Quantum Federated Learning for Vehicular Computing Scenarios

Joongheon Kim
School of Electrical Engineering, Korea University, Seoul, Republic of Korea
E-mail: joongheon@korea.ac.kr

***Abstract*—With the rise of autonomous vehicles (AVs), the number of self-driving vehicles has increased in recent years and vehicular computing (VC) was actively used to ensure road safety by controlling AVs. However, the recent escalation in demand for a massive scale vehicle network has prevented VC from achieving its purpose. To overcome this problem, a framework which combined VC and federated learning (FL) was proposed. Although the vehicular FL was initially effective, it also faced challenges as the excessive increase in the amount and size of data generated by AVs and the serious threat of data leakage have severely degraded the performance of vehicular FL. Thus, quantum computing was exploited to further improve on the pre-existing FL and proposed dynamic quantum federated learning (DQFL). This work proposes the application of DQFL to public safety scenarios to investigate the effectiveness of the model in controlling the AVs under real-life constraints.**

I. INTRODUCTION

The technology of autonomous vehicles (AV) has become one of the most impactful technologies that currently exist. According to a market report by *Allied Market Research*, the value of AV market is expected to achieve $2161 billion by 2030 [1]. As the growing market suggests, the influence of AVs on people will only continue to grow in the future. This is mainly because of two reasons. Firstly, the sheer number of cars that are used in modern society is responsible for the scale of impact caused by AVs. Currently, there are over 800 million cars on the road globally and the number is consistently growing over time. Assuming all the vehicles become autonomous, many aspects of daily lives of people will be changed by the self-moving car.

Additionally, the rise of artificial intelligence technology has resulted in the rediscovery of a field known as *vehicular computing* (VC) [2]. This technology aims to control vehicles using computing techniques [3]. VC can be used to enhance safety on road environments and implement stable traffic control. However, as mentioned above, countless vehicles exist in urban environments around the world which is why coordination and cooperation between massive scale of vehicles is an essential pre-requisite to the proper implementation of VC [4]. Yet, simultaneous coordination of numerous vehicles is not a simple task and requires significant amount of complex computations which generally cannot be handled by a single entity. Therefore, the machine learning technique known as federated learning (FL) must be used because it alleviates the computational load by distributing the task among several devices [5]. Consequently, FL is an effective method in realistically implementing vehicular computing to control multiple vehicles on a road environment.

Despite these strengths, vehicular FL networks face a diverse set of challenges when applied to the field of AVs [5]. As AVs continue to move in real time, wireless communication must be used to transmit neural network (NN) parameters during FL. Furthermore, road environments tend to be extremely hectic due to the sheer number of vehicles which will inevitably lead to unstable wireless communication channels because of the significant amount of interference caused by other vehicles on the road. As a result, a considerable amount of model parameters will be lost during the transmission process and the performance of the vehicular FL model will deteriorate because insufficient data is available for optimization. Moreover, the size of data being generated by edge devices has been constantly increasing recently as high resolution cameras become more advanced and widely used [6]. Hence, it has become increasingly cumbersome for classical computers to process such dense data, leading to computational delays in vehicular computing networks. Due to the nature of the tasks, these delays must be avoided as it may result in critical losses. Additionally, the data transmitted among the AVs contain highly sensitive data(i.e., personal information, vehicle identification number) and leakage of such data must also be prevented. Since wireless communication is frequently used for data transmission, data security risks are increasing and methods to reinforce data security are desperately needed [7].

Therefore, the advantages of quantum computing (QC) are exploited in order to face the challenges of vehicular FL networks. In comparison to classical computing, QC is a next-generation computing technique which utilizes a different type of information unit. Via QC, quantum neural networks (QNN) can be implemented [8]–[10]. Additionally, the strengths of QC stemming from this distinction can be organized into three parts. Firstly, QC has high parameter efficiency which allows a QNN to perform better than a classical NN despite utilizing a smaller number of model dimension [11]–[13]. Furthermore, smaller model dimension also means that a QNN requires lesser resources to implement as well. Secondly, QC can also process more data in the same time than a classical NN. If more data is processed, the effectiveness of the vehicular FL network will improve, minimizing computational delays. Finally, as QC has many different characteristics compared to classical computing, it has some unique characteristics which can be utilized to strengthen data security during wireless transmission of sensitive data. Note that this effect is the result of the inherent traits of QC which means that no additional resources are needed. It can be seen that the three strengths of QC serve as a perfect fit solution to the three challenges faced by vehicular FL network which is why quantum federated learning (QFL) must be used [14]–[22].

As mentioned above, VC is commonly used to ensure road safety. Therefore, this article proposes the application of dynamic quantum federated learning (DQFL) to a scenario of using AVs to ensure public safety on a road environment. Currently, securing road safety is a task which requires heavy amounts of resources (i.e., manpower, time) across the world. Therefore, being able to execute this task only with driverless AVs will greatly increase the resource efficiency in general. By performing several thorough simulations, this work will corroborate the necessity of FL in implementing vehicular computing and quantum supremacy.

The remaining contents of this article which is organized as shown below. Sec. II will explain the concept of vehicular computing and its limitations in detail. Sec. III explains the various FL architectures of the proposed DQFL model used in the work. Sec. IV then lays out the task carried out by the AVs and the overall mechanism of DQFL. Finally, Sec. V concludes this article by summarizing its contents.

II. Vehicular Computing

A. Concept

VC is a research field which actively utilizes computing technologies and systems such as the global positioning system, cameras and communication systems. vehicles. By using these technologies, VC aims to provide advanced levels of assistance to drivers and even achieve autonomous control of unmanned vehicles to perform various complex tasks [3]. VC is constantly gaining importance in recent years because it has the potential to significantly improve the safety, efficiency and convenience of vehicles. Combined with the fact that the number and influence of vehicular technology are expected to increase in the near future, it is profoundly clear that VC is a key technology in establishing future urban environments.

In urban cities, the condition of road environments are often decided by the vehicles which actually occupy the road. Therefore, controlling a single vehicle is insufficient in impacting the safety of road environments. Instead, controlling vehicles on a massive scale is needed in order to ensure that VC can actually influence road environments. If a large number of cars can be controlled by a system, information can be shared among the vehicles which results in a *connected vehicle network*. Using this network, the state of any road environments can be quickly and accurately analyzed by the information provided by each individual vehicle on the road. Then, this information can be distributed to the drivers and autonomous vehicles such that safer autonomous driving, advanced driver assistance and easier traffic control can be achieved. As these are all key factors in ensuring road safety, VC is an important technology that brings about significant benefits. However, the need for a massive scale connected network leads to some critical limitations of VC discussed in the next section.

B. Limitations

In a massively connected vehicle network, numerous transmission of large amounts of data must be done constantly and they must be reliable to prevent any delays which are extremely difficult to achieve simultaneously. Due to this difficulty, VC faces a total of three main challenges. Firstly, VC requires a constant exchange of data among vehicles because information about road environments provided to AVs must be updated in real time as road environments change extremely rapidly. Thus, a delay in the update of information to AVs may result in catastrophic accidents that must be avoided. However, achieving stable channel condition is impossible as wireless transmission is used. Instead, the parameter transmitted by the AVs must be reduced in size to increase the probability of successful transmission [3]. Secondly, executing all of the data transmissions in a centralized manner is extremely costly in terms of computational resources. This is especially true in recent years as the sizes of data are being enlarged due to the quality of data (i.e., image, video, audio) becoming increasingly sophisticated. As a result, the computational load placed on a single centralized device is extremely high and the process is also exceptionally inefficient. Thus, a decentralized method of distributing the total computational load among several devices must be implemented. Finally, the data collected by the AVs will usually contain sensitive information that will cause irrevocable damage if leaked. In addition, the parameters are transmitted using wireless communication and data that are transmitted over wireless channels are especially vulnerable to cyberattacks [7]. Hence, a way to reinforce data security during the transmission within the connected vehicle network must be implemented as well. Now that the limitations of VC have been elaborated, the architecture and the reason why FL is a perfect solution to the problems will be explained in the next section.

III. Federated Learning Architectures

A. Classical Federated Learning

The machine learning framework for the AVs will be discussed in this section. FL is a fast emerging field of research in response to the proliferation of mobile edge devices and the ensuing production of massive scale data. In terms of structure, this framework is composed of a centralized server and several edge devices each equipped with NNs. Initially, the NN model within each device will be trained separately regardless of the NNs in other devices. Afterwards, the parameters of the trained NNs will be transmitted to the central server for aggregation. The aggregated parameter values will be used to compute the global model parameter which will be distributed back to the local devices. There are multiple methods to achieve this such as *FedAvg* [23], *FedBN* [24] and *FedProx* [25]. The performance of the FL model will differ according to the methods used during aggregation. Essentially, the purpose of this model is to optimize the global model over several

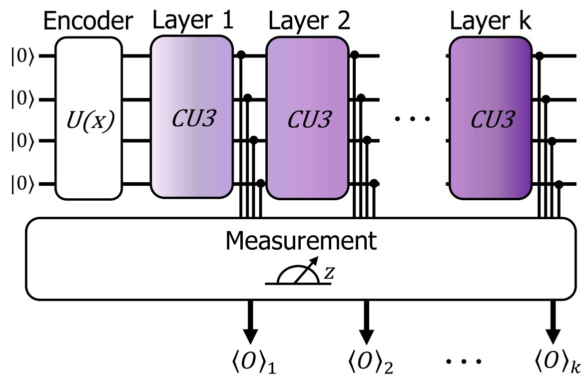

Fig. 1: Structure of adaptive quantum neural network.

iterations of local model training and update of global model via local parameters aggregation.

This specific method of machine learning is especially suitable in solving the problems of VC because the computation required for the deduction of an optimal model is distributed among numerous edge devices. Furthermore, only the transmission of local model parameters of each AV is required to achieve FL. Since no data need to be transmitted, the risk of data leakage is significantly reduced. Considering how the computing power of edge devices and the amount of produced data are increasing, FL is a efficient way of minimizing computational delays, alleviating the computational load on the model and ensuring privacy in the process. Thus, it can be confidently stated that FL is the right solution to the limitations of VC.

Yet, FL is still faced with several critical challenges despite its strengths [26], [27]. For instance, as wireless transmission is commonly used in FL, the loss rate that occurs from transmitting the parameters of a large NN model across a wireless channel is critical to the point that performance of FL will be severely degraded. Secondly, the amount of computing power required to train all the devices in FL are becoming excessively large for classical computers to handle because the amount and the size of data being processed is becoming larger. This is mainly due to the increase in average number of edge devices and the significant advancement of sensor technologies. Lastly, the large number of transmission increases the risk of data leakage during FL which calls for stronger data security measures such that leakage of sensitive and private data can be prevented [27]. Thus, QC is introduced to the situation to mitigate the aforementioned problems.

B. Quantum Federated Learning

Based on the structure provided by the classical FL, quantum federated learning (QFL) can be implemented. As the name implies, QFL is a quantum implementation of the classical FL where all the classical NNs are replaced with QNNs while maintaining the overall structure of the framework. This architecture was proposed to exploit the strengths of QC in order to overcome the limitations of FL. To briefly introduce QC, it is a newly emerging technology that has the potential to overtake classical computers in the realm of theoretical computer science. Development of quantum computers has been ongoing for a long time but a crucial milestone was achieved by *Google* in 2019, where *quantum supremacy* was announced to the world [28], [29]. This work declared quantum supremacy was real by proving that quantum computers could solve complex mathematical problems that were considered unsolvable by classical supercomputers [30]. Additionally, QC can be used to implement quantum machine learning (QML) by utilizing QNNs and the three limitations of FL can be mitigated by quantum supremacy [13], [31] Firstly, the parameter efficiency of qubits allows QNNs to utilize a smaller number of parameters compared to a classical NNs when accomplishing an identical task. Thus, the amount of parameter data transmitted by the AVs are greatly reduced, which is significantly beneficial in consideration of unstable wireless channel conditions as this leads to an easier transmission of the QNN over wireless channel. Secondly, the increased computational power of QC allows the FL model to handle more data produced by the devices. Hence, QFL architectures will be able to show similar levels of performance to classical FL framework despite the increased amount of edge devices. Finally, the unique characteristics of a QNN such as the *quantum state encoding* and *measurement* processes reinforce data security during transmission. During quantum state encoding, the original input data are used as parameters for the quantum rotation gates and the dimensions of the input data are hidden during this process. As a result, a hacker will not be able to identify the type of data used which can increase the level of security. Furthermore, the measurement process to the correct axis fitted to the quantum data is required before properly utilizing it and an incorrect measurement will render the data useless. Hence, even if an unauthorized party obtains the quantum data, it cannot be used if the correct measurement axis is unknown which can greatly increase data security of the model.

C. Dynamic Quantum Federated Learning

In order to improve the robustness of QFL against dynamic channel conditions, a novel framework known as dynamic quantum federated learning (DQFL) was proposed [32]. A different type of QNN known as the *dynamic quantum neural network* (DQNN) is utilized in this framework as shown in Fig. 1. Unlike QNN, *Controlled-Universal* (CU3) gates are used instead of basic rotation gates. Furthermore, the parameterized circuit is divided into discrete layers such that the output quantum state of each layer can be measured. While it is the general rule of thumb that larger NN model size will result in better performance, this may not apply for QNNs because the increase in quantum noise is inevitable as more computations are executed. Hence, limiting the number of computations may be beneficial for the performance of the quantum circuit rather than maximizing the amount of computations which is the main motivation behind the mechanism of

DQNN. Suppose that the state of a wireless channel is inferior and rate of accurate transmission is low. Then, the output quantum data of the first or second layer must be used in order to minimize the rate of error of the utilized data. As a result, when faced with a constantly changing wireless channel, DQNN can flexibly choose the desired quantum data that can maximize performance which is impossible for a fixed-sized QNN. Due to this increased adaptability of DQNN in dynamic channel conditions, DQFL will have better performance than QFL.

IV. Public Safety Scenario via AVs

A. Scenario Overview

In this section, the real-life public safety scenario involving AVs for the application of DQFL architecture will be introduced and elaborated. AVs equipped with cameras are deployed on road environments (i.e., highways, urban areas), where numerous cars are located. Furthermore, a centralized server is assumed to be positioned within the wireless transmission range of the AVs. Note that all the scenario elements are equipped with quantum processors such that QNNs can be utilized. Initially, all the AVs are assumed to be moving on a pre-planned trajectory. Then, a report containing information such as the type and location of task will be sent from related authorities (i.e., police, traffic management centre) to the AVs. Once the information is received, the AVs will mobilize to the reported location for task execution. Some examples of the possible tasks include locating specific vehicles, issuing parking tickets, traffic management and reporting road accidents. All of these tasks require the AVs to recognize license number plates via image classification and will ensure road safety. Thus, the performance of DQFL in this AV scenario will be done by investigating top-1 accuracy values of image classification.

B. Mechanism Pipeline

The mechanism of the DQFL framework is composed of four stages which are sensing, local training, uplink of parameters with superposition coding and parameters aggregation with successive decoding and local update. The entire pipeline will be elaborated carefully to understand how this framework operates.

1) Sensing: In this stage, a single AV will receive task information and move to the reported location for task execution. During this process, the AV must capture images of license plates of vehicles moving on the road such that the vehicles can be recognized. After recognition, the image data of license plates will be stored for the next stage instead of being discarded.

2) Local Training: : Using the stored image data, the AV will begin training its local QNN. During this process, all AVs will be trained differently from each other as the natures of the data collected and the tasks executed will be different.

3) Uplink of Parameters using Superposition Coding: After an iteration of training is finished, each AV will encode the raw data in to signals using superposition coding such that it can be transmitted to the centralized server. Due to the mobile characteristic of AVs, the communication channel state of some AVs may be inferior. However, by using the DQNN model, this limitation can be mitigated to a certain extent.

4) Parameters aggregation with Successive Decoding: At the server side, the SC-encoded signals are received which undergo successive decoding. Afterwards, the data sent by the AVs can now be aggregated. As mentioned above, several different techniques of data aggregation exist such as FedAvg and FedBN. The most efficient technique that is compatible with the given data and situation should be used to maximize performance.

5) Local Update: Finally, the aggregated parameters are used to build a global model which is distributed back to all the AVs simultaneously. For this process, transmission is assumed to succeed at all times because the server side is assumed to have surplus power that ensures successful transmission. Then, the AVs replace their original local QNN model with the new, global model to execute the given tasks which starts another iteration of optimization.

V. Conclusions

In conclusion, this work is the first in proposing a novel application of DQFL to the AV scenario as far as the authors know. Therefore, there are still room for improvement that can be realized in future works. For instance, other different applications such as satellites and unmanned aerial vehicles can be realized. Furthermore, the DQFL model architecture itself can be improved by exploring more suitable methods in optimizing QNNs. Until now, QC technology has received significant skepticism about its potential because of critical limitations like NISQ. However, remarkable advancements are being made which bring QC closer to its full potential and this work is one of the numerous efforts in realizing that potential. At its peak performance, QC is expected to revolutionize the field of VC and many other research fields as well.

Acknowledgement

This research was funded by the National Research Foundation of Korea (NRF-Korea) (2022R1A2C2004869). The author thanks to Mr. Jae Pyoung Kim for his contribution on research initiation, during his graduate study under the guidance of Prof. Joongheon Kim.

References

[1] A. S. S and S. M, “Autonomous vehicle market size, share, value, report, growth,” Feb 2022. [Online]. Available: https://www.alliedmarketresearch.com/autonomous-vehicle-market

[2] F. Tang, B. Mao, N. Kato, and G. Gui, “Comprehensive survey on machine learning in vehicular network: Technology, applications and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 2027–2057, 2021.

[3] R. Meneguette, R. De Grande, J. Ueyama, G. P. R. Filho, and E. Madeira, “Vehicular edge computing: architecture, resource management, security, and challenges,” *ACM Computing Surveys (CSUR)*, vol. 55, no. 1, pp. 1–46, 2021.

[4] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Network*, vol. 27, no. 5, pp. 48–55, 2013.

[5] J. Posner, L. Tseng, M. Aloqaily, and Y. Jararweh, "Federated learning in vehicular networks: Opportunities and solutions," *IEEE Network*, vol. 35, no. 2, pp. 152–159, 2021.

[6] D. Gehrig and D. Scaramuzza, "Are high-resolution event cameras really needed?" *CoRR*, vol. abs/2203.14672, 2022.

[7] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2725–2764, 2020.

[8] H. Baek, W. J. Yun, S. Park, and J. Kim, "Stereoscopic scalable quantum convolutional neural networks," *Neural Networks*, vol. 165, pp. 860–867, August 2023.

[9] H. Baek, W. J. Yun, and J. Kim, "FV-Train: Quantum convolutional neural network training with a finite number of qubits by extracting diverse features," in *Proc. AAAI Conference on Artificial Intelligence (AAAI) Symposium on Educational Advances in Artificial Intelligence (EAAI)*, Washington, DC, USA, February 2023, pp. 16 156–16 157.

[10] W. J. Yun, J. Park, and J. Kim, "Quantum multi-agent meta reinforcement learning," in *Proc. AAAI Conference on Artificial Intelligence (AAAI)*, Washington, DC, USA, February 2023, pp. 11 087–11 095.

[11] C. Park, W. J. Yun, J. P. Kim, T. K. Rodrigues, S. Park, S. Jung, and J. Kim, "Quantum multi-agent actor-critic networks for cooperative mobile access in multi-uav systems," *IEEE Internet of Things Journal*, pp. 1–1, 2023 (Early Access).

[12] W. J. Yun, J. P. Kim, S. Jung, J.-H. Kim, and J. Kim, "Quantum multiagent actor–critic neural networks for internet-connected multirobot coordination in smart factory management," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9942–9952, June 2023.

[13] W. Yun, Y. Kwak, J. Kim, H. Cho, S. Jung, J. Park, and J. Kim, "Quantum multi-agent reinforcement learning via variational quantum circuit design," in *Proc. IEEE International Conference on Distributed Computing Systems (ICDCS)*, Bologna, Italy, July 2022, pp. 1332–1335.

[14] Y. Kwak, W. J. Yun, J. P. Kim, H. Cho, J. Park, M. Choi, S. Jung, and J. Kim, "Quantum distributed deep learning architectures: Models, discussions, and applications," *ICT Express*, vol. 9, no. 3, pp. 486–491, June 2023.

[15] J. Choi and J. Kim, "A tutorial on quantum approximate optimization algorithm (QAOA): Fundamentals and applications," in *Proc. IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea, October 2019, pp. 138–142.

[16] J. Choi, S. Oh, and J. Kim, "The useful quantum computing techniques for artificial intelligence engineers," in *Proc. IEEE International Conference on Information Networking (ICOIN)*, Barcelona, Spain, January 2020, pp. 1–3.

[17] ——, "A tutorial on quantum graph recurrent neural network (QGRNN)," in *Proc. IEEE International Conference on Information Networking (ICOIN)*, Jeju, Korea, January 2021, pp. 46–49.

[18] S. Oh, J. Choi, J.-K. Kim, and J. Kim, "Quantum convolutional neural network for resource-efficient image classification: A quantum random access memory (QRAM) approach," in *Proc. IEEE International Conference on Information Networking (ICOIN)*, Jeju, Korea, January 2021, pp. 50–52.

[19] J. Pyoung Kim, W. Joon Yun, H. Baek, and J. Kim, "Modern trends in quantum AI: Distributed and high-definition computation," in *Proc. IEEE International Conference on Information Networking (ICOIN)*, Bangkok, Thailand, January 2023, pp. 750–754.

[20] Y. Kwak, W. J. Yun, S. Jung, J.-K. Kim, and J. Kim, "Introduction to quantum reinforcement learning: Theory and PennyLane-based implementation," in *Proc. IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea, October 2021, pp. 416–420.

[21] J. Kim, Y. Kwak, S. Jung, and J.-H. Kim, "Quantum scheduling for millimeter-wave observation satellite constellation," in *Proc. IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, Osaka, Japan, August 2021, pp. 1–5.

[22] Y. Kwak, W. J. Yun, S. Jung, and J. Kim, "Quantum neural networks: Concepts, applications, and challenges," in *Proc. IEEE International Conference on Ubiquitous and Future Networks (ICUFN)*, Jeju, Korea, August 2021, pp. 413–416.

[23] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, "On the convergence of fedavg on non-iid data," *CoRR*, vol. abs/1907.02189, 2019.

[24] X. Li, M. Jiang, X. Zhang, M. Kamp, and Q. Dou, "Fedbn: Federated learning on non-iid features via local batch normalization," *CoRR*, vol. abs/2102.07623, 2021.

[25] X.-T. Yuan and P. Li, "On convergence of fedprox: Local dissimilarity invariant bounds, non-smoothness and beyond," *CoRR*, vol. abs/2206.05187, 2022.

[26] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.

[27] C. Ma, J. Li, M. Ding, H. H. Yang, F. Shu, T. Q. S. Quek, and H. V. Poor, "On safeguarding privacy and security in the framework of federated learning," *IEEE Network*, vol. 34, no. 4, pp. 242–248, 2020.

[28] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, October 2019.

[29] S. Y.-C. Chen, C.-H. H. Yang, J. Qi, P.-Y. Chen, X. Ma, and H.-S. Goan, "Variational quantum circuits for deep reinforcement learning," *IEEE Access*, vol. 8, pp. 141 007–141 024, August 2020.

[30] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, p. R2493, 1995.

[31] O. Lockwood and M. Si, "Reinforcement learning with quantum variational circuit," in *Proc. of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment*, vol. 16, no. 1, Virtual, October 2020, pp. 245–251.

[32] W. J. Yun, J. P. Kim, S. Jung, J. Park, M. Bennis, and J. Kim, "Slimmable quantum federated learning," in *Proc. ICML Workshop on Dynamic Neural Networks*, Baltimore, MD, USA, July 2022.