational overhead, raising concerns for real-time edge deployment.

5.2. BlockFL for cyber-security life cycle

Fig. 6 shows BlockFL solutions mapped across the cyber security lifecycles of DERs.

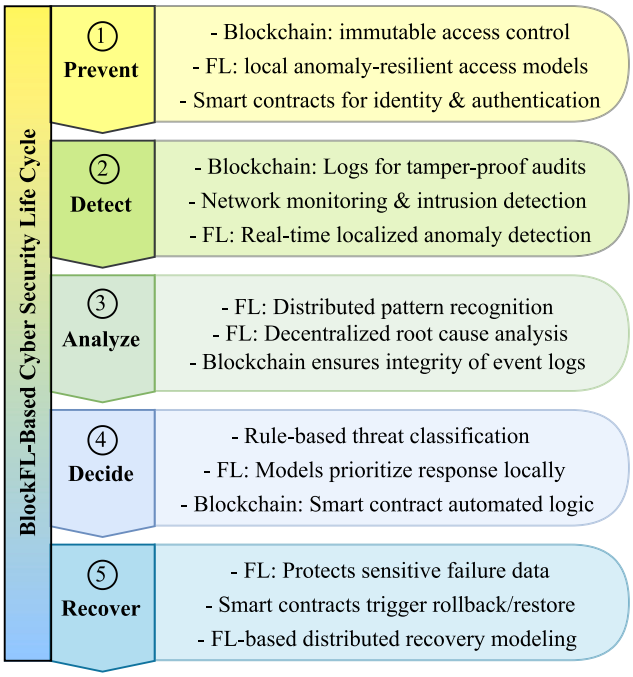

Fig. 6. BlockFL solutions mapped across the cyber security lifecycle of DERs.

5.2.1. Prevention

BlockFL prevents cyber security incidences by removing single points of failure, supporting secure edge intelligence, enforcing immutable access policies, and predicts anomalies before they escalate.

Decentralized authentication and trust. Blockchain eliminates the single point of failure by enabling decentralized identity and access management. Smart contracts enforce access rules, while tamper-proof logs validate network behavior [86,97]. In EV-based virtual power plants, [84] applies FL to predict behaviors and proactively optimize energy management while maintaining secure aggregator-EV interactions on a blockchain.

Privacy-preserving forecasting. [85,94] show that integrating sparse transformer or bidirectional long short-term memory models via FL avoids data exposure while improving renewable energy and EV load forecasting. This reduces attack surfaces on centralized data lakes.

Tamper-proof policy enforcement. [98] used hierarchical blockchain to enforce access control and encrypted FL model exchanges using CKKS, preventing unauthorized interventions in EV charging networks.

5.2.2. Detection

BlockFL enables early detection via distributed data patterns, nonrepudiation and traceability of cyber events, and combined real-time model feedback with historical audit logs.

Anomaly detection with federated models. [95,96] employ FL for real-time anomaly detection without compromising data locality, improving responsiveness.

Blockchain-logged evidence trails. Every FL model update and node behavior can be logged immutably on blockchain [94], ensuring transparent detection of tampering or poisoned models.

Cross-node intelligence sharing. In peer-to-peer microgrids, [97] use blockchain to aggregate insights from distributed dew servers. Anomalies in transactions or data patterns are detected by correlating logs across the network.

Table 7
Integrated blockchain-federated learning solutions across DER cyber security layers.

Layer	Challenges	Blockchain solution	Federated learning solution
Device Layer	- Sensor/data tampering - Hardware Trojans - Physical access vulnerabilities	- Hardware identity verification via blockchain [93] - Tamper-proof component provenance records	- Lightweight FL models for local anomaly detection [94] - Local drift detection without raw data exposure
Firmware Layer	- Maximum power-point tracking or converter logic manipulation - Compromised firmware updates - Insider threats via legacy access	- Immutable firmware logs and version control on blockchain [95] - Smart contract-based update validation	- Anomaly detection using FL across DERs [95,96] - Encrypted gradient sharing in FL
Cyber Network Layer	- Man-in-the-middle attacks - Denial of Service (DoS) - Spoofed control signals - Packet interception	- Blockchain-secured communications with integrity checks [96], [97] - Time-stamped immutable logs [98]	- Distributed FL intrusion detection systems [94] - Traffic anomaly detection via local FL agents
DERMS Application Layer	- Scheduling/dispatch manipulation - Adversarial ML attacks - False market bids or poisoned models	- Smart contracts for policy enforcement [97] - Proof of SoC for transaction validation [86]	- Encrypted hierarchical FL models [98] - Distributed model training to resist poisoning [84]

5.2.3. Analysis

BlockFL provides immutable, time-sequenced forensic data, allows collaborative threat attribution across organizations and maintains confidentiality during cyber incident analysis.

Forensic integrity with blockchain. With blockchain maintaining a tamper-proof history of actions, analysts can trace event chains and attribute malicious activity reliably [93].

Distributed model comparison. FL enables comparison of local model deviations to identify malicious or compromised nodes [99]. For instance, if a subset of clients shows model divergence, it may signal a poisoning attack.

Secure and auditable aggregation. Federated model updates stored on blockchain allow secure backtracking and root cause analysis, while preserving local data privacy [86].

Edge-centric correlation. Smart contracts and FL coordination allow local logs to be analyzed in correlation with global events [100], enhancing threat attribution across charging infrastructure.

5.2.4. Decision

BlockFL reduces reaction time through local decision-making, eliminates human bottlenecks via smart contracts and increases decision trust via consensus mechanisms.

Autonomous smart contracts. Blockchain-based smart contracts [97, 101] automate decisions like isolating a node or triggering re-authentication, without central authority delays.

Adaptive learning with FL. FL facilitates fast local model updates in response to new threats [85], enabling near-real-time decision-making without retraining the full global model.

Weighted model aggregation. Trust scores and model accuracy metrics logged on-chain can inform decision-making in FL aggregation [94], balancing participation against risk.

5.2.5. Recovery

BlockFL maintains operational continuity, provides trusted state snapshots, and facilitates long-term resilience through collaboration.

Model rollbacks and reinitialization. Since blockchain stores prior FL updates immutably, it enables trusted rollback to known-good model versions [54].

Dynamic reconfiguration of network trust. Compromised or underperforming nodes can be flagged and excluded through consensus mechanisms, while the rest of the network continues functioning securely [84].

Distributed data revalidation. Blockchain-backed logs and federated metrics can be revalidated to restore operational parameters post-attack without risking data leakage [98].

Collaborative reputation recovery. Federated approaches using blockchain can help nodes rebuild their trust scores through validated contributions over time.

5.3. Overall evaluation

Table 8 summarizes the features of the key literature on BlockFL. Across these studies, blockchain serves as a foundational trust anchor, enabling secure validation of transactions, coordinated agent interactions, and tamper-proof management of model updates. Its immutability ensures data integrity, which is essential in highly decentralized environments such as EV charging networks, peer-to-peer energy trading, and smart microgrids. In parallel, FL offers scalable and privacy-preserving intelligence, allowing edge devices like electric vehicles, prosumers, and sensors to collaboratively train global models without disclosing raw data. This is particularly valuable for applications such as load forecasting, user utility optimization, and dynamic energy pricing. Many recent studies adopt hybrid architectures, including hierarchical or semi-decentralized topologies [96–98], to strike a balance between local autonomy and global coordination. Notably, FL models tend to experience only marginal performance degradation—typically around 1.7–5.7%—relative to centralized training approaches, indicating that the trade-off between accuracy and privacy is acceptable in practical implementations.

Nevertheless, the integration of blockchain and FL presents several technical and operational challenges. Resource constraints remain a primary concern, as both technologies introduce additional computational and communication overhead—especially on low-power edge devices. Promising research directions include model compression, adaptive consensus algorithms, and lightweight encryption methods. Furthermore, interoperability issues arise from the use of non-standardized blockchain protocols and consensus mechanisms such as Avalanche or Proof-of-State-of-Charge, which may limit seamless integration with conventional grid infrastructures. The complexity of embedding FL logic within smart contracts, as explored in works like [101], also introduces difficulties in scaling and debugging. In addition, while some consensus mechanisms like Proof of Authority and Federated Byzantine

Table 8
Summary of key literature on integrated blockchain-federated learning for DERs.

Reference	Application	Blockchain type	Key contribution	Advantage	Disadvantage
Electric Vehicle Applications					
[96]	EVs in VPPs	Not specified	AI-chip and blockchain-based EV integration using FL	Cost-efficient and secure	Slight accuracy drop in FL; memory and latency overhead
[84]	EVs in VPPs	Semi-decentralized blockchain	FL-QLMS algorithm with reduced transactions and improved prediction	5.7% better RMSE; robust against attacks	FL-QLMS implementation complexity
[86]	EV energy trading	Avalanche blockchain	Federated reinforcement learning + Proof of State of Charge	High user utility; validated in real-world blockchain	Complexity of custom consensus
[95]	Smart EV consumer electronic devices in cities	Not specified	Privacy-aware FL with blockchain for secure smart EV data sharing	Secure data exchange; system reliability	Generic blockchain, lacks deployment details
[98]	EV charging networks	Hierarchical blockchain	FL with CNN-BiLSTM-Attention + Cheon-Kim-Kim-Song (CKKS) encryption	Low latency, high accuracy, strong privacy	Homomorphic encryption is computationally heavy
[85]	EV load forecasting	Decentralized blockchain	Block-FeDL: BiLSTM + blockchain-based FL aggregation	Up to 96% MAE improvement; decentralized learning	High model complexity; heavy BiLSTM computation
[99]	EV charging recommender system	Blockchain for cloudlet communication	Vertical FL + blockchain to preserve EV user privacy	Reduced latency, improved security	Limited generalization beyond cloudlet clusters
[100]	Vehicle-to-grid (V2G) operation	Distributed ledger	Privacy-preserving V2G scheduling using FL and edge computing	Scalability, reduced latency, data protection	Needs intelligent edge devices at all charging points
Energy Trading and Microgrids					
[97]	P2P Energy Trading	Dew-computing blockchain	BDC-FL system for private, profitable energy trading	Up to 18% profit gain; privacy-preserving	Requires dew-computing infrastructure
[102]	Secure energy trading in microgrids	Not specified (edge computing based)	Distributed framework for energy trading using blockchain and FL	Trustworthy, secure, real-time edge trading	Implementation complexity in vehicular environments
[101]	Energy trading and sharing among microgrids	Smart contracts on blockchain	Hybrid P2P energy trading/sharing with smart contracts	Autonomous switching between trade/share; privacy	Complexity in forecasting and switching logic
Renewable Energy Systems and Forecasting					
[94]	RES prosumer forecasting	Blockchain-integrated FL	Sparse Transformer in FL for renewable energy forecasting	Up to 20.4% MSE improvement; privacy-preserving	Training complexity of Transformer models
[54]	Blade icing detection in wind turbines	Blockchain-enhanced FL	BlockFL framework with validation and imbalanced learning	Improves privacy and robustness of detection	Added complexity for validation/imbalance handling
Grid Control and Management					
[103]	Decentralized frequency control in islanded MG	Proof-of-Authority	Smart contract participation matrix for P2P trading	Robust frequency control, decentralized contracts	Complexity in design and validation
[104]	Guarantee of Origin verification	Federated Byzantine Agreement (FBA)	Blockchain platform for Guarantee of Origin traceability compatible with European Energy Certificate System	Fast processing, low energy consumption	FBA adoption complexity and scalability limitations
General Frameworks and Taxonomies					
[93]	Internet of Energy	Not specified	Classified models combining blockchain, smart contracts, and FL in internet of energy	Broad overview and taxonomy; clear research directions	No experimental implementation or quantitative analysis

VPP is virtual power plant, P2P is peer to peer, QLMS is quaternionic least mean squares, BDC is blockchain and dew computing, RMSE is root mean square error, and CNN-BiLSTM is hybrid Convolutional Neural Networks and Bidirectional Long Short-Term Memory networks.

Agreement offer reduced latency and energy use, they may compromise decentralization and fault tolerance. Finally, data heterogeneity and non-IID (non-independent and identically distributed) characteristics—common in dynamic systems such as EV fleets and wind farms—continue to pose unresolved challenges for robust federated model training.

6. Challenges and future trends

The preceding state-of-the-art literature review reveals several persistent challenges that hinder the seamless integration of BlockFL DER systems. These challenges span technical, operational, and systemic domains, impacting the scalability, security, and efficiency of such integrations. While early BlockFL systems were only required for simply logging updates securely, present-day BlockFL systems are active in aggregation, incentives, and privacy proofs. Based on current research directions, and emerging technological capabilities, future trends include BlockFLs with sector-optimized multi-chains which are quantum-safe and are autonomously incentivized. This section is a comprehensive discussion on the challenges and future trends of BlockFL solutions for DER systems.

6.1. Challenges

6.1.1. Resource constraints on edge devices and network

The embedded processing units on DERs often have limited computational power, storage capacity, and energy resources. However, several BlockFL architectures propose the concurrent execution of FL

Table 9
Existing standards for blockchain and federated learning.

Standard	Scope	Specification	Relevance
IEEE 3230.02-2024 [105]	Blockchain Testing Specification	Definitions, types, test specifications, test methods, and test processes for blockchain systems including functional, performance, security, stability, and compliance testing	Provides testing framework for blockchain components in DER management systems
IEEE 3127-2025 [106]	Blockchain-based Federated ML Framework	Architectural framework guide for blockchain-based federated machine learning systems integration	Directly addresses BlockFL integration challenges for DER applications
IEEE 3241.01-2024 [107]	Blockchain in Low Carbon Zones	Standard for using blockchain technology in low carbon zone evaluation and management	Specific to renewable energy and carbon footprint tracking in DER systems
IEEE 3217-2023 [108]	Blockchain Application Interface	API collection and data transmission format between chain layer and application layer in blockchain systems	Standardizes DER system integration with blockchain networks
IEEE 2418.2-2020 [109]	Blockchain Data Format	Data format requirements, structures, types, and elements for blockchain systems	Ensures interoperability of DER data across blockchain platforms
ISO/TC 307 [110]	Blockchain and DLT Technologies	Comprehensive standardization framework for blockchain technologies and distributed ledger technologies	Foundational standards applicable to all DER blockchain implementations
ITU-T Y.4476 [111]	IoT Data Management via Blockchain	Recommendation for Internet of Things data management using blockchain technology	Addresses smart grid IoT device data management and security
ITU-T Y.2342 [112]	Next-Generation Networking	Architectural framework for next-generation networking technologies	Network infrastructure standards for distributed DER communications
ITU-T F.751.2 [113]	Secure Blockchain Processes	Standardized security processes and protocols for blockchain implementations	Security framework for critical power system blockchain applications

DER = Distributed Energy Resources; FL = Federated Learning; IoT = Internet of Things; API = Application Programming Interface DLT = Distributed Ledger Technology.

training and blockchain operations (mining and consensus participation), which exacerbate these limitations, and can lead to potential system inefficiencies. Furthermore, blockchain systems require increased storage demands, while FL necessitates frequent communication between clients and servers for model updates. These factors can also increase network overheads and impact system performance.

6.1.2. Data heterogeneity and non-independent or identical distributions

FL schemes often assume that data on edge devices is independent and identically distributed (IID) across clients. However, DER systems can have non-IID data due to geographical, temporal, and operational differences. This non-IID nature of data can lead to biased global models and reduced convergence rates.

6.1.3. Consensus mechanism efficiency and scalability

Traditional blockchain consensus mechanisms, such as PoW and PoS, are often resource-intensive and may not be suitable for the dynamic and resource-constrained environments of DER systems. These mechanisms can introduce significant latency and energy consumption, hindering real-time operations. Proof of authority (PoA) consensus mechanism is a highly energy-efficient alternative as it eliminates the need for computationally intensive mining.

6.1.4. Smart contract vulnerabilities

Smart contracts can be susceptible to various vulnerabilities such as incorrect exception handling and parameter type confusion. Adversaries could take advantage of these weaknesses to disrupt operations or gain unauthorized access. Since these smart contracts are associated with FL processes in BlockFl, it is crucial to ensure their security and accuracy.

6.1.5. Interoperability and standardization challenges

The lack of standardized protocols and frameworks for integrating blockchain and FL in DER systems poses significant interoperability challenges. Although several standards have been published for IoT and network applications Table 9, their specifications do not always explicitly address the unique characteristics of DERs in smart grids. Also, diverse blockchain platforms and FL frameworks may not seamlessly interact, leading to fragmented systems and increased complexity in deployment and maintenance.

6.1.6. Security threats

Both blockchain and FL systems are susceptible to various security threats earlier outlined. Ensuring robust security measures to detect and mitigate such threats is essential for maintaining the trustworthiness of BlockFL systems.

6.1.7. Lack of standardized pilot projects

Despite the significant research progress, a major challenge hindering the widespread adoption of BlockFL in DERs is the limited number of large-scale, real-world pilot projects and commercial deployments. Most current validation efforts are confined to laboratory-scale prototypes, simulations using synthetic or historical data, or conceptual frameworks. Bridging this gap requires collaborative efforts between academia, industry, and regulatory bodies to de-risk pilot deployments and demonstrate scalability and reliability in live grid environments.

6.2. Future research trends

6.2.1. Multi-chain federated learning

Multi-chain FL involves FL systems operating across multiple heterogeneous interacting blockchains with sophisticated cross-chain consensus mechanisms. This means different lightweight blockchains can specialize in different types of DERs while still contributing to a unified energy management system. This architecture is crucial for integrating diverse energy networks that span multiple geographic regions, regulatory jurisdictions, and energy resource types. A multi-chain system can include specialized blockchains for solar PV performance optimization, wind farm output prediction, vehicle-to-grid coordination, and energy storage management. Cross-chain protocols would enable these specialized systems to contribute to global grid optimization while maintaining their domain-specific operations.

6.2.2. Quantum-resilient BlockFL

Energy infrastructure are critical infrastructure with long lifecycle requirements. Quantum-resilient BlockFL incorporates post-quantum cryptographic algorithms into both blockchain protocols and FL systems to ensure security against future quantum computing attacks. This

can be done by replacing current cryptographic primitives with post-quantum alternatives in both blockchain transaction verification and FL model update encryption. This ensures that even if quantum computers become capable of breaking current cryptography, historical energy data and trained models remain secure.

Gharavi et al. [114] proposed a post-quantum blockchain-based protocol for FL which integrates post-quantum cryptographic algorithms to counter quantum threats posed by Shor and Grover algorithms. The hybrid communication strategy provides computational cost optimization while maintaining $O(n^2)$ communication complexity across FL rounds. Another approach is a multivariate polynomial-based cryptography [115] that offers practical computationally-efficient quantum resilience, enabling immutable logging and access control while preserving privacy in DERs. Gurung et al.'s [116] hybrid stateless-stateful signature scheme combines Dilithium or Falcon with XMSS hash-based schemes, leveraging both computational efficiency and proven quantum resistance. The verifiable random function integration strengthens blockchain consensus mechanisms while optimizing performance based on computational power and stake accumulation.

6.2.3. Verifiable computation for FL

This trend involves smart contracts not only logging model updates but actively verifying the correctness of FL training using zero-knowledge proofs, without revealing the underlying data. Verification is critical in DERs where incorrect models could lead to grid instability or inefficient resource allocation. This can involve renewable energy plants proving correctly trained forecasting models on their actual generation data without revealing proprietary information on hardware configurations or exact generation patterns.

6.2.4. Autonomous incentive mechanisms

Blockchain-based decentralized autonomous organizations can autonomously manage FL incentives by rewarding high-quality model updates and penalizing lazy or malicious nodes through programmatic governance. For instance, there can be independent evaluations of the quality of wind farm production forecasts contributed to a collaborative prediction model, distributing token rewards based on forecast accuracy. This would incentivize the continuous improvement of forecasting models while penalizing poor contributions.

6.2.5. Adaptive blockchain layering

Adaptive blockchain layering involves protocols that dynamically switch between on-chain and off-chain processing based on FL workload requirements, network conditions, and security needs. During normal grid operations, energy forecasting models might update using lightweight off-chain channels. When critical events occur (extreme weather, demand spikes), the system would automatically transition to full on-chain validation to ensure maximum security and consensus during high-risk periods.

6.2.6. Federated analytics with blockchain

A federated analytics system might analyze patterns across thousands of home battery systems to predict available capacity for grid services, without ever centralizing the data about individual households. Blockchain would secure the analytics process and ensure fair compensation for participation.

7. Conclusion

This paper has presented an in-depth examination of integrating blockchain and federated learning to enhance cybersecurity in distributed energy resources. This comprehensive analysis establishes that architecture selection necessitates careful consideration of inherent performance trade-offs, where computational efficiency conflicts with security guarantees, scalability requirements compete with implementation complexity, and deployment context across device, firmware, network, and application layers determines optimal architectural choices for achieving desired operational objectives in distributed energy resource management. The review of recent integrated blockchain and federated learning architectures demonstrates that while significant advances have been made, particularly in privacy preservation, distributed intelligence, and trustless coordination, challenges such as interoperability, computational load, and consensus scalability remain. Also, while integrated blockchain and federated learning presents a promising solution for secure, reliable, and scalable next-generation smart grids, its full potential will be realized as more comprehensive real-world validations and pilot projects emerge to demonstrate its practical efficacy and address implementation challenges. Moving forward, future integrated blockchain and federated learning systems must evolve beyond basic security logging to support active coordination, privacy proofs, and dynamic incentives.

Nomenclature

BlockFL	Integrated blockchain-federated learning
DER	Distributed energy resource
DERMS	DER management system
EV	Electric vehicle
FL	Federated learning
IoT	Internet of things
MARL	Multi-agent reinforcement learning
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof-of-stake
PoW	Proof-of-work
SCADA	Supervisory control and data acquisition

CRediT authorship contribution statement

Oluleke O. Babayomi: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Ikechi Saviour Igboanusi:** Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Data curation. **Love Allen Chijioke Ahakonye:** Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Data curation. **Dong-Seong Kim:** Writing – review & editing, Validation, Supervision, Project administration, Methodology, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported in part (40%) by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612) and in part (30%) by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003) and in part (30%) by the Institute of Information & Communications Technology Planning & Evaluation(IITP)-ITRC(Information Technology Research Center) grant funded by the Korea government (Ministry of Science and ICT)(IITP-2025-RS-2024-00438430). The authors acknowledge permission received for the use of icons from iconscout.com.

Data availability

Data will be made available on reasonable request.

References

[1] Zhuang P, Zamir T, Liang H. Blockchain for cybersecurity in smart grid: A comprehensive survey. IEEE Trans Ind Informatics 2020;17(1):3–19.

[2] Chen J, Yan J, Kemmeugne A, Kassouf M, Debbabi M. Cybersecurity of distributed energy resource systems in the smart grid: A survey. Appl Energy 2025;383:125364.

[3] Babayomi O, Zhang Z, Dragicevic T, Hu J, Rodriguez J. Smart grid evolution: Predictive control of distributed energy resources—A review. Int J Electr Power Energy Syst 2023;147:108812.

[4] Rahman MA, Mohsenian-Rad H, Sridharan V, Burnett AK. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Trans Smart Grid 2024;15(3):2836–47.

[5] Zhang Z, Babayomi O, Dragicevic T, Heydari R, Garcia C, Rodriguez J, Kennel R. Advances and opportunities in the model predictive control of microgrids: Part I–primary layer. Int J Electr Power Energy Syst 2022;134:107411.

[6] Sugunaraj N, Balaji SRA, Chandar BS, Rajagopalan P, Kose U, Loper DC, Mahfuz T, Chakraborty P, Ahmad S, Kim T, Apruzzese G, Dubey A, Strezoski L, Blakely B, Ghosh S, Reddy MJB, Padullaparti HV, Ranganathan P. Distributed energy resource management system (DERMS) cybersecurity scenarios, trends, and potential technologies: A review. IEEE Commun Surv & Tutorials 2025;1.

[7] Mollah MB, Zhao J, Niyato D, Lam K-Y, Zhang X, Ghias AMYM, Koh LH, Yang L. Blockchain for future smart grid: A comprehensive survey. IEEE Internet Things J 2021;8(1):18–43.

[8] Yap KY, Chin HH, Klemeš JJ. Blockchain technology for distributed generation: A review of current development, challenges and future prospect. Renew Sustain Energy Rev 2023;175:113170.

[9] Zhang Z, Rath S, Xu J, Xiao T. Federated learning for smart grid: A survey on applications and potential vulnerabilities. 2024, arXiv preprint arXiv:2409.10764.

[10] Wu C, Wu F, Cao Y, Huang Y, Xie X. Communication-efficient federated learning via knowledge distillation. Nat Commun 2022;13(2032).

[11] McMahan HB, Moore E, Ramage D, Hampson S, y Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics. PMLR; 2017, p. 1273–82.

[12] Wendl M, Doan MH, Sassen R. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. J Environ Manag 2023;326:116530.

[13] Pacheco M, Oliva G, Rajbahadur GK, Hassan A. Is my transaction done yet? An empirical study of transaction processing times in the ethereum blockchain platform. ACM Trans Softw Eng Methodol 2023;32(3).

[14] Utkarsh K, Srinivasan D. Distributed machine learning in energy management and control in smart grid. In: Women in computational intelligence: key advances and perspectives on emerging topics. Springer; 2022, p. 219–51.

[15] Zhang W, Zhou Q, Tang Q, Xiong N, Zhang Y. Blockchained federated learning for internet of things: A comprehensive survey. ACM Comput Surv 2024;57(1):1–43.

[16] Kumari A, Shukla D, Datt R, Patel A, Kumar P, Kumar S, K A, Katarmal U. S-EVPF: A secure and decentralized EV prediction framework using federated learning. In: 2024 eighth international conference on parallel, distributed and grid computing. PDGC, 2024, p. 658–63.

[17] Asante M, Epiphaniou G, Maple C, Al-Khateeb H, Bottarelli M, Ghafoor KZ. Distributed ledger technologies in supply chain security management: A comprehensive survey. IEEE Trans Eng Manage 2023;70(2):713–39.

[18] Sugunaraj N, Balaji SRA, Chandar BS, Rajagopalan P, Kose U, Loper DC, Mahfuz T, Chakraborty P, Ahmad S, Kim T, Apruzzese G, Dubey A, Strezoski L, Blakely B, Ghosh S, Reddy MJB, Padullaparti HV, Ranganathan P. Distributed energy resource management system (DERMS) cybersecurity scenarios, trends, and potential technologies: A review. IEEE Commun Surv & Tutorials 2025;1.

[19] Albertini AR, Yabe VT, Di Santo SG. Distributed energy resources management systems (DERMS). In: Sguarezi Filho AJ, Jacomini RV, Capovilla CE, Casella IRS, editors. Smart grids—renewable energy, power electronics, signal processing and communication systems applications. Cham: Springer International Publishing; 2024, p. 143–72.

[20] Tayebi S, Amini H. The flip side of the coin: Exploring the environmental and health impacts of proof-of-work cryptocurrency mining. Environ Res 2024;252:118798.

[21] Rukhiran M, Boonsong S, Netinant P. Sustainable optimizing performance and energy efficiency in proof of work blockchain: A multilinear regression approach. Sustainability 2024;16(4).

[22] Sukhwani H, Martínez JM, Chang X, Trivedi KS, Rindos A. Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In: 2017 IEEE 36th symposium on reliable distributed systems. SRDS, 2017, p. 253–5.

[23] Ramaswamy V, Penny D. On the performance of PBFT-based permissioned blockchain networks in constraint environments. In: ICC 2021 - IEEE international conference on communications. 2021, p. 1–6.

[24] Ahmad S, Nakka K, Kim T, Han D, Won D, Ahn B. Blockchain-assisted resilient control for distributed energy resource management systems. IEEE Access 2024;12:191748–62.

[25] Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N. The transparency challenge of blockchain in organizations. Electron Mark 2022;32(3):1779–94.

[26] Han D, Zhu Y, Li D, Liang W, Souri A, Li K-C. A blockchain-based auditable access control system for private data in service-centric IoT environments. IEEE Trans Ind Informatics 2022;18(5):3530–40.

[27] Omar IA, Jayaraman R, Salah K, Simsekler MCE, Yaqoob I, Ellahham S. Ensuring protocol compliance and data transparency in clinical trials using blockchain smart contracts. BMC Med Res Methodol 2020;20(1):224.

[28] Saxena S, Farag HEZ, Brookson A, Turesson H, Kim H. A permissioned blockchain system to reduce peak demand in residential communities via energy trading: A real-world case study. IEEE Access 2021;9:5517–30.

[29] Nakai T, Sakurai A, Hironaka S, Shudo K. A formulation of the trilemma in proof of work blockchain. IEEE Access 2024;12:80559–78.

[30] Han H-JK, Han S-S. TPS analysis, performance indicator of public blockchain scalability. J Inf Process Syst 2024;20(1):85–92, Available DOI: 10.3745/JIPS.04.0304.

[31] Neiheiser R, Inácio G, Rech L, Montez C, Matos M, Rodrigues L. Practical limitations of ethereum's layer-2. IEEE Access 2023;11:8651–62.

[32] Negka LD, Spathoulas GP. Blockchain state channels: A state of the art. IEEE Access 2021;9:160277–98.

[33] Thibault LT, Sarry T, Hafid AS. Blockchain scaling using rollups: A comprehensive survey. IEEE Access 2022;10:93039–54.

[34] Hashim F, Shuaib K, Zaki N. Sharding for scalable blockchain networks. SN Comput Sci 2022;4(1):2, Available DOI: 10.1007/s42979-022-01435-z.

[35] Jain AK, Gupta N, Gupta BB. A survey on scalable consensus algorithms for blockchain technology. Cyber Secur Appl 2025;3:100065, Available https://www.sciencedirect.com/science/article/pii/S2772918424000316.

[36] Amadi CS, Ajakwe SO, Igboanusi IS, Kim D-S, Jun T. Lightweight federated learning and blockchain system for industrial IoT big data security. In: 2024 15th international conference on information and communication technology convergence. ICTC, 2024, p. 2009–14.

[37] Nnadiekwe CA, Igboanusi IS, Lee JM, Kim D-S. Revolutionizing healthcare supply chains with a blockchain framework for NFT-based product certification and inventory management. In: 2025 international conference on artificial intelligence in information and communication. ICAIIC, 2025, p. 0454–8.

[38] Kim D-S, Igboanusi IS, Chijioke Ahakonye LA, Anyanwu GO. Proof-of-authority-and-association consensus algorithm for IoT blockchain networks. In: 2025 IEEE international conference on consumer electronics. ICCE, 2025, p. 1–6.

[39] Igboanusi IS, Allwinnaldo A, Alief RN, Ansori MRR, Lee J-M, Kim D-S. Smart auto mining (SAM) for industrial IoT blockchain network. IET Commun 2022;16(18):2123–32, Available https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cmu2.12465.

[40] Umar A, Kumar D, Ghose T. Blockchain-based decentralized energy intra-trading with battery storage flexibility in a community microgrid system. Appl Energy 2022;322:119544.

[41] Saeed N, Wen F, Afzal MZ. Decentralized peer-to-peer energy trading in microgrids: Leveraging blockchain technology and smart contracts. Energy Rep 2024;12:1753–64.

[42] Rana MT, Numan M, Yousif M, Hussain T, Khan AZ, Zhao X. Enhancing sustainability in electric mobility: Exploring blockchain applications for secure EV charging and energy management. Comput Electr Eng 2024;119:109503.

[43] Diaz-Valdivia A, Poblet-Balcell M. The governance of the ReFi ecosystem: Integrity in voluntary carbon markets as a common resource. Int J the Commons 2025;19(1):100–19.

[44] Cantillo-Luna S, Moreno-Chuquen R, Chamorro HR, Sood VK, Badsha S, Konstantinou C. Blockchain for distributed energy resources management and integration. IEEE Access 2022;10:68598–617.

[45] Augello A, Gallo P, Sanseverino ER, Sciumè G, Tornatore M. A coexistence analysis of blockchain, SCADA systems, and openadr for energy services provision. IEEE Access 2022;10:99088–101.

[46] Finck M. Blockchains: Regulating the unknown. Ger Law J 2018;19(4):665–92.

[47] Akkaoui R, Stefanov A, Palensky P, Epema DHJ. A taxonomy and lessons learned from blockchain adoption within the internet of energy paradigm. IEEE Access 2022;10:106708–39.

[48] Tran QT, Luu NA, Amicarelli E, et al. Distributed energy resource management system. In: Local electricity markets. Elsevier; 2021, p. 159–75.

[49] Strezoski L. Distributed energy resource management systems—DERMS: State of the art and how to move forward. Wiley Interdiscip Rev: Energy Environ 2023;12(1):e460.

[50] Wilk P, Wang N, Li J. Multi-agent reinforcement learning for smart community energy management. Energies 2024;17(20):5211.

[51] Feng N, Ran C. Design and optimization of distributed energy management system based on edge computing and machine learning. Energy Informatics 2025;8(1):17.

[52] Giannelos S, Borozan S, Konstantelos I, Strbac G. Option value, investment costs and deployment levels of smart grid technologies. Sustain Energy Res 2024;11(1):47.

[53] Mischos S, Dalagdi E, Vrakas D. Intelligent energy management systems: a review. Artif Intell Rev 2023;56(10):11635–74.

[54] Cheng X, Tian W, Shi F, Zhao M, Chen S, Wang H. A blockchain-empowered cluster-based federated learning model for blade icing estimation on IoT-enabled wind turbine. IEEE Trans Ind Informatics 2022;18(12):9184–95.

[55] Anjana M, Devidas AR, Ramesh MV. Federated learning-enabled energy management in smart buildings for sustainability. In: International conference on innovative computing and communication. Springer; 2024, p. 349–57.

[56] Darshi R, Shamaghdari S, Jalali A, Arasteh H. Decentralized energy management system for smart microgrids using reinforcement learning. IET Gener Transm Distrib 2023;17(9):2142–55.

[57] Martínez A, Arévalo P. Distributed peer-to-peer optimization based on robust reinforcement learning with demand response: A review. Computers 2025;14(2):65.

[58] Lami B, Alsolami M, Alferidi A, Slama SB. A smart microgrid platform integrating AI and deep reinforcement learning for sustainable energy management. Energies 2025;18(5):1157.

[59] Gharbi A, Ayari M, Elkamel A, Elsayed MS, Klai Z, Khedhiri N. A reinforcement learning framework for decentralized decision-making in smart energy systems. Int J Multiphysics 2024;18(4).

[60] Zekiye A, Özkasap Ö. Blockchain-based federated learning for decentralized energy management systems. In: 2023 fifth international conference on blockchain computing and applications. BCCA, 2023, p. 186–93.

[61] Ahmad S, Nakka K, Kim T, Han D, Won D, Ahn B. Blockchain-assisted resilient control for distributed energy resource management systems. IEEE Access 2024;12:191748–62.

[62] Zhang K, Yang Z, Liu H, Zhang T, Basar T. Fully decentralized multi-agent reinforcement learning with networked agents. In: Dy J, Krause A, editors. Proceedings of the 35th international conference on machine learning. Proceedings of machine learning research, 80, PMLR; 2018, p. 5872–81, Available https://proceedings.mlr.press/v80/zhang18n.html.

[63] Kumari A, Kakkar R, Tanwar S, Garg D, Polkowski Z, Alqahtani F, Tolba A. Multi-agent-based decentralized residential energy management using deep reinforcement learning. J Build Eng 2024;87:109031.

[64] Monon JS, Barua DD, Khan MM. Enhancing heterogeneous multi-agent cooperation in decentralized marl via GNN-driven intrinsic rewards. 2024, http://dx.doi.org/10.48550/arXiv.2408.06503, arXiv preprint arXiv:2408.06503.

[65] Gao J, Wang W, Nikseresht F, Govinda Rajan V, Campbell B. Pfdrl: Personalized federated deep reinforcement learning for residential energy management. In: Proceedings of the 52nd international conference on parallel processing. 2023, p. 402–11.

[66] Lee S, Xie L, Choi D-H. Privacy-preserving energy management of a shared energy storage system for smart buildings: A federated deep reinforcement learning approach. Sensors 2021;21(14):4898.

[67] Ju Z, Wei T, Shen F. BEFL: Balancing energy consumption in federated learning for mobile edge IoT. 2024, http://dx.doi.org/10.48550/arXiv.2412.03950, arXiv preprint arXiv:2412.03950.

[68] Li Y, Li X, Li G, Li Z. Privacy protection in prosumer energy management based on federated learning. IEEE Access 2021;9:16707–15.

[69] Babayomi O, Kim D-S. Federated anomaly detection and mitigation for EV charging forecasting under cyberattacks. In: 2025 international conference on ICT convergence. ICTC, 2025.

[70] Yıldırım F, Yalman Y, Bayındır KÇ, Terciyanlı E. Comprehensive review of edge computing for power systems: State of the art, architecture, and applications. Appl Sci 2025.

[71] Mongaillard T, Lasaulce S, Varma VS. Smart energy management: From conventional optimization to generative AI techniques. In: Internet of vehicles and computer vision solutions for smart city transformations. Springer; 2025, p. 337–61.

[72] Saikia AP, Dey K, Gill A, Gantra A. Leveraging data analytics and ML for enhanced renewable energy resource management. Int J Syst Assur Eng Manag 2025;1–12.

[73] Safari A, Daneshvar M, Anvari-Moghaddam A. Energy intelligence: A systematic review of artificial intelligence for energy management. Appl Sci 2024;14(23):11112.

[74] Ahakonye LAC, Nwakanma CI, Lee J-M, Kim D-S. Low Computational Cost Convolutional Neural Network for Smart Grid Frequency Stability Prediction. Internet Things 2024;25:101086.

[75] Nguyen H-T, Safder U, Loy-Benitez J, Yoo C. Optimal demand side management scheduling-based bidirectional regulation of energy distribution network for multi-residential demand response with self-produced renewable energy. Appl Energy 2022;322:119425.

[76] Mohammadi M, Mohammadi A. Empowering distributed solutions in renewable energy systems and grid optimization. In: Distributed machine learning and computing: theory and applications. Springer; 2024, p. 141–55.

[77] Babayomi O, Zhang Z, Dragicevic T, Heydari R, Li Y, Garcia C, Rodriguez J, Kennel R. Advances and opportunities in the model predictive control of microgrids: Part II–secondary and tertiary layers. Int J Electr Power Energy Syst 2022;134:107339.

[78] Ye J, Giani A, Elasser A, Mazumder SK, Farnell C, Mantooth HA, Kim T, Liu J, Chen B, Seo G-S, et al. A review of cyber–physical security for photovoltaic systems. IEEE J Emerg Sel Top Power Electron 2021;10(4):4879–901.

[79] Sahoo S, Dragičević T, Blaabjerg F. Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities. IEEE J Emerg Sel Top Power Electron 2021;9(5):5326–40.

[80] Ahn B, Kim T, Ahmad S, Mazumder SK, Johnson J, Mantooth HA, Farnell C. An overview of cyber-resilient smart inverters based on practical attack models. IEEE Trans Power Electron 2024;39(4):4657–73.

[81] Babayomi OO, Oluseyi PO. Intelligent fault diagnosis in a power distribution network. 2016;2016:1–10.

[82] Babayomi O, Li Y, Zhang Z, Park K-B. Advanced control of grid-connected microgrids: Challenges, advances, and trends. IEEE Trans Power Electron 2025;40(6):7681–708.

[83] Edwards J. A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice. John Wiley & Sons; 2024.

[84] Wang Z, Ben Abdallah A. A robust multi-stage power consumption prediction method in a semi-decentralized network of electric vehicles. IEEE Access 2022;10:37082–96.

[85] Danish SM, Hameed A, Ranjha A, Srivastava G, Zhang K. Block-fedl: Electric vehicle charging load forecasting using federated learning and blockchain. IEEE Trans Veh Technol 2025;74(2):2048–56.

[86] Moniruzzaman M, Yassine A, Benlamri R. Blockchain and federated reinforcement learning for vehicle-to-everything energy trading in smart grids. IEEE Trans Artif Intell 2024;5(2):839–53.

[87] Feng L, Yang Z, Guo S, Qiu X, Li W, Yu P. Two-layered blockchain architecture for federated learning over the mobile edge network. IEEE Netw 2022;36(1):45–51.

[88] Yuan S, Cao B, Sun Y, Wan Z, Peng M. Secure and efficient federated learning through layering and sharding blockchain. IEEE Trans Netw Sci Eng 2024;11(3):3120–34.

[89] Duan L, Huang H, Li C, Ni W, Cheng B. A novel cross-chain hierarchical federated learning framework for enhancing service security and communication efficiency. IEEE Trans Serv Comput 2025;1–14.

[90] Ebrahimi E, Sober M, Hoang A-T, Ileri CU, Sanders W, Schulte S. Blockchain-based federated learning utilizing zero-knowledge proofs for verifiable training and aggregation. In: 2024 IEEE international conference on blockchain (blockchain). 2024, p. 54–63.

[91] Sai S, Chamola V. A blockchain-enabled split learning framework with a novel client selection method for collaborative learning in smart healthcare. IEEE Trans Consum Electron 2024;70(3):5887–94.

[92] Tong Z, Wang J, Hou X, Chen J, Jiao Z, Liu J. Blockchain-based trustworthy and efficient hierarchical federated learning for UAV-enabled IoT networks. IEEE Internet Things J 2024;11(21):34270–82.

[93] Zekiye A, Özkasap Ö. Blockchain-based federated learning for decentralized energy management systems. In: 2023 fifth international conference on blockchain computing and applications. BCCA, 2023, p. 186–93.

[94] Hameed A, Danish SM, Ranjha A, Srivastava G. Block-fest: Blockchain-enhanced federated sparse transformers for privacy-preserving RES forecasting in internet of vehicles systems. IEEE Internet Things J 2025;1.

[95] Das D, Chaterjee P, Ghosh U, Blakely B. Secure and privacy aware data sharing approach for smart electric vehicles. IEEE Consum Electron Mag 2025;1–7.

[96] Wang Z, Ogbodo M, Huang H, Qiu C, Hisada M, Abdallah AB. AEBIS: AI-enabled blockchain-based electric vehicle integration system for power management in smart grid platform. IEEE Access 2020;8:226409–21.

[97] Singh P, Kaur A, Hedabou M. Blockchain and dew computing-based model for secure energy trading in smart grids. In: 2023 IEEE international conference on communications workshops (ICC workshops). 2023, p. 176–81.

[98] Li B, Guo Y, Du Q, Zhu Z, Li X, Lu R. P^3: Privacy-preserving prediction of real-time energy demands in EV charging networks. IEEE Trans Ind Informatics 2023;19(3):3029–38.

[99] Teimoori Z, Yassine A, Hossain MS. A secure cloudlet-based charging station recommendation for electric vehicles empowered by federated learning. IEEE Trans Ind Informatics 2022;18(9):6464–73.

[100] Shang Y, Li Z, Li S, Shao Z, Jian L. An information security solution for vehicle-to-grid scheduling by distributed edge computing and federated deep learning. IEEE Trans Ind Appl 2024;60(3):4381–95.

[101] Bouachir O, Aloqaily M, Özkasap Ö, Ali F. FederatedGrids: Federated learning and blockchain-assisted P2P energy sharing. IEEE Trans Green Commun Netw 2022;6(1):424–36.

[102] Otoum S, Ridhawi IA, Mouftah H. A federated learning and blockchain-enabled sustainable energy trade at the edge: A framework for industry 4.0. IEEE Internet Things J 2023;10(4):3018–26.

[103] Veerasamy V, Sampath LPMI, Singh S, Nguyen HD, Gooi HB. Blockchain-based decentralized frequency control of microgrids using federated learning fractional-order recurrent neural network. IEEE Trans Smart Grid 2024;15(1):1089–102.

[104] Nofuentes Á, Hernández JJ, Pons L. Blockchain-based guarantees of origin issuing platform. In: 2022 18th international conference on the European energy market. EEM, 2022, p. 1–4.

[105] IEEE. IEEE Standard for Testing Specification of Blockchain Systems. IEEE 3230.02-2024, New York, NY, USA: Institute of Electrical and Electronics Engineers; 2024.

[106] IEEE. IEEE Guide for an Architectural Framework for Blockchain-based Federated Machine Learning. Tech. Rep. IEEE 3127-2025, New York, NY, USA: Institute of Electrical and Electronics Engineers; 2025.
[107] IEEE. IEEE Standard for Using Blockchain in Low Carbon Zones Evaluation. Tech. Rep. IEEE 3241.01-2024, New York, NY, USA: Institute of Electrical and Electronics Engineers; 2024.
[108] IEEE. IEEE Standard for Blockchain Application Interface. Tech. Rep. IEEE 3217-2023, New York, NY, USA: Institute of Electrical and Electronics Engineers; 2023.
[109] IEEE. IEEE Standard for Blockchain Data Format. Tech. Rep. IEEE 2418.2-2020, New York, NY, USA: Institute of Electrical and Electronics Engineers; 2020.
[110] ISO/TC 307. Blockchain and Distributed Ledger Technologies. Tech. Rep., Geneva, Switzerland: International Organization for Standardization; 2024, Technical Committee 307.
[111] ITU-T. Requirements for IoT data management using blockchain in IoT applications. Tech. Rep. ITU-T Y.4476, Geneva, Switzerland: International Telecommunication Union; 2022.
[112] ITU-T. Framework of next generation network evolution. Tech. Rep. ITU-T Y.2342, Geneva, Switzerland: International Telecommunication Union; 2021.
[113] ITU-T. Framework of secure distributed ledger technology based services. Tech. Rep. ITU-T F.751.2, Geneva, Switzerland: International Telecommunication Union; 2020.
[114] Gharavi H, Granjal J, Monteiro E. PQBFL: A post-quantum blockchain-based protocol for federated learning. Comput Netw 2025;111472.
[115] Singh J, Singh P, Kaur A, Hedabou M. Post-quantum secure fog-edge computing using federated learning with blockchain: J. Singh et al.. J Supercomput 2025;81(13):1249.
[116] Gurung D, Pokhrel SR, Li G. Performance analysis and evaluation of postquantum secure blockchained federated learning. Comput Netw 2024;255:110849.