KDN-FLB: Knowledge-defined Networking through Federated Learning and Blockchain

Ying Li, Praveen Kumar Donta, *Senior Member, IEEE*, Xingwei Wang, Ilir Murturi, *Member, IEEE*, Min Huang, Schahram Dustdar, *Fellow, IEEE*

***Abstract*—In this article, we explore the opportunities and benefits of integrating federated learning (FL) and blockchain technologies to build an adaptable and secure Knowledge-Defined Networking (KDN) system. Our aim is to enhance network performance by ensuring self-learning, self-adapting, and self-adjustment capabilities in dynamic and decentralized network environments. The proposed conceptual architecture, KDN-FLB, also strategically addresses critical challenges in knowledge sharing and privacy preservation within network environments. We discuss the constituents, architecture, processes, and use cases of KDN-FLB in contemporary networking applications. Additionally, we analyze the benefits, challenges, and future prospects associated with KDN-FLB, making it more intelligent for large-scale, dynamic, and decentralized network environments.**

***Index Terms*—Knowledge-defined Networking, Blockchain, Federated Learning, Security and Privacy**

I. Introduction

THE rapid growth of the Internet of Things (IoT) has profoundly expanded the Internet's scale, resulting in increased dynamism and complexity in its applications. For these networks to remain effective, self-learning, self-adaptation, and self-adjustment capabilities are essential, and Knowledge-Defined Networking (KDN) can fulfill these needs [1]. KDN integrates Software-Defined Networking (SDN) with Artificial Intelligence (AI), aiming at efficient network management and control (illustrated in Fig. 1). KDN incorporates a knowledge plane (KP) into traditional SDN architectures to empower networks to autonomously learn from data, adapt to changing conditions in real-time, and optimize performance. On the other hand, Machine Learning (ML) and AI excel at tracking uncertain and dynamically evolving behaviors, rapidly adapting to changing network conditions, and even resolving issues autonomously. Nevertheless, existing research is mostly fragmented across various aspects of networks, generally addressing specific issues in isolation without comprehensive integration, resulting in two major drawbacks: Firstly, ML lacks interpretability, operating without clear understanding; secondly, it does not facilitate the aggregation of knowledge for global cognitive reasoning. Also, the current network infrastructure involves both physical and logical distributed resource allocation, creating an urgent need for distributed machine learning [2], which federated learning (FL) can effectively address [3].

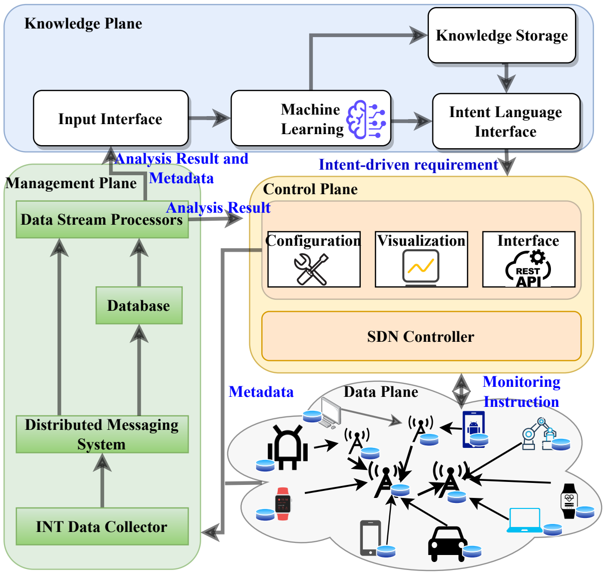


Fig. 1. Knowledge-Defined Networking Architecture.

In tackling the challenges mentioned above in the literature, limited efforts have been made in advancing KDN. Zhang et al. [4] introduced an advanced Deep-Q-Networks (DQN) routing algorithm enhanced with graph recurrent neural networks (GRNN) to support intelligent routing decisions within KDN environments. Their approach involved a comprehensive workflow that included developing a network architecture in Mininet, extracting features using GRNN, and employing DQN for dynamic path selection. It is necessary to verify the computational efficiency and robustness of this work. Rafiq *et al.* [5] presented a self-driving system based on KDN that leverages graph neural networks (GNN) to optimize service function chaining deployment and reactive traffic routing across edge clouds, ensuring efficient resource allocation and performance indicator estimation within an SDN framework. Pham *et al.* [6] explored the application of deep reinforcement learning (DRL) with convolutional neural networks within KDN to significantly enhance QoS-aware routing performance, addressing complex network challenges

Y. Li, X Wang is with the College of Computer Science and Engineering, Northeastern University, Shenyang 110819, China.
Email: liying1771@163.com, wangxw@mail.neu.edu.cn.

Y. Li, P. K. Donta, S. Dustdar, and I. Murturi are with Distributed Systems Group, TU Wien, Vienna 1040, Austria.
Email: {pdonta,dustdar,imurturi}@dsg.tuwien.ac.at.

P.K. Donta also with the Department of Computer and Systems Sciences, Stockholm University, 16425 Kista, Stockholm, Sweden.
Email: praveen@dsv.su.se

Min Huang is with the College of Information Science and Engineering, Northeastern University, Shenyang 110819, China.
Email: mhuang@mail.neu.edu.cn.

Corresponding author: Xingwei Wang.

and improving routing configurations in environments with multiple coexisting flows. He *et al.* [7] introduced MPDRL, a novel approach that combines DRL with a GNN structure. Based on experiments on the topologies of ISP networks, this approach successfully solves routing optimization problems in dynamic network environments. Another notable contribution comes from Lu *et al.* [8], who proposed a blockchain-enhanced FL framework for beyond 5G networks, addressing security, privacy, and resource optimization through DRL. Despite significant advancements in KDN, FL, and Blockchain technologies individually, there is a noticeable lack of comprehensive integration among them in the literature.

As KDN, FL, and blockchain integrate within network systems, they promise security and privacy for knowledge sharing, ownership, and collaboration. Their overarching goal centers on enhancing network systems' performance, imbuing them with self-learning, self-adaptation, and self-adjustment capabilities. In this context, we propose a novel reference framework called Knowledge-defined Networking through Federated Learning and Blockchain (KDN-FLB) to enhance large-scale and dynamic network performance, fortify security measures, and empower the network with self-learning, self-adaptation, and self-adjustment capabilities. The main contributions are summarized as follows:

- We provide a strong motivation of integrating KDN, FL, and blockchain to gain more benefit through KDN-FLB reference architecture.
- We discuss KDN-FLB reference architecture fundamentals, including its architecture, processes, and potential use cases in contemporary networking.
- We employ traffic engineering use cases to evaluate the performance of the proposed KDN-FLB and confirm its superiority.
- We further provide a set of open challenges to implement and extend KDN-FLB for next-generation internet-based applications.

II. Motivation

A primary goal of KDN is to integrate knowledge across multiple network nodes, facilitating comprehensive global cognitive reasoning and thereby improving overall network performance. This initiative aims to enhance the synergy among distributed nodes, fostering a collective cognitive capability that contributes to an efficient and optimized network.

Integrating FL into KDN is imperative due to the unique challenges in distributed knowledge environments. This multifaceted integration addresses privacy preservation, collaboration augmentation, and distributed knowledge utilization. FL serves as a robust solution to inherent privacy concerns, mitigating breach risks and aligning seamlessly with KDN's distributed nature. In addition to fostering collaboration and sharing knowledge, FL promotes collective intelligence while safeguarding the privacy of individual nodes. Moreover, FL resolves challenges posed by centralized approaches, making it easier to assemble and utilize distributed knowledge. This integration enables local learning and model updates, optimizing network performance, enhancing adaptability, and ensuring knowledge remains where it is generated. But, there are also a range of key challenges, including covering security and privacy issues in knowledge sharing, knowledge ownership, and collaboration.

Fortunately, blockchain technology presents immense potential due to its decentralization, immutability, openness, transparency, and traceability characteristics, providing innovative solutions to the above-mentioned issues. Blockchain's decentralized nature mitigates single points of failure, enhancing system stability and participant control over knowledge resources. Its non-tamperability, openness, and transparency establish a robust foundation for knowledge dynamics, ensuring credibility and authenticity. Blockchain's traceability strengthens knowledge credibility and origin scrutiny, fostering trust in knowledge sources within the KDN. It is vital to use these mechanisms to establish trust among KDN contributors and consumers.

III. KDN-FLB: Constituents, Architecture, Processes, and Use-cases

In this section, we discuss the components, architecture, and processes of the proposed KDN-FLB conceptual architecture.

A. Constituents

KDN-FLB is a multifaceted conceptual architecture that combines several entities to enable decentralized, privacy-preserving knowledge sharing. These entities work together to facilitate efficient and secure comprehensive knowledge integration and informed decision-making while protecting individual data. Each of the following constituents plays its individual role in the KDN-FLB architecture:

1) Distributed networks: The KDN-FLB architecture incorporates distributed networks consisting of diverse computing elements such as IoT devices, the Edge, or even a computing continuum. These elements typically perform various computational tasks such as data processing, FL model training, FL model aggregation, validation, and blockchain operations.

2) Participants: The KDN-FLB architecture encompasses several types of participants: individual end-users, organizations, and system administrators. End users utilize FL models and knowledge-sharing capabilities to gain insights, make informed decisions, or generate suggestions. Organizations may contribute data, resources, or expertise to the system and interact with FL models and knowledge-sharing processes. System administrators oversee and maintain the technical infrastructure of the KDN-FLB system, ensuring its overall well-being through system updates, security measures, and troubleshooting.

3) Miners: Miners play a pivotal role in the KDN-FLB architecture by maintaining the blockchain. They validate transactions, create transaction blocks, and secure the network through cryptographic processes such as Proof-of-Work or Proof-of-Stake.

B. Proposed KDN-FLB Conceptual Architecture

The KDN-FLB architecture consists of three components: client-side software, server-side software, and blockchain-side components, as illustrated in Fig. 2.

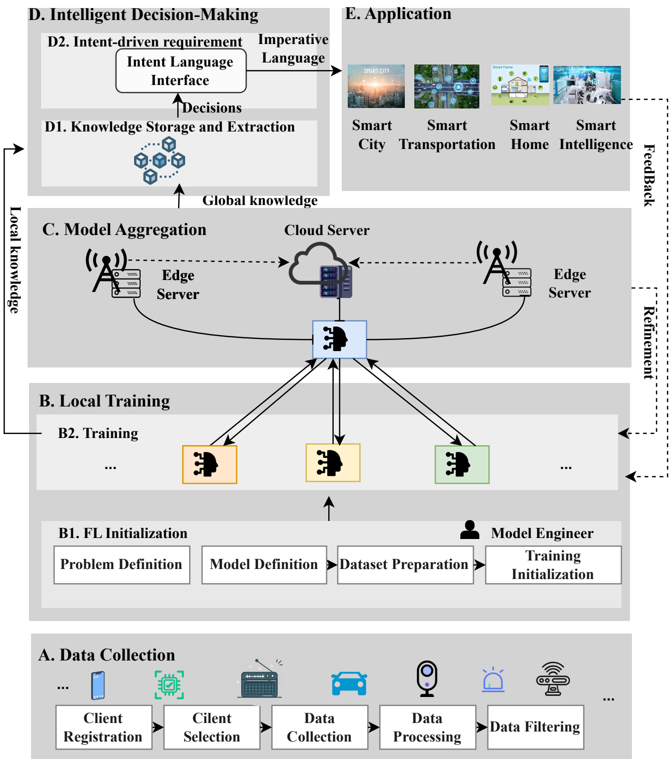


Fig. 2. The proposed KDN-FLB conceptual architecture.

On the client side, the user interface (UI) facilitates user interactions with the KDN-FLB system, providing visualization tools, controls, and feedback mechanisms for managing FL and blockchain processes. FL data collection involves gathering and preparing local data from individual clients, including user interactions, client-specific information, and other relevant data. Local clients contribute by uploading local model updates without raw data and participating in FL, interacting with server-side components.

The server side, typically in distributed networks, is managed by an FL server that coordinates the FL process, communicates with client-side clients, aggregates local model updates, and securely updates the global model. In hierarchical FL, edge servers can serve as intermediate aggregation servers. Communication middleware on the server side ensures secure data transmission through encryption, authentication, and other security measures. Blockchains receive global knowledge aggregated from distributed clients through the middleware.

On the blockchain side (typically managed by miners), employing a consensus mechanism is crucial for maintaining unanimity on the blockchain state across all nodes, preserving the integrity of the distributed ledger. Historical blockchain data supports intelligent decision-making, with the decision-making process transmitted to the intent language interface. This interface translates instructions into an imperative language for users to execute, provides feedback to the client side, and enhances system performance.

C. Processes

This section delineates the working process of the proposed KDN-FLB conceptual architecture, with Fig. 3 depicting the detailed process.

1) Data Collection: The initiation phase involves collecting data from dispersed clients, potentially including edge devices, IoT devices, or contributions from participants.

2) FL Model Training: Guided by the control plane, FL trains local models using distributed data, facilitating model training without sharing raw data.

3) Model Aggregation and Updates: Under the control plane, diverse clients' trained local model updates are aggregated to generate a global model, which is then disseminated back to each client.

4) Data Security and Transparency: Blockchain is used for data security and transparency by recording model training procedures and outcomes, mitigating tampering risks, and providing traceability. However, challenges such as scalability limitations and poor storage extensibility arise due to the blockchain consensus protocol, affecting data safety and reliability. KDN-FLB integrated blockchain involves building a private blockchain and connecting it to a public blockchain to address these issues.

5) Knowledge Extraction: The KP plays a crucial role in deriving meaningful insights from FL models. It involves discerning and extracting valuable knowledge embedded within the aggregated global model. In this phase, KDN-FLB uses FL to extract overall insights from various clients, while integrating blockchain to ensure knowledge authenticity and transparency. Therefore, it fosters decentralized intelligence while maintaining data privacy, which is reinforced through blockchain's secure, immutable ledger, which addresses privacy concerns. Also, KDN-FLB's dynamic adaptation utilizes blockchain's immutable record-keeping to secure historical insights, enabling FL to learn from past experiences and

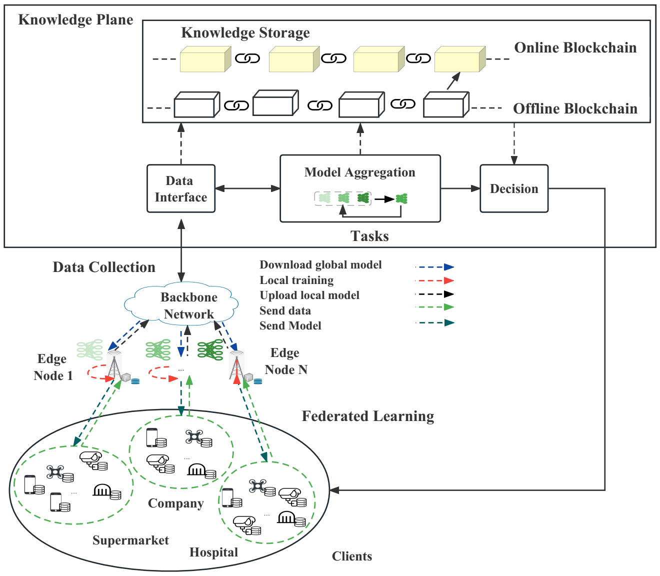


Fig. 3. The working process of KDN-FLB.

optimize over time. Adapting to evolving network conditions through continuous knowledge extraction improves operational efficiency and user experience.

6) Intelligent Decision-making: Intelligent decision-making utilizes extracted knowledge to guide strategic choices within distributed networks. Integrating FL and blockchain ensures that decisions are intelligent, privacy-preserving, and secure. FL's integration with knowledge extraction supports decentralized decision-making, where each client contributes insights from local data, fostering a dynamic distributed decision-making process adaptable to varying conditions. Adaptive decision-making is enabled by continuous knowledge extraction, allowing the network to adaptively respond to dynamic environmental changes. The immutable record of historical decisions on the blockchain allows decision-makers to refine and optimize future decisions based on past outcomes. Furthermore, blockchain technology ensures the integrity of decision-making processes by providing a decentralized, tamper-resistant ledger for decision records. Bringing FL and blockchain together enhances the security and trustworthiness of decision outputs, establishing a reliable framework for strategic network decisions.

D. Use-Cases

In this section, we explore the most appropriate use cases that demonstrate the effectiveness and usefulness of the KDN-FLB conceptual architecture in addressing real-world challenges.

1) Traffic Engineering: Traffic engineering optimizes telecommunications network performance and efficiency through strategic control of data, voice, and video traffic. This discipline is essential for effectively utilizing network resources, minimizing congestion, and meeting service quality objectives. Traditional methods often lack intelligence, making it challenging to classify and control incoming traffic based on existing features. Therefore, AI methods such as GNN or Multi-Agent Reinforcement Learning are considered optimal for early traffic classification, enhancing scheduling and load balancing in dynamic distributed networks to mitigate congestion [9]. In the context of KDN-FLB, historical knowledge trained by FL can be analyzed and stored on the blockchain to learn patterns and relationships between network traffic load and various factors. It facilitates proactive network optimization and enhancements by enabling more accurate traffic load predictions.

2) Network Anomaly Detection: Network anomaly detection is critical for identifying and addressing abnormal behaviors in networks. Traditional methods face challenges due to dynamic network changes and the likelihood of false positives or negatives, leading to misinterpretations and ineffective responses. KDN-FLB will be a robust solution for network anomaly detection since it combines the benefits of FL and blockchain. KDN-FLB enhances anomaly detection accuracy by combining historical data from distributed networks with intelligent learning, ensuring proactive and secure network management

3) Supply Chain Transparency: Supply chain transparency ensures clarity and accessibility of information throughout the entire supply chain, from raw material procurement to product delivery, providing stakeholders, including consumers, with precise details about goods' origins, manufacturing processes, and distribution channels. Contemporary supply chains, characterized by intricacies and fragmentation, raise challenges to reliable product tracking and monitoring. Restricted visibility and data silos hinder accurate inventory tracking. KDN-FLB uses blockchain to establish traceability and provenance through the creation of an immutable ledger of supply chain events. KDN-FLB also facilitates compliance and audit efforts by building trust between supply chain clients. In addition, it can enhance security by decentralizing data storage and automating decision-making processes. In summary, KDN-FLB provides a robust architecture for efficient supply chain transparency, ensuring efficiency, security, and trust.

IV. Experiments

We employ traffic engineering use cases to evaluate the performance of the proposed KDN-FLB. Existing long and short-flow classification research relies heavily on static thresholds, which frequently results in high error rates due to the dynamic nature of network traffic. This paper introduces a dynamic coarse-grained classification method based on KDN-FLB to address the complexities and variations in network conditions. The scheduling module subsequently uses the classification results to optimize traffic management, reduce packet loss, and improve transmission stability.

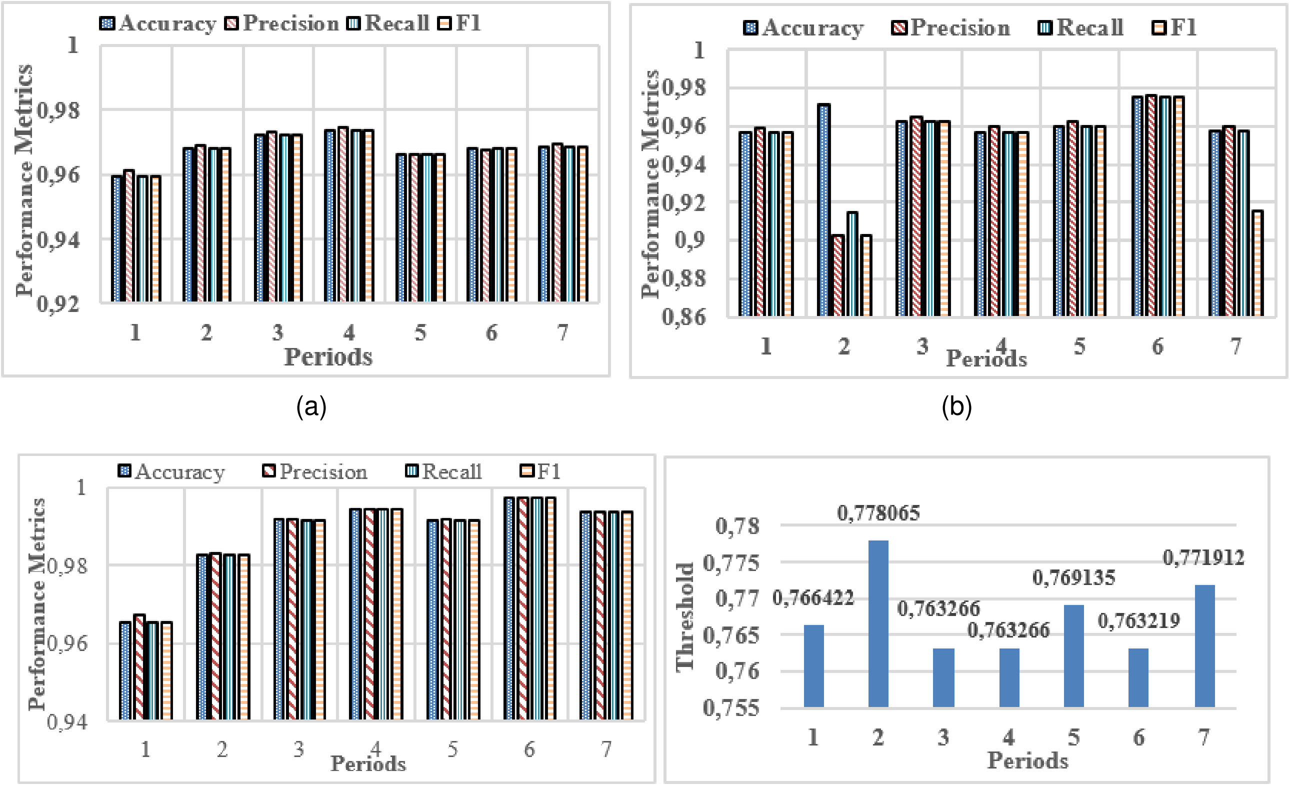
A. Dataset

Flow size is a key criterion for classifying long and short flows. Al-Fares *et al.* [10] defined a long flow as a flow that consumes more than 10% of the total link capacity regardless of its duration, which is one of the most important characteristics of flow scheduling. We perform data analysis on the ISCX2016 dataset, revealing that up to 90% of flows have a size smaller than Ψ MB. Based on flow size, the classification of flow types is outlined in Table I.

TABLE I
Classification of Flow Types by Flow Size.

Flow Size	Category	Classification
$< \Psi$MB	0	Short
$\geq \Psi$MB	1	Long

To expedite coarse-grained long and short flow classification, this study utilizes the FlowMeter tool to extract flow information from the first three packets in the dataset, producing a CSV file with 41,816 records and 64 features each. Due to the long-tail distribution, the dataset exhibits sample imbalance, which was addressed using SMOTE, resulting in a balanced dataset of 75,172 records. The data is divided into seven periods, with each period generating 10,738 records. Here, the random forest was selected as the machine learning algorithm for flow classification.



(a)

(b)

(c)

(d)

Fig. 4. Results for (a) Static Model Classification Scheme. (b) Single Dataset Dynamic Classification Scheme (c) Fusion Dataset Dynamic Classification Scheme (d) Dynamic flow size threshold

B. Comparison of Experimental Schemes

1) Static Model Long and Short Flow Classification: Currently, most schemes for long and short-flow classification rely on static threshold division. In coarse-grained classification using random forest under static threshold conditions, a model is first trained on existing data to distinguish between long and short flows. This model is then applied to classify all subsequent traffic data accordingly. The experimental results are shown in Figure 4(a).

Experimental results indicate that using the static threshold method for coarse-grained long and short-flow classification leads to inconsistent performance. The classification accuracy fluctuates, sometimes achieving high performance and other times low, with no significant overall improvement.

2) Single Dataset Dynamic Long and Short Flow Classification: To adapt to the evolving and complex nature of network traffic, this paper introduces a dynamic long and short-flow classification model update algorithm for a single dataset. Periodically, a new model is trained based on the latest traffic data, which varies over time. Consequently, each trained model differs, tailored to classify traffic specific to its corresponding period. The experimental results are presented in Figure 4(b).

Experimental results show that when only the most recent data is used for training coarse-grained long and short-flow classification at regular intervals, the performance metrics of the classification remain suboptimal, show little improvement, and may even deteriorate.

3) Fusion Dataset Dynamic Long and Short Flow Classification Based on KDN-FLB: To improve the accuracy and stability of dynamic coarse-grained long and short-flow classification, this paper designs a dynamic flow classification model update scheme based on KDN-FLB using a fused dataset. The specific process is as follows:

- Clients request participation in the training process and prepare their local flow data.
- In each period, clients in FL train local models on the client data, generate local models and calculate the respective flow classification thresholds.
- Under the coordination of the control plane, the local models from different clients are aggregated to update the global model and the flow classification thresholds. This ensures the accuracy and adaptability of the model.
- The new global model and flow classification thresholds are combined with the previous global model and thresholds to generate the final global model and flow classification thresholds.
- Blockchain is used to record the final global model and flow classification thresholds to prevent tampering and ensure traceability. Only authorized users can obtain the global model.
- Users utilize the newly obtained global model to classify flow data into long and short flows. The classification results are then provided to the scheduling module to im-

prove traffic scheduling, reduce packet loss, and enhance transmission stability.

The results of Fusion Dataset Dynamic Long and Short Flow Classification Based on KDN-FLB are illustrated in Figure 4(c). The experimental findings show that periodic coarse-grained long and short-flow classification training, which incorporates both previous and current flow data, leads to a steady improvement in classification performance. Ultimately, the performance stabilizes at over 99%, indicating a highly favorable outcome.

4) Dynamic thresholds: As network traffic dynamically changes, the threshold for classifying traffic into long and short flows varies accordingly. This paper illustrates the dynamic threshold changes for traffic classification as shown in Figure 4(d).

V. Challenges and Discussion

KDN-FLB presents a promising approach to enhancing security and empowering the network with self-learning, self-adaptation, and self-adjustment capabilities. Nevertheless, it has its own set of challenges.

Scalability. In KDN-FLB, scalability challenges arise due to FL and blockchain technologies. Specifically, the growing number of clients introduces heightened communication overhead in FL and model aggregation intricacies. This challenge can be mitigated in expanded network settings by using strategies such as hierarchical FL, client selection, and model compression techniques. Scalability issues may arise with blockchain ledger growth and consensus mechanisms. In order to resolve this challenge, various strategies can be adopted, including sharding to facilitate parallel transaction processing, enabling off-chain transactions via state channels and sidechains [11], managing ledger size with data pruning, and integrating cross-chain technologies. Addressing these scalability challenges allows for a more adept design and implementation of KDN-FLB, ensuring high scalability and efficiency in large-scale network environments.

Energy Consumption. In the KDN-FLB architecture, FL poses a risk of increased energy consumption, especially due to training models on resource-constrained devices. Additionally, integrating consensus algorithms into the blockchain raises energy usage concerns. It is essential to integrate optimized FL model training, energy-efficient blockchain consensus mechanisms, adaptive energy management [12], renewable energy sources [13], and energy sharing into the KDN-FLB system to ensure its sustainability and effectiveness.

Network Latency. Communication and coordination between FL and blockchain are optimized and managed by addressing network latency in KDN-FLB. It is crucial to adopt strategies such as using latency-optimized FL algorithms [14], integrating distributed edge intelligence, optimizing blockchain networks through efficient consensus mechanisms, deploying adaptive asynchronous mechanisms [15], and utilizing hybrid blockchain models. These measures reduce network latency's adverse effects on KDN-FLB architecture performance.

Computational Overhead. The KDN-FLB framework encounters considerable computational overhead challenges, primarily due to the demanding computational requirements of FL algorithms and the power-intensive consensus mechanisms essential for blockchain functionality. These challenges can be addressed by optimizing FL algorithms by using methods such as model pruning and knowledge distillation [16], adopting energy-efficient blockchain consensus mechanisms [17], utilizing hardware accelerators to boost computation efficiency, and integrating edge computing to process data closer to the source. The KDN-FLB framework benefits from these targeted interventions by enhancing network intelligence and security under decentralized circumstances.

Interoperability. In the KDN-FLB architecture, addressing interoperability challenges in integrating blockchain platforms and FL becomes imperative. Developing communication and data exchange standards may be crucial to ensuring seamless integration of the two technologies. The KDN-FLB architecture encompasses establishing universal standards [18], designing cross-platform communication APIs, and fostering consortium and collaborative efforts for standardization to ensure interoperability issues.

Deployment of the KDN-FLB in Real-World Environments. The deployment of the KDN-FLB framework in real-world networks presents several challenges, including guaranteeing technical compatibility across various hardware and software ecosystems, overcoming bandwidth and computational resource limitations, and navigating cross-domain collaboration. Addressing these challenges necessitates a multifaceted approach that includes adapting the framework to be modular and flexible [19], harnessing advanced technologies like 5G/6G and edge computing to mitigate resource constraints [20], and establishing robust governance models that facilitate trust and cooperation among stakeholders while ensuring data privacy and integrity. Furthermore, continuous engagement with stakeholders and creating a feedback loop are crucial for the iterative refinement of the framework, ensuring its effectiveness and relevance. With these solutions, the KDN-FLB framework can overcome the above-mentioned barriers, allowing it to significantly transform networked systems.

Considering the intricate interplay between FL and blockchain within the KDN-FLB framework is imperative for mitigating these challenges. KDN-FLB's strategic approach aims to overcome obstacles and maximize its benefits, but further research is needed.

VI. Conclusion

In this article, we explore the potential of combining federated learning and blockchain technologies to create an intelligent Knowledge Delivery Network (KDN) system, specifically known as the KDN-FLB architecture. The proposed KDN-FLB conceptual architecture combines the collaborative nature of FL with blockchain security and transparency features to present a decentralized and next-generation intelligent KDN architecture. The proposed KDN-FLB architecture aims to enhance dynamic and distributed network performance, enhance security measures, and empower the network with self-learning, self-adapting, and self-adjustment capabilities. We will evaluate the proposed architecture in different use cases and demonstrate its superiority to existing platforms in the future.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No.92267206 and No. 62032013. Research has partially received funding from grant agreement Nos. 101079214 (AIoTwin), 101135576 (INTEND), and 101070186 (TEADAL) by EU Horizon.

References

[1] A. Mestres, A. Rodriguez-Natal, J. Carner, P. Barlet-Ros, E. Alarcón, M. Solé, V. Muntés-Mulero, D. Meyer, S. Barkai, M. J. Hibbett *et al.*, "Knowledge-Defined Networking," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 3, pp. 2–10, 2017.

[2] A. Hazra, A. Morichetta, I. Murturi, L. Lovén, C. K. Dehury, V. C. Pujol, P. K. Donta, and S. Dustdar, "Distributed ai in zero-touch provisioning for edge networks: challenges and research directions," *Computer*, vol. 57, no. 3, pp. 69–78, 2024.

[3] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Artificial intelligence and statistics*. PMLR, 2017, pp. 1273–1282.

[4] Y. Zhang, J. Li, Y. Yu, Z. Fan, H. Ma, and X. Wang, "SDN Multi-Domain Routing for Knowledge-Defined Networking," in *2023 15th International Conference on Communication Software and Networks (ICCSN)*. IEEE, 2023, pp. 24–29.

[5] A. Rafiq, S. Rehman, R. Young, W.-C. Song, M. A. Khan, S. Kadry, and G. Srivastava, "Knowledge defined networks on the edge for service function chaining and reactive traffic steering," *Cluster Computing*, vol. 26, no. 1, pp. 613–634, 2023.

[6] T. A. Q. Pham, Y. Hadjadj-Aoul, and A. Outtagarts, "Deep Reinforcement Learning Based QoS-Aware Routing in Knowledge-Defined Networking," in *Quality, Reliability, Security and Robustness in Heterogeneous Systems: 14th EAI International Conference, Qshine 2018, Ho Chi Minh City, Vietnam, December 3–4, 2018, Proceedings 14*. Springer, 2019, pp. 14–26.

[7] Q. He, Y. Wang, X. Wang, W. Xu, F. Li, K. Yang, and L. Ma, "Routing Optimization With Deep Reinforcement Learning in Knowledge Defined Networking," *IEEE Transactions on Mobile Computing*, 2023.

[8] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for 5G Beyond," *Ieee Network*, vol. 35, no. 1, pp. 219–225, 2020.

[9] G. Bernárdez, J. Suárez-Varela, A. López, X. Shi, S. Xiao, X. Cheng, P. Barlet-Ros, and A. Cabellos-Aparicio, "Magnneto: A graph neural network-based multi-agent system for traffic engineering," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 2, pp. 494–506, 2023.

[10] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, A. Vahdat *et al.*, "Hedera: dynamic flow scheduling for data center networks." in *Nsdi*, vol. 10, no. 8. San Jose, USA, 2010, pp. 89–92.

[11] Y. Li, Y. Yu, and X. Wang, "Three-tier Storage Framework Based on TBchain and IPFS for Protecting IoT Security and Privacy," *ACM Transactions on Internet Technology*, vol. 23, no. 3, pp. 1–28, 2023.

[12] Y. Li, X. Wang, R. Zeng, P. K. Donta, I. Murturi, M. Huang, and S. Dustdar, "Federated domain generalization: A survey," *arXiv preprint arXiv:2306.01334*, 2023.

[13] Y. Xu, Z. Liu, C. Zhang, J. Ren, Y. Zhang, and X. Shen, "Blockchain-Based Trustworthy Energy Dispatching Approach for High Renewable Energy Penetrated Power Systems," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10 036–10 047, 2021.

[14] L. Toka, M. Konrád, I. Pelle, B. Sonkoly, M. Szabó, B. Sharma, S. Kumar, M. Annavazzala, S. T. Deekshitula, and A. A. Franklin, "5G on the Roads: Latency-Optimized Federated Analytics in the Vehicular Edge," *IEEE Access*, 2023.

[15] Y. Qu, L. Gao, Y. Xiang, S. Shen, and S. Yu, "FedTwin: Blockchain-Enabled Adaptive Asynchronous Federated Learning for Digital Twin Networks," *IEEE Network*, vol. 36, no. 6, pp. 183–190, 2022.

[16] Y. Jiang, S. Wang, V. Valls, B. J. Ko, W.-H. Lee, K. K. Leung, and L. Tassiulas, "Model Pruning Enables Efficient Federated Learning on Edge Devices," *IEEE Transactions on Neural Networks and Learning Systems*, 2022.

[17] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-pow:an energy-efficient blockchain proof-of-work consensus algorithm," *Computer Networks*, vol. 214, p. 109118, 2022.

[18] S. Schindler and S. Marvin, "Constructing a universal logic of urban control? International standards for city data, management, and interoperability," *City*, vol. 22, no. 2, pp. 298–307, 2018.

[19] S. Otoum, I. Al Ridhawi, and H. Mouftah, "A Federated Learning and Blockchain-Enabled Sustainable Energy Trade at the Edge: A Framework for Industry 4.0," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3018–3026, 2022.

[20] G. Qu, N. Cui, H. Wu, R. Li, and Y. Ding, "ChainFL: A Simulation Platform for Joint Federated Learning and Blockchain in Edge/Cloud Computing Environments," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3572–3581, 2021.

Ying Li (S'20) received a B.S. degree in the Internet of Things from Anyang Institute Of Technology, Anyang, China, in 2017, and an M.S. degree in computer technology from Northeastern University, Shenyang, China, in 2020, where she is currently pursuing the Ph.D. degree in computer science and technology. She is a visiting PhD at Distributed Systems Group, TU Wien, Austria from 2022 to 2024.

Her research interests include federated learning, blockchain, and edge intelligence. Contact her at liying1771@163.com

Praveen Kumar Donta (SM'22) currently a Senior Lecturer at Stockholm University, Sweden. He was a Postdoctoral researcher in the Distributed Systems Group, TU Wien, Austria until June 2024. He received his Ph.D. from the Department of Computer Science and Engineering at the Indian Institute of Technology (Indian School of Mines), Dhanbad, India. He was a visiting Ph.D. student at the University of Tartu, Estonia. He received his Master and Bachelor of Technology from JNTU Anantapur, India, in 2014 and 2012, respectively. His current research is on Learning-driven distributed computing continuum systems, Cyber-physical continuum, and Intelligent data protocols. Contact him at praveen@dsv.su.se

Xingwei Wang received the B.S., M.S., and Ph.D. degrees in computer science from Northeastern University, Shenyang, China, in 1989, 1992, and 1998, respectively. He is currently a Professor with the College of Computer Science and Engineering, Northeastern University. He has published more than 100 journal articles, books and book chapters, and refereed conference papers.

His research interests include cloud computing and future Internet. Prof. Wang has received several best paper awards. Contact him at wangxw@mail.neu.edu.cn

Ilir Murturi (M'20) is a Postdoctoral Researcher in the Distributed Systems Group, TU Wien, Austria. He received a Ph.D. in the Distributed Systems Group, Technische Universität Wien (TU Wien), Vienna, Austria, and an MSc in Computer Engineering from the University of Prishtina, Prishtina, Kosova. His current research interests include the Internet of Things, Distributed Computing Continuum Systems, EdgeAI, and privacy in distributed, self-adaptive, and cyber-physical systems. Contact him at imurturi@dsg.tuwien.ac.at

Min Huang (Member, IEEE) received the B.S. degree in automatic instrument, the M.S. degree in systems engineering, and the Ph.D. degree in control theory from Northeastern University, Shenyang, China, in 1990, 1993, and 1999, respectively. She is currently a Professor with the College of Information Science and Engineering, Northeastern University. She has published more than 100 journal articles, books, and refereed conference papers. Her research interests include modeling and optimization for logistics and supply chain system. Contact her at mhuang@mail.neu.edu.cn

Schahram Dustdar (Fellow, IEEE) is a full professor of computer science (informatics) with a focus on Internet Technologies heading the Distributed Systems Group at the TU Wien. He is a member of the Academia Europaea. He is the recipient of the ACM Distinguished Scientist Award and Distinguished Speaker award, and the IBM Faculty Award. He is an associate editor of IEEE Transactions on Services Computing, ACM Transactions on the Web, and ACM Transactions on Internet Technology, and on the editorial board of IEEE Internet Computing and IEEE Computer. He is the editor-in-chief of Computing (an SCI-ranked journal of Springer). Contact him at dustdar@dsg.tuwien.ac.at