Cureus Journal of Computer Science

Open Access Review Article

Security of Quantum Federated Machine Learning With Blockchain for Electronics Health Records

Fabrice Nazaire Kameni Tcheumaga [1] , Kevin Umba [1] , Padmapriya Velupillaimeikandan [1] , Md Munirul Haque [2] , Sheikh Iqbal Ahamed [1]

1. Ubicom Lab, Marquette University, Milwaukee, USA 2. Computer Science, Butler University, Indianapolis, USA

Corresponding author: Fabrice Nazaire Kameni Tcheumaga, fabrice.kameni@marquette.edu

Received 04/22/2025
Review began 05/02/2025
Review ended 09/03/2025
Published 09/08/2025

DOI:
https://doi.org/10.7759/s44389-025-03870-4

Abstract

The continuous growth of healthcare data requires robust architectures and solutions. Thanks to Quantum Federated Machine Learning (QFML), which combines quantum computing power, federated learning, and blockchain technology, that enhances decentralization and privacy-preserving benefits. However, the combination of these technologies brings a new level of complexity. This paper presents a systematic literature review on the security of QFML in blockchain for healthcare. Our review shows the limitations and the lack of adequate and robust solutions to address the current vulnerabilities. The review then paves the road for advancing the security of the QFML system on blockchain for healthcare applications.

Categories: Quantum Computing, Blockchain and Cryptocurrency, Machine Learning (ML)
Keywords: data security and privacy, quantum federated learning, machine learning, security, electronic health records

Introduction And Background

The continuously growing population worldwide imposes an increasing quantity of data to process and store in local devices and the cloud. Healthcare is one of the most critical sectors that produces large amounts of sensitive data. Quantum Federated Machine Learning (QFML) has emerged as a promising technology that can foster the development of models using the computational advantage of quantum computers. The federated learning system has produced good results in terms of efficiency, privacy, and security [1,2]. However, integrating the quantum system and the blockchain adds more complexity, requiring more investigation. Our work aims to reveal the potential threat to QFML for healthcare. In addition, we also shed light on the future of harnessing the security and data privacy of sensitive information in the complex architecture of QFML and blockchain. The main contributions of this paper are as follows: to our knowledge, this is the first survey that investigates the security of QFML in the blockchain system. A holistic study on how the security of QFML on blockchain systems presents a taxonomy of current vulnerabilities. We discuss current problems, open issues, and future directions.

Three research questions guide our reflection: what is the current state of quantum federated learning for electronic healthcare applications? What are the specific quantum-based adversarial attacks that could potentially exploit QFML systems? What are the key challenges in ensuring security and data privacy for QFML systems integrated with blockchain, and what potential solutions can mitigate these risks?

Introduction to quantum computing

Quantum computing is the newest technology in computer science that leverages the potentialities of quantum mechanics to perform computing operations with exponential results compared to classic computers, where those operations were almost impossible. Unlike a classical computer that uses bits, 0 or 1, as the essential representation of information to compute the data, quantum computing brings new paradigms.

Qubits: The essential representation of information lies in quantum bits or qubits. A qubit is the fundamental unit of quantum information. It is a linear combination of two states, 0 or 1, as a vector representation in a Hilbert space:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

where α and β represent complex numbers satisfying the equation [3-5]:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

Superposition and Entanglement: Superposition is a property of quantum mechanics that allows qubits to exist as a combination of multiple states simultaneously. Unlike classical computing, this property

provides quantum computing to handle various solutions simultaneously and increase computational parallelism. The illustration of the previous quantum bit in a superposition state looks as follows:

$$|\psi\rangle = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle \quad (3)$$

Entanglement is a quantum phenomenon in which two qubits are so related in such a way that the modification of one qubit impacts the other one [6,7]. This property allows quantum computing to be more efficient in terms of speed.

Quantum Gates and Circuits: Quantum gates are the logical representation of the classical gate for the quantum area. They are reversible because we can recover the input from the output. They can change the amplitude of superposition and create entanglement between two or more qubits [8]. The standard gates are the Hadamard gate (H), which helps create superposition; Pauli gates (X, Y, Z) work as the classical version of the Not gate; the CNOT gate is used for entanglement [9]. Quantum circuits are like a model for quantum computation. Many gates are used in a quantum circuit to solve complex computations [10].

Introduction to quantum machine learning

Quantum machine learning is a field that combines the advantages of quantum mechanics with well-known machine learning methods. The robustness of quantum computing shows tremendous promise in processing data with less time.

A couple of parameters help improve a quantum machine learning system. The first one lies in quantum mechanics principles, which can reduce the size of machine learning models and the training time [11]. The critical aspect to remember here is quantum fidelity, which calculates the distance between two quantum states and is valid for classification and other algorithms that compare data [12]. The second parameter concerns optimization of the parameterized quantum circuits, which tend to reduce the cost function and attenuate the noise and decoherence related to quantum hardware [13].

Some techniques help researchers succeed in this domain. Quantum data modeling and mapping are essential for mapping classical data into quantum models [14]. Some common approaches concern angle encoding, amplitude encoding, and basis encoding [15]. Feature mapping helps map the quantum circuits to map data to a high-dimensional Hilbert space to compute data more efficiently [12,14].

Introduction to quantum federated learning

QFML is a technology that unites the computational capacity of quantum computing with machine learning algorithms. The idea stems from the need for organizations to protect their sensitive data. Data is no longer sent to a central server for computation but is accessed locally by dedicated frameworks. This decentralized learning model guarantees data security [16].

Another essential element is the quantum weights, which ensure that the data will be fully trained in the quantum domain [17]. Only these weights are transferred to the central model for merging.

Review

Research methodology

In carrying out our literature review, we were keen to avoid bias in data collection for this study. To this end, we decided to follow the PRISMA method, which offers a clear and precise approach to the success of such an undertaking. The PRISMA approach consists in defining the research questions, defining the keywords for the article searches, and selecting the quality databases. Once the articles were collected, we applied a filter based on our keywords to define a list of initial papers. Applying the principle of inclusion and exclusion, we were able to delimit a reasonable number of papers for our study.

The keywords selected for our study concern “Electronic Health Records,” “Blockchain,” “Federated Learning,” “Data security,” “Security of Quantum Machine Learning,” “Quantum Attack Vector,” “Data Privacy,” “Medical Devices,” “Quantum Computing,” “Quantum Key Distribution,” and “Quantum-Safe Encryption.”

The initial research yielded the results presented in Table *1*.

Database	Initial Keyword Search
IEEE Xplore	3,662
OpenAlex	1,856
ArXiv	2,137
Google Scholar	265
ACM	668
PubMed	154
Wiley	42
Science Direct	1,335

TABLE 1: Initial keyword search results by database

Before applying the inclusion and exclusion criteria, we ran the automated tool to identify the duplicates. We found out that 2,256 items were duplicates. Table *2* describes the inclusion criteria.

The exclusion criteria concern papers with keywords such as wireless 5G, 6G communication, servers, general data models, network protocols security, quantum hardware, and scalability. We did not consider papers on traditional blockchain that were not related to quantum federated learning.

Keywords for inclusion		
Electronic health record	Blockchain security	Quantum federated learning
Quantum computing security	Data privacy	Security and privacy
Security of quantum machine learning	Decentralized model aggregation	Data leakage
Quantum backdoor attacks	Medical devices	Privacy enhancement techniques
Model poisoning	Data poisoning	Smart contracts

TABLE 2: Keywords for inclusion criteria

Figure *1* describes the flow diagram that summarizes our search process.

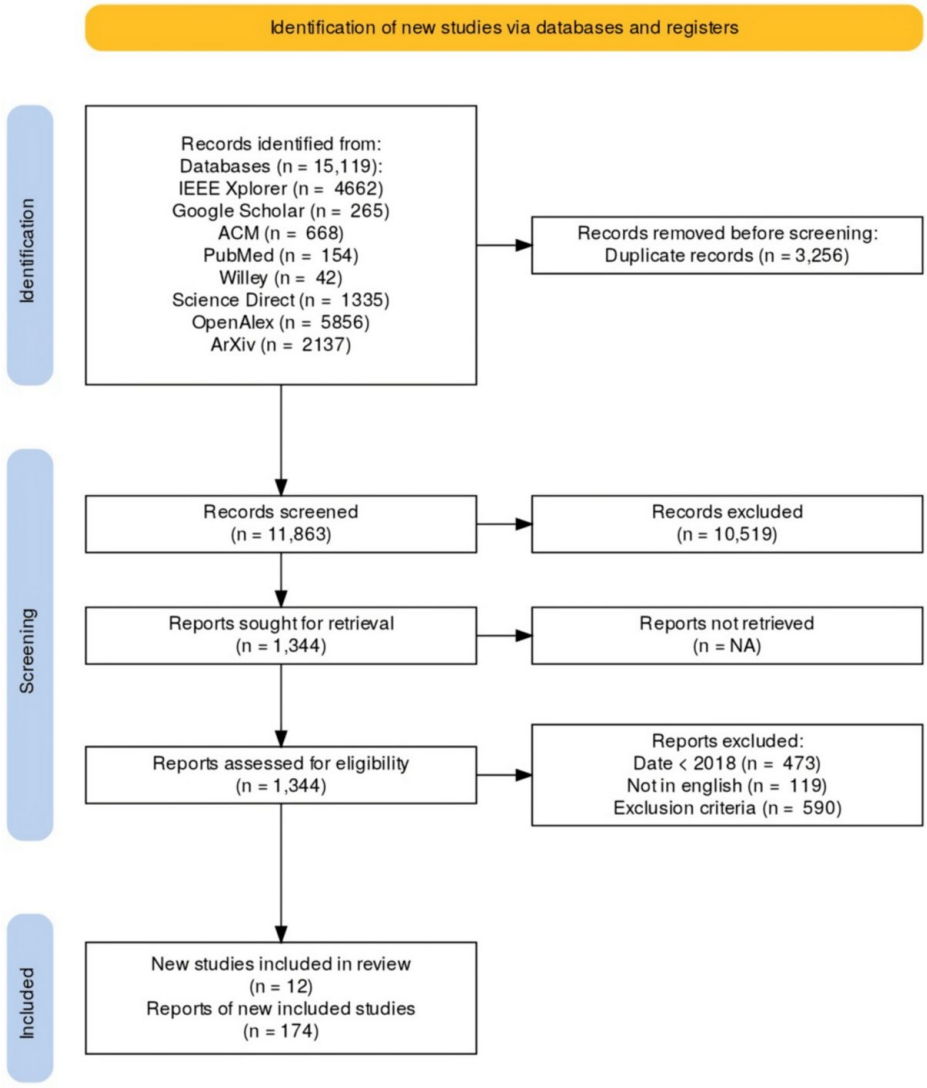

FIGURE 1: Search process documentation

To facilitate the screening phase, we used the intelligent filters of our search tool. By combining these filters according to the inclusion criteria, we could filter out articles directly relevant to our study. Around 6,519 articles were excluded. A total of 1,344 records were retrieved; 473 were excluded due to the published data dating before 2020. A total of 814 articles were excluded according to the exclusion criteria, and 19 articles needed to be fully in English. We were unable to access four papers due to some restrictions. From this screening process, only 38 articles were retained for our study.

The following section introduces the state of the art of quantum federated learning.

State of the art of quantum federated learning for electronic health records

Quantum federated learning shows a promising future in the field of electronic health records (EHRs). Before looking into that specific field, we will first investigate the general application and benefits of quantum federated learning.

One of the first advantages of using federated learning is its capacity to produce high-performance and convergence models. The Quantum Convolutional Neural Network for acoustic modeling shows a competitive accuracy of 95.12% on the Google Speech Commands Dataset due to their novel decentralized feature extraction framework [18,19]. Quantum federated learning improves accuracy and performance on data, especially on quantum data [20], and it shows promising results compared to classical federated learning [21]. It facilitates model convergence. Zhao [22], for instance, addresses convergence issues arising from non-IID data by proposing a one-shot communication that enables a great convergence on the model. Quantum federated learning helps in improving system performance. Yun et al. [23]

optimize system-level performance by introducing entangled slimmable Quantum Neural Networks and superposition coding. QuantumFed also shows excellent results on system performance by enabling collaborative training of a global model across quantum models without data exchange [24-26]. In general, quantum federated learning helps to manage resource allocation effectively. Blind quantum computing, for instance, helps to afford the computation of heavy tasks to remote servers [24,25,27].

Application of Quantum Federated Learning in Healthcare

Several healthcare sectors are already using quantum computing algorithms and platforms. Although the robustness of quantum computing shows considerable advantages, its adoption needs to catch up. In medical imaging, some studies [26,28] have proposed Digital Twin-assisted Quantum Federated Learning, an intelligent system, to facilitate disease diagnosis via 5G. Lusnig et al. [29] also proposed a hybrid neural network to facilitate the classification of images of liver steatosis for accurate diagnosis. Kais et al. [30] have proposed Quantum Convolutional Networks for medical image analysis. Their approach facilitates the distribution of training across different edges. The solution outperforms the classification task for pneumonia and CT-kidney. Quantum federated learning also helps to discover early cardiovascular and chronic diseases. Munshi et al. [31] suggested a framework to detect heart failure by integrating quantum federated learning for heart disease prediction using Quantum Support Vector Classifiers and Variational Quantum Classifiers [31,32]. Bhatia and Neira [33] also enabled a quantum tensor network as a collaborative tool to enhance federated learning in cancer diagnostics across multiple healthcare institutions. The framework optimizes the quantum tensor network for medical image analysis by enhancing accuracy while preserving patient privacy.

Privacy and Security Enhancement With Quantum Federated Learning

Privacy and security are preeminent values in securing sensitive, especially healthcare, data. The goal of quantum federated learning is to ensure that there will not be any leakage of sensitive data during the training process in multiple locations. Many protocols, techniques, and frameworks are used to tackle the challenges of securing sensitive data.

Among the protocols, the Gradient Hiding protocol shows promising results. Built upon the blind Quantum Bit Commitment [27,34], Li et al. [35] use the GHZ-based phase encoding multiparty summation protocol to propose two distinct protocols, one based on private inner-product and another one on incremental learning, to guarantee substantial privacy preservation with low communication resources. Another protocol that is used is Quantum Differential Privacy. Zhou and Ying [36] and Rofougaran et al. [37] introduced Quantum Differential Privacy to add some noise compatible with quantum states. The goal here is to guarantee a robust privacy scheme while allowing the benefits of quantum algorithms. Hirche et al. [38] pushed that work forward by looking for the amount of noise that could be added without making the computation useless.

Adopting quantum federated learning through quantum communication channels regarding techniques and frameworks ensures privacy preservation and HIPAA compliance [30,33]. The works of Wang et al. [16] and Javeed et al. [39] and FedQNN [40] provide a safe quantum communication channel to secure privacy data from eavesdrop attacks. Many frameworks, such as Pennylane [41], Qiskit, and Cirq [42], TensorFlow Federated frameworks [43], etc., help build computing frameworks and federated learning. The combination of these tools and frameworks can help build reliably secured quantum federated learning using Quantum Key Distribution such as BB84 [44] or E91 [45] to establish secure communication channels. Even though these tools and frameworks are not so widely used to secure quantum federated learning systems, they showed positive results in securing federated learning systems using Quantum Homomorphic Encryption [46,47], Quantum Secure Multiparty Computation [48], and Quantum Zero-Knowledge Proofs [49].

Integration of Blockchain With Quantum Federated Learning in Healthcare

Blockchain technology significantly enhances security and privacy using various mechanisms. Combined with federated learning and quantum federated learning, it brings more layers of security for safeguarding sensitive data. To foster privacy-preserving data sharing, Gayathri Hegde et al. [50] propose a blockchain-based federated learning framework that integrates decentralized technology for the security and privacy of EHRs. The use of encryption mechanisms also helps deepen security and privacy. Kanamarlapudi et al. [51] included an Attribute-Based Encryption within the blockchain technology to secure EHRs. CryptoQFL targets security and privacy challenges in quantum federated learning by introducing a framework that leverages quantum homomorphic encryption for distributed Quantum Neural Networks [52]. The data at rest and in transit allows hospitals to send the weight of their trained models safely. The study by Balasubramaniam and Surendiran [53] introduced a novel quantum-inspired blockchain that makes use of entanglement states to connect blocks and enhance security and privacy. The paper suggested an Entangled Quantum Medical Record system that can be used through the Medical Internet of Things to enhance privacy [53]. Decentralized model aggregation and secure access control are other key benefits of

the integration of blockchain and quantum federated learning. The study by Chen et al. [54] and Prajapat et al. [55] guarantees secure access to sensitive data through the blockchain by proposing a new token segmentation algorithm that allows patients and doctors to have total access to their data more efficiently. The usefulness of blockchain relies on the system's traceability and suitability. Such properties are essential in a healthcare environment. Sun et al. [56] proposed a framework that leverages Ethereum smart contracts as an architecture that provides EHR with a layer of security that guarantees robust data traceability and ownership [56,57].

The smart contract plays a pivotal role in integrating blockchain and QFML. The smart contract is an automated, predefined protocol to facilitate, verify, and enforce digital negotiation among involved parties [58,59]. Smart contract integration in the blockchain relies on many technologies and components. The first component concerns the verification mechanism, initialization, and registration. A designated manager and authority party initialize the smart contract at this stage. All the clients who want to participate must register for the smart contract [60]. Secure aggregation is another component. The data aggregation relies on two approaches. The first one is the on-chain mode, where the global model θ_{global}, for N clients, is computed as $\theta_{global} = 1/N\Sigma_i^N\Delta\theta_i$, for simple averaging, fast contributions, and high-quality updates [60]. The second approach uses off-chain mode, where contracts emit an event. The designated node reads the list of models, retrieves the full parameter, and performs the aggregation model [60]. The security and robustness are built around adding masks, authentication, and fault tolerance mechanisms. The third component is about the validation process. The contract validates the aggregation result at each round, and the authorized node can then download the θ_{global}. An incentive mechanism is used as a reward for consistent nodes [60].

There exist several other solutions that integrate blockchain technology, focusing on decentralization, privacy, and incentives that could be good candidates for QFML. The AgriFLChain is a blockchain solution that integrates smart contracts for secure model updates. Though it is designed for agriculture, it could be adapted for EHRs [61]. Blockchain-empowered Federated Learning provides a comprehensive survey on solutions that leverage blockchain technology for security, transparent federated learning, and smart contracts for model aggregation [62]. The Post-Quantum Secure Blockchain-based Federated Learning integrates post-quantum security like lattice-based cryptography to secure federated learning against quantum attacks [63]. Those solutions need the integration of the QML model. Quantum federated learning with a quantum data framework is a potential candidate for integrated blockchain technology [20]. Some solutions integrate decentralized quantum federated learning. Gurung et al. [64] proposed a blockchain-based quantum federated learning framework for metaverse environments. Liu et al. [65] proposed a framework that trains a classical model on a quantum-enhanced blockchain for federated learning. Table *3* presents a summary of some existing solutions.

Name	Description	Blockchain	Machine learning algorithm
CryptoQFL	Leverages quantum homomorphic encryption for federated learning	Not Integrated	QNN
AgriFLChain	Federated learning on a blockchain-based framework	Blockchain-based Decentralized Identifiers, verifiable credentials, smart contracts	ResNet-16, ResNet-28, CNN-DNN, and CNN-LSTM
QUMA	Quantum Unified Medical Architecture using blockchain	Quantum Blockchain system	Not integrated
PSQ-BFL	Post-Quantum Secure Blockchain-Based Federated Learning	Smart contract for PQC signature verification, recording hashes	CNN
Quantum Federated Learning framework	Quantum federated learning framework over quantum data	Not integrated	QCNN
BQFL	Blockchain-based Quantum Federated Learning framework for the metaverse	Smart contract	QNN
Quantum-enhanced blockchain FL	Integrates quantum Byzantine agreement	Quantum Blockchain system	Fully CNN, CNN

TABLE 3: Some existing frameworks

CryptoQFL, Cryptographic Quantum Federated Learning; AgriFL, Agricultural Federated Learning Chain; QUMA, Quantum Unified Medical Architecture; PSQ-BFL, Post-Quantum Secure Blockchain-Based Federated Learning; BQFL, Blockchain-based Quantum Federated Learning; QNN, Quantum Neural Network; CNN, Convolutional Neural Network; DNN, Deep Neural Network; LSTM, Long Short-Term Memory; QCNN, Quantum Convolutional Neural Network; PQC, Post-Quantum Cryptography; FL, Federated Learning

Security, Scalability, and Architecture Dilemma

Table *3* reveals that there are not many solutions that integrate blockchain technology with QFML algorithms. The complexity of such solutions requires attention to the security aspect of the designed architecture. Two types of blockchain can be chosen for the integration of QML. The first type is a permissionless blockchain that offers significant decentralization, transparency, censorship resistance due to the decentralized nature of public ledgers, and accessibility [66]. The second type is permissioned blockchain, which is suitable for private data where privacy and full contract are paramount. Some advantages of permissioned blockchain are high control over data, scalability, efficient handling of vast volumes of data, customization, and friendliness with regulatory compliance [66]. Permissioned blockchain could be a good candidate for EHR data [67].

When training a large volume of data, scalability becomes a critical aspect to consider. There is a dilemma of integration, scalability, and blockchain with security. For the sensitive element of EHRs, permissioned blockchain will rely on on-chain storage for security purposes. Such architecture brings challenges about storage overhead. Suppose we have a model with 1 million parameters, each of which is a 32-bit floating point number of 4 bytes. The architecture will require 40 KB to store a single model update. When we have 50 clients, the federated system will require storing at least 200 MB of data permanently for a single round. In the long run, this could lead to a scalability burden due to the high latency in data convergence. Since each client needs to send updates to the system to save the round on-chain, network congestion can increase the number of attack surfaces for fake clients.

This section enlightened the state of the art of quantum federated learning for healthcare. However, introducing and combining those technologies brings more complexity to the system, allowing new threats and vulnerabilities. The following section introduces us to the threats to quantum federated learning with blockchain.

Threats to QFML on blockchain

Integrating quantum federated learning with blockchain brings powerful results and complexifies the architecture, opening up many attack vectors. This section aims to navigate through the different components to analyze the potential impact such architecture could have on security and data privacy. Table *4* presents a taxonomy of the other attacks on QFML on Blockchain.

Area	Attack vector	Possible security solutions
QFML	Data poisoning	QKD, Lattice-based cryptography, DFQSB
	Model poisoning	QuMos, STIQ
	Gradient Leakage attack	Differential Privacy
	Quantum backdoor attack	QKD
	Quantum adversarial perturbation	Quantum Classifiers
Communication	Sybil attack, Noise exploitation, Grover's and Shor's algorithms	Post-quantum cryptography, Homomorphic encryption, QKD
Consensus mechanism	Majority attack, Byzantine fault tolerance, Grover's and Shor's algorithms	Post-quantum cryptography, Homomorphic encryption, QKD

TABLE 4: Attack vectors and possible security solutions

QFML, Quantum Federated Machine Learning; QKD, Quantum Key Distribution; STIQ, Secure and Transparent Information Quantum

Quantum Poisoning Attack

We can classify the poisoning attack into data and model poisoning attacks. Quantum data poisoning significantly threatens machine learning models, especially in quantum neural network systems. We can identify data poisoning attacks from the perspective of the nature of the attack. Here, the model structure could be at risk, and the attacker could take advantage of the diversity of the encoding methods and model structure used. For instance, in Quantum Neural Networks (QNNs), attackers can find avenues to launch attacks since the attack surface is large [68]. The attacker can mislabel by poisoning the data, potentially impacting the accuracy and the performance of the whole data [69,70]. Jia et al. [71] pointed out different data poisoning attacks such as targeted and untargeted poisoning attacks, scaling attacks, a little is enough attacks, and edge attacks that an attacker can leverage against the quantum federated model. The second type of poisoning attack refers to model poisoning. The literature reveals that the lack of centralized control of models' aggregation could be a potential factor in model poisoning attacks. The attackers can launch the attack by explicitly boosting the updates of the model and by leveraging a stealthy model poisoning attack that minimizes the accuracy of validation data and weight update statistics [72]. Another type of poisoning model happens during the model update. The attacker can exploit a model by injecting malicious data to alter model weights. Some tools and techniques, such as PoisonedFL, enhance the capability of poisoning data on the model by leveraging the multi-round consistency and the dynamic attack magnitude [73].

Gradient Leakage Attack

Gradient leakage attack is a security breach that targets quantum machine learning. Through the training and averaging process, the attacker can leverage this attack over gradient information to infer sensitive data. The inversion attack is a gradient leakage attack that can use the sensitivity of the gradient to infer private data. According to Wang et al. [74], the attacker can start by initializing random dummy data to feed into the model to get a dummy gradient; that dummy gradient will be successfully optimized to get close to the actual private data. Even though Mu [75] highlights the risk associated with gradient information leakage in the convolutional neural network, and due to the inherent nature of distributed computing protocols [35], Du et al. [76] questioned the effectiveness of gradient inversion attack on practical federated learning systems. Their study highlights the challenges such attack faces from the perspective of local training, model, and post-processing to reconstruct data under practical local training [76]. However, such an attack could be more realistic in a quantum area. Wu et al. [77] hypothesized that the key factor that makes inversion attacks successful relies on a low entanglement among gradients per data within the batch during stochastic optimization. A more sophisticated attack can leverage a timing side-channel attack to infer information about the executed quantum algorithms. Lu et al. [78] show that with such an attack, only ten measurements are enough to identify a specific quantum computer currently executing a circuit. With 500 measurements, leaked data could be achieved.

Quantum Backdoor Attacks

The classical approach of backdoor attacks has been applied to quantum computing. Quantum systems are vulnerable to backdoor attacks due to their decentralized nature and the complexity of quantum data processing. Quantum backdoor attack refers to the set of techniques that an attacker can leverage to

create hidden vulnerabilities that can be triggered at a different time. Many tools have been developed to test their models' effectiveness and stealthiness. QTrojan [79] proposes a circuit-level backdoor attack that adds two extra layers around the encoding layer of the victim QNN [79]. The two layers can be activated or deactivated anytime through a configuration file. Despite this improvement, QTrojan cannot attack QNNs universally with different circuit architectures since it was developed to attack circuits designed with an encoding layer [80]. QDoor extends these limitations by introducing novel quantum backdoor attacks that create a backdoor upon approximate synthesis in a QNN [80]. The experimentations show that QDoor provides a high success rate in performing backdoor attacks. Guo et al. [81] investigated adversarial and backdoor attacks on hybrid classical-quantum neural networks. They introduced a Qcolor backdoor that leverages Variational Quantum Circuit to encode qubits based on image color shifts as a trigger to design their backdoor attack. Unlike these frameworks based on triggers to be active and designed to be undetectable under standard conditions, there is still room for attackers to leverage classical backdoors on quantum systems [82,83]. Abad et al. [84] developed a new attack strategy that distributes backdoor triggers across multiple devices to enhance effectiveness and stealthiness.

Quantum Adversarial Perturbations

One attack vector which is difficult to counter is quantum adversarial perturbations. The attacker uses specific data manipulation that can significantly impact the quantum model and mislead the model into making incorrect predictions. The attacker will try to make a perceptible change in quantum encoded data at the level of superposition and entanglement. Liu and Wittek [85] were among the first authors to show the impact of adversarial attacks on quantum classifiers used in sensitive applications. The author demonstrated that the amount of perturbation required by an adversary to mislead a quantum classification system is inversely proportional to the dimensionality of the Hilbert space [86]. This indicates that the more dimensional spaces are, the more impact the adversarial attack will have. Gong and Deng [86] expanded this reflection by stating the existence of universal adversarial examples that can affect quantum classifiers [87]. The author demonstrated that for a set of k classifiers, increasing the perturbation by $O(\ln(k)/2^n)$ is sufficient to attain a universal adversarial risk that an attacker can leverage to launch an adversarial attack on a quantum federated learning system [86]. The adversarial perturbation could be challenging to detect, especially in the case of collective manipulation, where the attackers' actions are almost unnoticeable. Gómez-Ruiz et al. [88] investigated such reality and showed that when the number of qubit-bosonic modes is more than 3 in a given quantum information system, a group of quantum-enabled adversaries can maximally disrupt the global quantum state of the system. Moreover, in such a scenario, it is difficult to perceive the collective attack since the actions or movements of the attacker are not noticeable [88].

Attacks on Blockchain System

This section aims to address some attacks at the level of the blockchain system that affect the quantum federated system that uses blockchain technology. We will focus on network communication attacks such as Sybil and noise exploitation. We will look at attacks on consensus mechanisms such as majority attacks, Byzantine fault tolerance, and double-spending attacks. The cryptographic system's vulnerability is outside this study's scope.

Quantum Sybil attack is a type of Sybil attack on a quantum system where an attacker multiplies fake clients or entities to dominate a network, affecting the model updates from the learning process [89]. In differential privacy, where some noise is introduced in the sensitive data, it increases the risk of a Sybil attack and makes it difficult to identify [89]. The probabilistic nature of the quantum states and operations makes detecting a Sybil attack difficult. Based on this property, an attacker can quickly launch a poisoning attack by injecting malicious data, opening the room to other attacks, such as a Backdoor attack [90].

Noise exploitation is a vulnerability that an attacker can use to disrupt a quantum system. Noise results from the imperfection of gates and all the inherent processes of the quantum system, such as superposition states and entanglement. Subsequent excessive noise can lead to errors in quantum computations or affect the learning process and ultimately influence the model accuracy [91]. In that case, an attacker can deliberately inject additional noise to reach this goal. In such a situation, the attacker will directly or indirectly increase the communication cost, reducing the capability of the quantum federated learning system to handle many datasets or more complex models [91].

The reliability of a quantum federated system on blockchain will rely on the effectiveness of the consensus mechanism, which is a crucial component of the blockchain. Consensus mechanisms, such as Proof of Work and Proof of Stake, are used to ensure that all the participants agree on the current state of the ledger [92]. Vulnerability on the consensus mechanism can allow an attacker to try to gain control of more than 51% of the computing power (51% attack). A vulnerability in the consensus mechanism can also lead to the Byzantine attack, where an attacker can trick a node (Byzantine node) by sending randomly generated unitary to the server [93]. Since the quantum federated system globally updates the model periodically from each node, the Byzantine attack can harm the training process [93].

Quantum computing, with strong algorithms like Grover and Shor, poses a significant concern to cryptographic systems. In the case of quantum federated learning on blockchain, the communication channel where the system exchanges model weights is at risk. Grover's algorithm can break public-key encryption such as RSA and ECC to reveal sensitive data [94]. Shor's algorithm can speed up the brute force attack to weaken the consensus mechanism of the blockchain system.

Attackers have developed sophisticated techniques and methods to bypass existing security solutions, as seen in this section. The following section will focus on the new strategies, methods, and tools used to tackle the complexity of quantum federated systems on blockchain architecture.

Security solution and challenges for quantum federated learning on blockchain system

Researchers are working on new strategies to overcome the difficulties of facing complex attacks on quantum federated learning systems on blockchain. This section will limit our reflection to solutions directly related to data and model poisoning, backdoor attacks, gradient leakage, and adversarial perturbation attacks. Before we dig into the technical solution to threats to QFML, it will be essential for us to address the scalability issues, since they raise concerns about enlarging the attack surface.

A robust system should allow fast convergence for model aggregation. The architecture should be flexible and manageable to avoid network congestion, which the attackers can exploit. One solution to address the scalability issue is to use a sharding method that operates at layer 1 of the blockchain. Rebello et al. [95], for such an approach, propose ScaleFL as a scalable blockchain-based sharding solution. The framework allows interoperability by splitting the off-chain federated learning to facilitate model updates and verifications. Vadisetty and Polamarasetti investigate other solutions, such as optimistic and zero-knowledge rollups, to address the scalability issues of blockchain-based architecture [96]. Adding on to the solutions for scalability, Table *5*, inspired by the work of Liang et al. [66], presents some security aspects that can help build robust blockchain-based systems.

Items	Permissionless	Permissioned
Identity Privacy Protection	Cryptographic methods such as zero-knowledge proofs and ring signatures	Group and ring signatures; Attribute-Based Encryption (ABE)
Transaction Privacy Protection	Raiden network (Ethereum); Homomorphic encryption; Bulletproofs	On-chain encryption using Zero-knowledge proofs; Trusted Execution Environment (TEE); Differential privacy
Smart Contract Privacy Protection	Hawk – smart contract into a public on-chain; Ekiden that executes smart contract into TEEs	FabZk uses ZKP for private smart contracts; Confide executes transactions within TEEs
Use cases	Cryptocurrencies; Decentralized Finane (DeFi); Non-Fungible Token (NFTs)	Healthcare; Supply chain management; Financial services
Regulatory compliance (HIPAA)	Low integration due to a lack of access control management system	High integration due to robust governance and strong access control

TABLE 5: Comparison of permissionless and permissioned blockchain architecture

ZKP, Zero-Knowledge Proof

Data poisoning in a quantum federated system involves an attacker injecting malicious data into a dataset to manipulate the outcome of a model. Solutions to tackle such attacks refer to designing quantum cryptography and key distribution techniques, particularly Quantum Key Distribution. These provide a secure method to protect data at rest and in transit [97,98]. Since quantum federated learning system involves cloud computing to store data, Quantum Key Distribution with traditional encryption methods such as AES and lattice-based cryptography with E91 protocols have been experienced to secure data poisoning in the cloud [99]. Another solution that employs a Quantum Permutation Pad claims to secure data by integrating two cryptographic schemes that use quantum Clifford operators for authentication [100]. With the integration of a blockchain system, the solution is a Dual-Factor Quantum-Safe Blockchain, a tri-layered modular architecture with a dual-flow mechanism that uses quantum-safe encryption to assure the protection of data in transit against poisoning data [101]. The literature does not show extensive research on quantum security against model poisoning attacks. QuMoS was introduced as the first framework for preserving the security of the quantum machine learning model [102]. The approach of QuMoS is to distribute the model into multiple parts across different quantum cloud providers. It uses a reinforcement learning approach to optimize searching for the best computing nodes

to improve security and model accuracy [102]. The STIQ (Safeguarding Training and Inferencing of Quantum Neural Networks for Untrusted Cloud) framework proposed a novel method to secure quantum neural networks on distributed cloud systems, which can mask the accuracy and losses of the individual hosted model by up to 76% [103].

Tremendous efforts are ongoing to leverage defensive solutions against quantum adversarial perturbation that can also cause adequate damages to quantum federated systems. Researchers, for example, are developing quantum algorithms using variational approaches to optimize the model while preserving robustness against input noise. This is precisely the case of [104] which shows that quantum classifiers protect against weak perturbations of data and also against universal adversarial attacks.

The blockchain architecture brings enormous advantages for security gradient leakage since only aggregated updates can be communicated [105]. In his intent to propose a metric to measure the maximal quantum leakage, Farokhi [106] highlights two properties that can help build resilient architecture against gradient leakage. For this author, the channel application reduces information leakage, and if we maintain the quantum state independent of classical data, we reduce the risk of data leakage [106]. The integration of differential privacy into quantum federated systems shows promising results. The challenge remains in the calibration of the level of noise for an accurate balance between model accuracy and privacy. Li et al. [35] proposed two protocols, private inner product estimation to perform model aggregation and an incremental learning protocol to advance the ability to secure sensitive data in distributed federated systems.

Securing a quantum federated learning system on blockchain still has many challenges due to the complexity of the quantum system. There are yet-to-be-proven security measures that could effectively address specific attack types, such as quantum backdoor attacks.

Table *6* presents an overview of the security threats to quantum machine learning systems and the existing defense mechanisms and their limitations.

Security threats	
Quantum poisoning attacks	Data poisoning attacks: Scaling attacks, A Little Is Enough (ALIE) attacks, and edge attacks
	Model poisoning attacks: PoisonedFL framework, multi-round consistency attacks [63]
Quantum gradient leakage attacks	Gradient inversion attacks
	Timing side-channel attacks
Quantum backdoor attacks	Circuit-level backdoor attack (QTrojan)
	Approximate synthesis backdoor (QDoor)
	Hybrid classical-quantum backdoor (QColor)
Quantum adversarial perturbations	Universal adversarial attacks
	Collective attack
Blockchain specific attacks	Sybil attack
	Consensus mechanism attacks: Majority attack (51%), Byzantine fault tolerance, Double-spending attack
	Noise exploitation
Defense mechanisms	
Quantum resistant security solutions	Quantum Key Distribution (QKD)
	Lattice-based Cryptography
	Quantum Permutation Pad (QPP)
	Quantum Differential Privacy (QDP)
	Quantum Classifiers
	Quantum Homomorphic Encryption (QHE)
	Quantum Secure Multiparty Computation (QSMPC)
	Quantum Zero-Knowledge Proofs (QZKP)

Federated learning solutions	Gradient hiding
	Private Inner Product Estimation
	Incremental Learning Protocol
	Secure Channel using QKD
Blockchain security solutions	Attribute-Based Encryption
	Entangled Quantum Medical Records (EQMRs)
	Smart Contracts
	Homomorphic Encryption
Frameworks and tools	QuMoS
	Safeguarding Training and Inferencing of Quantum (STIQ) Neural Network for Untrusted Cloud
	Federated Learning using Quantum Neural Networks
	Frameworks: Pennylane, Qiskit, Cirq, Tensorflow Federated
Limitations	
Lack of robust solution to detect and prevent attacks like quantum backdoor attacks	
Lack of standardization to facilitate complexity and interoperability among quantum computing, federated learning, and blockchain architecture	
There is still open issue due to scalability and data latency. High communication overhead and low model accuracy give room for attacks such as Sybil and Denial-of-Service attacks	
There is still a lack of proper trade-off between noise inherent of quantum system like Noisy Intermediate-Scale Quantum computer (gates error, decoherence, measurement errors, crosstalk) with noise from Differential Privacy techniques	
Research gaps and future directions	
Budling of a standardized network that integrate quantum federated machine learning with blockchain	
The development of an advanced technique for noise mitigation in quantum area with differential privacy	
The development of robust framework capable of detecting and preventing backdoor and adversarial attacks	

TABLE 6: Security threats, defense mechanisms, limitations, and research gaps

Discussion and future directions

Quantum federated learning is becoming interesting in healthcare due to its ability to quickly process massive data. Integrating federated learning into healthcare has already shown promising results for security and privacy. The integration of federated learning with quantum systems and blockchain brings more complexity. The complexity relies on the interoperability issues regarding the type of language used to develop each system and the choice of the protocol and framework, which can pose some challenges for the aggregation of model weights from many hospitals. Since the philosophy of the quantum federated learning on blockchain is to facilitate the training process on hospital data, it will be urgent to lay down standards to facilitate the exchange of sensitive information among hospitals. Extensive work needs to be done in this area to assess the problem of data latency issues and scalability concerns when the number of clients is considerable. Some studies [64,107] started the conversation to address the question of quantum federated learning with the complexity concerning resource allocation, large-scale data complexity, and time constraint between the central server and the different nodes. However, the question of security regarding quantum federated learning remains at stake.

Quantum federated learning needs more investigation in terms of security. Concerning the backdoor attack, for instance, though we have some sophisticated tools [79] that launch successful attacks on quantum systems, we still lack counter solutions. Table 7 presents current solutions for classical federated learning with promising results.

Framework	Core mechanism	Accuracy	Attack success rate	Adaptability
DifFence [108]	Differential testing, two-step MAD outlier	N/A	4%	Quantum-resistant outlier detection
Zero-knowledge [109]	Zero-knowledge proofs, robust learning	N/A	N/A	Quantum-safe ZKP/crypto
Fedward [110]	Backdoor decomposition, magnitude sparsification	85%	10%	Quantum AmGrad, quantum clustering
G2uardFL [111]	Graph clustering for malicious isolation	N/A	10.61%	Quantum k-means clustering
Hybridized Shield [112]	Random grouping, partial disclosure, outlier analysis	97.92%	10.11%	Quantum grouping, quantum outlier, quantum encryption/QKD
FedCL [113]	Model prediction uncertainty	97.92%	10.11%	Quantum clipping, quantum outlier
BoBa [114]	Overlapping clustering for robustness	N/A	N/A	Quantum k-means, quantum data inference

TABLE 7: Comparison of classical backdoor frameworks

FedCL, Federated Contrastive Learning; MAD, Median Absolute Deviation; QKD, Quantum Key Distribution; ZKP, Zero-Knowledge Proof

DifFence Framework

DifFence framework uses differential testing that generates inputs to detect suspect behavior. It also uses Two-Step Median Absolute Deviation Outlier Detection, which helps identify malicious agents by detecting outliers in model prediction. The framework is efficient, with a backdoor accuracy of less than 4%. The framework is scalable in classical systems but needs further investigation into quantum systems. The challenges and limits are that the framework relies on classical machine learning techniques, which require an adaptation to the quantum systems. The framework does not have an integration mechanism to deal with noise and decoherence inherent to the quantum system. An adaption to a quantum system will require the development of quantum outlier detection to replace classical outlier detection methods. There is also a need to develop quantum differential testing or to build a hybrid solution to combine the two approaches.

Zero-Knowledge With Robust Learning

Zero-knowledge with Robust Learning uses a non-interactive zero-knowledge proof technique with a robust learning rate to filter out malicious model updates. The framework could be a good candidate for a quantum system. However, investigations need to be done to reduce communication overhead in a quantum system while considering noise and decoherence.

Fedward Framework

Fedward framework offers a robust defense system that uses Amplified magnitude sparsification (AmGrad) on local model updates, adaptive OPTICS clustering (AutoOPTICS), and adaptive clipping to eliminate backdoor attacks with a success rate of less than 10%. These techniques help to magnify malicious updates, making it easier to detect them. AutoOPTICS uses clustering with adaptive distance to separate good models from infected models. Adaptive clipping also uses model updates while preserving model accuracy. All these techniques apply to non-IID scenarios. However, they still lack a counterpart in the quantum system. The limitation is that the framework relies mainly on classical machine-learning methods. The framework is specific to classical backdoor attacks.

Hybridized Shield

The Hybridized Shield framework resists backdoor attacks by leveraging Oblivious Random Grouping, Partial Parameter Disclosure (PPD), and differential outlier analysis that help with detection and mitigation. The framework effectively reduces the attack success rate to 10.11% compared to insecure federated learning while maintaining an accuracy of 97.92% on clean data (MNIST and CIFAR-10). The framework relies on classical ML techniques such as random grouping and parameter disclosure, which

may not yet have a solution in a quantum system. There is a need to develop compatible quantum solutions such as a quantum Oblivious Random Grouping, a quantum-resistant Partial Parameter Disclosure, and a quantum outlier detection.

FedCL Framework

FedCL framework resists backdoor attacks by using highly uncertain models to detect potential malicious code. The dynamic clipping technique is used to limit the impact of undetected malicious updates on the global model. The framework provides good accuracy, 97.92% on clean data (MNIST, CIFAR-10). It maintains a low attack success rate (10.11%). FedCL claims robustness to non-IID data. However, the framework uses classical machine learning models such as uncertainty and dynamic clipping that do not allow direct translation to quantum systems. There is still a need to have a quantum-compatible uncertainty filtering technique. Quantum-resistant clipping and quantum outlier detection are needed to adapt FedCL to quantum systems.

G2uardFL

G2uardFL framework uses graph clustering to detect and isolate malicious clients. G2uardFL uses an attributed graph that captures client relationships based on their model updates. It then uses graph clustering to group clients with the same characteristics. Adaptive Poisoning Eliminating is the last module that mitigates previous implanted backdoor attacks. This approach makes it easier to detect malicious clients. Developing a new quantum graph clustering algorithm to adapt it to the quantum system is possible.

BoBa Framework

BoBa framework uses data distribution inference and overlapping clustering to detect malicious clients. The framework uses a voting system to assess the trustworthiness of clients in each cluster. This technique helps isolate malicious clients. Since the framework uses data distribution inference, we should find compatibility to handle quantum state similarities. We can also adapt quantum clustering techniques such as quantum k-means to handle classical quantum clustering methods.

Integrating quantum computing into these classical federated learning systems will open the need for a benchmark to test the robustness. The benchmark should also help to validate the scalability of the quantum federated learning system in terms of communication overhead, accuracy model, and the security aspect.

HIPAA compliance has two key rules, privacy and security, that align well with blockchain technology [115]. Using private blockchain technology, such as Hyperledger, a permissioned blockchain, enforces HIPAA compliance. Hospitals can rely on permissioned blockchain to implement robust governance and strict access control to EHRs. However, we do not have enough literature that combines quantum computing, federated machine learning, and security with blockchain. The study of HIPAA compliance on such architecture remains an area to explore.

Another area for further investigation concerns building QFML with blockchain, where quantum teleportation is used to share weights or model updates among nodes or clients. The integration of quantum network communication could be a potential candidate for dealing with issues regarding scalability.

The noise remains a challenging question to address. On the one hand, we have the noise inherent in the architecture of the quantum system itself. The Noisy Intermediate-Scale Quantum (NISQ) computer generates noise due to gate error, decoherence, measurement error, and crosstalk [116]. On the other hand, we have differential privacy that injects some noise to protect data. Considering these two aspects, we need a strong technique to mitigate noise and a concrete formula to measure the amount of noise to inject into sensitive data to enhance security and privacy without affecting the accuracy of the average model.

Solutions like post-quantum cryptography, homomorphic encryption, and secure smart contracts integrating non-fungible tokens with blockchain architecture bring some robustness to protecting data privacy and sensitive data in classical federated learning. We need more investigation to see how far those solutions remain robust in the quantum area.

Open issues

Some issues still need to be addressed. As we have seen, some backdoor attacks still bypass existing solutions. There is still a lack of a robust solution to detect and prevent attacks like backdoor attacks. We must overcome the lack of standardization to facilitate complexity and interoperability among quantum computing, federated learning, and blockchain architecture. Standardization should also promote interoperability among different quantum computing providers. There is a lack of a unified framework that can compute the same quantum circuit on different quantum providers. Scalability, data latency, and high energy consumption remain open issues. A complex dataset requires many qubits, leading to high error rates, noise, and low model accuracy. High communication overhead and low model accuracy allow attacks like Sybil and Denial-of-Service. Noise mitigation remains a big issue, and there is still a lack of a proper trade-off between noise inherent in quantum systems (like NISQ computers - gate errors, decoherence, measurement errors, crosstalk) and noise from Differential Privacy techniques. There is still a lack of a standardized network that integrates QFML with blockchain architecture.

Conclusions

As we have seen, the QMFL system on blockchain presents promising results in developing healthcare data security. Although integrating quantum systems on blockchain adds more complexity to existing federated learning solutions, it opens more room to hope for a better future. This work presented the specific attacks we can encounter in such an architecture. This study also helped us to find existing solutions that can help mitigate those threats and determine the future direction in which we should seek solutions. We still need to perform many experiments to see to what extent the threats to classical federated learning could potentially harm QFML on the blockchain.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Fabrice Nazaire Kameni Tcheumaga, Md Munirul Haque, Sheikh Iqbal Ahamed

Acquisition, analysis, or interpretation of data: Fabrice Nazaire Kameni Tcheumaga, Kevin Umba, Padmapriya Velupillaimeikandan

Drafting of the manuscript: Fabrice Nazaire Kameni Tcheumaga, Kevin Umba, Padmapriya Velupillaimeikandan, Md Munirul Haque

Critical review of the manuscript for important intellectual content: Kevin Umba, Padmapriya Velupillaimeikandan, Md Munirul Haque, Sheikh Iqbal Ahamed

Supervision: Md Munirul Haque, Sheikh Iqbal Ahamed

Disclosures

Conflicts of interest: In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Al-Huthaifi R, Li T, Huang W, et al.: Federated learning in smart cities: Privacy and security survey. Information Sciences. 2023, 632:833-857. 10.1016/j.ins.2023.03.033
2. Zhang Y, Zeng D, Luo J, et al.: A survey of trustworthy federated learning with perspectives on security, robustness, and privacy. arXiv. 2023, 10.48550/arXiv.2302.10637
3. Recio Hernandez A, Dzul Bermejo JH, Esparza Maldonado AL: Architecture of quantum computing. Journal of Engineering Research. 2024, 4:2-10. 10.22533/at.ed.3174152421055
4. Danish M, Rengarajan A: Quantum computing: Simplifying the future of communication. International Journal of Innovative Research in Computer and Communication Engineering. 2024, 12:6319-6322.
5. Nielsen MA, Chuang IL: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, New York; 2012. 10.1017/CBO9780511976667
6. Gill SS, Kumar A, Singh H, et al.: Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience. 2022, 52:66-114. 10.1002/spe.3039
7. Das K: Quantum computing. International Journal for Research in Applied Science and Engineering Technology. 2024, 12:895-903.
8. Barenco A, Bennett CH, Cleve R, et al.: Elementary gates for quantum computation. Physical Review A. 1995, 52:3457-3467. 10.1103/PhysRevA.52.3457

9. DiVincenzo DP: Two-bit gates are universal for quantum computation. Physical Review A. 1995, 51:1015-1022. 10.1103/PhysRevA.51.1015
10. Nayak P, Rathod S, Surabhi, et al.: Quantum computing: Circuits, algorithms and application. International Journal of Advanced Research in Science, Communication and Technology. 2024, 19321:149-158.
11. Evans EN, Byrne D, Cook MG: A quick introduction to quantum machine learning for non-practitioners. arXiv. 2024, 10.48550/arXiv.2402.14694
12. Schuld M, Killoran N: Quantum machine learning in feature Hilbert spaces. Physical Review Letters. 2019, 122:040504. 10.1103/PhysRevLett.122.040504
13. Benedetti M, Lloyd E, Sack S, et al.: Parameterized quantum circuits as machine learning models. Quantum Science and Technology. 2019, 5:019601. 10.1088/2058-9565/ab5944
14. Havlíček V, Córcoles AD, Temme K, et al.: Supervised learning with quantum-enhanced feature spaces. Nature. 2019, 567:209-212. 10.1038/s41586-019-0980-2
15. Schuld M, Sinayskiy I, Petruccione F: An introduction to quantum machine learning. arXiv. 2014, 10.48550/arXiv.1409.3097
16. Wang T, Tseng HH, Yoo S: Quantum federated learning with quantum networks. ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Seoul, Republic of Korea. 2024, 13401-13405. 10.1109/ICASSP48485.2024.10447516
17. Pokhrel SR, Yash N, Kua J, et al.: Quantum federated learning experiments in the cloud with data encoding. arXiv. 2024, 10.48550/arXiv.2405.00909
18. Yang C-HH, Qi J, Chen SY-C, et al.: Decentralizing feature extraction with quantum convolutional neural network for automatic speech recognition. arXiv. 2021, 10.48550/arXiv.2010.13309
19. Zhang Y, Zhang C, Zhang C, et al.: Federated learning with quantum secure aggregation. arXiv. 2023, 10.48550/arXiv.2207.07444
20. Chehimi M, Saad W: Quantum federated learning with quantum data. arXiv. 2021, 10.48550/arXiv.2106.00005
21. Yun WJ, Baek H, Kim J: Quantum split neural network learning using cross-channel pooling. arXiv. 2023, 10.48550/arXiv.2211.06524
22. Zhao H: Non-IID quantum federated learning with one-shot communication complexity. arXiv. 2023, 10.48550/arXiv.2209.00768
23. Yun WJ, Kim JP, Baek H, et al.: Quantum federated learning with entanglement controlled circuits and superposition coding. arXiv. 2022, 10.48550/arXiv.2212.01732
24. Xia Q, Li Q: QuantumFed: A federated learning framework for collaborative quantum training. arXiv. 2022, 10.48550/arXiv.2106.09109
25. Huang R, Tan X, Xu Q: Quantum federated learning with decentralized data. IEEE Journal of Selected Topics in Quantum Electronics. 2022, 28:1-10. 10.1109/JSTQE.2022.3170150
26. Qu Z, Li Y, Liu B, et al.: DTQFL: A digital twin-assisted quantum federated learning algorithm for intelligent diagnosis in 5G mobile network. IEEE Journal of Biomedical and Health Informatics. 2023, 1-10. 10.1109/JBHI.2023.3303401
27. Li W, Lu S, Deng DL: Quantum federated learning through blind quantum computing. arXiv. 2021, 10.48550/arXiv.2103.08403
28. Ullah F, Srivastava G, Xiao H, et al.: A scalable federated learning approach for collaborative smart healthcare systems with intermittent clients using medical imaging. IEEE Journal of Biomedical and Health Informatics. 2024, 28:3293-3304. 10.1109/JBHI.2023.3282955
29. Lusnig L, Comelli M, Boccato T, et al.: Hybrid quantum image classification and federated learning for hepatic steatosis diagnosis. Diagnostics. 2024, 14:558. 10.3390/diagnostics14050558
30. Kais S, Bhatia A, Alam M: Quantum federated learning in healthcare: The shift from development to deployment and from models to data. Research Square. (2023). https://www.researchsquare.com/article/rs-2723753/v1.
31. Munshi M, Gupta R, Jadav NK, et al.: Quantum machine learning-based framework to detect heart failures in Healthcare 4.0. Software: Practice and Experience. 2024, 54:168-185. 10.1002/spe.3264
32. Zielinski K, Kowalczyk N, Kocejko T, et al.: Federated learning in healthcare industry: Mammography case study. 2023 IEEE International Conference on Industrial Technology (ICIT), Orlando, FL, USA. 2023, 1-6. 10.1109/ICIT58465.2023.10143132
33. Bhatia AS, Neira DEB: Federated hierarchical tensor networks: A collaborative learning quantum AI-driven framework for healthcare. arXiv. 2024, 10.48550/arXiv.2405.07735
34. Brassard G, Crepeau C, Jozsa R, et al.: A quantum bit commitment scheme provably unbreakable by both parties. Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, Palo Alto, CA, USA. 1993, 362-371. 10.1109/SFCS.1993.366851
35. Li C, Kumar N, Song Z, et al.: Privacy-preserving quantum federated learning via gradient hiding. Quantum Science and Technology. 2024, 9:035028. 10.1088/2058-9565/ad40cc
36. Zhou L, Ying M: Differential privacy in quantum computation. 2017 IEEE 30th Computer Security Foundations Symposium (CSF), Santa Barbara, CA, USA. 2017, 249-262. 10.1109/CSF.2017.23
37. Rofougaran R, Yoo S, Tseng H-H, et al.: Federated quantum machine learning with differential privacy. ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Seoul, Republic of Korea. 2024, 9811-9815. 10.1109/ICASSP48485.2024.10447155
38. Hirche C, Rouzé C, França DS: Quantum differential privacy: An information theory perspective. arXiv. 2023, 10.48550/arXiv.2202.10717
39. Javeed D, Saeed MS, Ahmad I, et al.: Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. TechRxiv. 2023, 10.36227/techrxiv.170259169.96559894/v1
40. Innan N, Khan MA-Z, Marchisio A, et al.: FedQNN: Federated learning using quantum neural networks. arXiv. 2024, 10.48550/arXiv.2403.10861
41. Bergholm V, Izaac J, Schuld M, et al.: PennyLane: Automatic differentiation of hybrid quantum-classical computations. arXiv. 2022, 10.48550/arXiv.1811.04968
42. GAQ Team. Cirq. GitHub. (2024). https://github.com/quantumlib/Cirq.
43. Broughton M, Verdon G, McCourt T, et al.: TensorFlow Quantum: A software framework for quantum machine learning. arXiv. 2021, 10.48550/arXiv.2003.02989

44. Bennett CH, Brassard G: Quantum cryptography: Public key distribution and coin tossing. arXiv. 2020, 10.48550/arXiv.2003.06557
45. Ekert AK: Quantum cryptography based on Bell's theorem. Physical Review Letters. 1991, 67:661-663.
46. Broadbent A, Jeffery S: Quantum homomorphic encryption for circuits of low T-gate complexity. Advances in Cryptology -- CRYPTO 2015. Gennaro R, Robshaw M (ed): Springer, Berlin, Heidelberg; 2015. 9216:609-629. 10.1007/978-3-662-48000-7_30
47. Dulek Y, Schaffner C, Speelman F: Quantum homomorphic encryption for polynomial-sized circuits. arXiv. 2016, 10.48550/arXiv.1603.09717
48. Crepeau C, Gottesman D, Smith A: Secure multi-party quantum computing. arXiv. 2002, 10.48550/arXiv.quant-ph/0206138
49. Kumar B, Topno V, Banerjee P, et al.: Revolutionizing national security: An analysis of quantum computing's impact on government and defense. 2023 2nd International Conference on Futuristic Technologies (INCOFT), Belagavi, Karnataka, India. 2023, 1-9. 10.1109/INCOFT60753.2023.10425191
50. Gayathri Hegde M, Shrishti Bekal M, Deepa Shenoy P, et al.: Preserving privacy and security of electronic health records using blockchain-based federated learning (BFL) framework. 2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC), Rajkot, India. 2023, 853-859. 10.1109/R10-HTC57504.2023.10461823
51. Kanamarlapudi J, Singh A, Garg P: Privacy preserving for electronic health records using enhanced attribute-based encryption with blockchain. 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India. 2024, 1-6. 10.1109/IATMSI60426.2024.10503075
52. Chu C, Jiang L, Chen F: CryptoQFL: Quantum federated learning on encrypted data. arXiv. 2023, 10.48550/arXiv.2307.07012
53. Balasubramaniam A, Surendiran B: QUMA: Quantum unified medical architecture using blockchain. Informatics. 2024, 11:33. 10.3390/informatics11020033
54. Chen D, Zhang L, Liao Z, et al.: Flexible and fine-grained access control for EHR in blockchain-assisted e-healthcare systems. IEEE Internet of Things Journal. 2024, 11:10992-11007. 10.1109/JIOT.2023.3328382
55. Prajapat S, Kumar P, Kumar D, et al.: Quantum secure authentication scheme for Internet of Medical Things using blockchain. IEEE Internet of Things Journal. 2024, 11:38496-38507. 10.1109/JIOT.2024.3448212
56. Sun L, Liu D, Li Y, et al.: A blockchain-based e-healthcare system with provenance awareness. IEEE Access. 2024, 12:110098-110112. 10.1109/ACCESS.2024.3440170
57. Akarca D, Xiu PY, Ebbitt D, et al.: Blockchain secured electronic health records: Patient rights, privacy and cybersecurity. 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2019, 108-111. 10.1109/DESSERT.2019.8770037
58. Ye W: Private law interpretation of smart contracts. Renmin Chinese Law Review: Selected Papers of The Jurist. Shi J (ed): Edward Elgar Publishing, Cheltenham; 2023. 10:227-249. 10.4337/9781035313976.00013
59. Raghuvanshi KK, Kumar S, Kumar S, et al.: Smart contracts: Medical insurance contract for patient. Creating Smart Healthcare with Blockchain and Advanced Digital Technology. Malviya R, Sundram S (ed): Apple Academic Press, Oakville;; 2025. 145-162. 10.1201/9781003453963
60. Wu B, Seneviratne O: Blockchain-based framework for scalable and incentivized federated learning. WWW '25: Companion Proceedings of the ACM on Web Conference. 2025, 1761-1767. 10.1145/3701716.3717649
61. Manoj T, Makkithaya K, Narendra VG: A blockchain-assisted trusted federated learning for smart agriculture. SN Computer Science. 2025, 6:221. 10.1007/s42979-025-03672-4
62. Zhu J, Cao J, Saxena D, et al.: Blockchain-empowered federated learning: Challenges, solutions, and future directions. ACM Computing Surveys. 2023, 55:1-31. 10.1145/3570953
63. Commey D, Crosby GV: PQS-BFL: A post-quantum secure blockchain-based federated learning framework. arXiv. 2025, 10.48550/arXiv.2505.01866
64. Gurung D, Pokhrel SR, Li G: Decentralized quantum federated learning for metaverse: Analysis, design and implementation. arXiv. 2023, 10.48550/arXiv.2306.11297
65. Liu HW, Liu ZP, Yin HL, et al.: Quantum-enhanced blockchain federated learning via quantum Byzantine agreement. Science China Information Sciences. 2025, 68:180503. 10.1007/s11432-025-4471-7
66. Liang W, Liu Y, Yang C, et al.: On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: A comprehensive survey. ACM Computing Surveys. 2024, 56:1-35. 10.1145/3676164
67. Vinayasree P, Mallikarjuna Reddy A: A scalable, secure, and efficient framework for sharing electronic health records using permissioned blockchain technology. International Journal of Computational and Experimental Science and Engineering. 2024, 10:1-8. 10.22399/ijcesen.535
68. Lu S, Duan LM, Deng DL: Quantum adversarial machine learning. Physical Review Research. 2020, 2:033212. 10.1103/PhysRevResearch.2.033212
69. Tolpegin V, Truex S, Gursoy ME, et al.: Data poisoning attacks against federated learning systems. arXiv. 2020, 10.48550/arXiv.2007.08432
70. Koh PW, Steinhardt J, Liang P: Stronger data poisoning attacks break data sanitization defenses. Machine Learning. 2022, 111:1-47. 10.1007/s10994-021-06119-y
71. Jia Y, Fang M, Liu H, et al.: Tracing back the malicious clients in poisoning attacks to federated learning. arXiv. 2024, 10.48550/arXiv.2407.07221
72. Sun SH, Sugrim S, Stavrou A, et al.: Partner in crime: Boosting targeted poisoning attacks against federated learning. arXiv. 2024, 10.48550/arXiv.2407.09958
73. Xie Y, Fang M, Gong NZ: Model poisoning attacks to federated learning via multi-round consistency. arXiv. 2024, 10.48550/arXiv.2404.15611
74. Wang J, Guo S, Xie X, et al.: Protect privacy from gradient leakage attack in federated learning. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. 2022, 580-589. 10.1109/INFOCOM48880.2022.9796841
75. Mu Y: Deep leakage from gradients. arXiv. 2022, 10.48550/arXiv.2301.02621
76. Du J, Hu J, Wang Z, et al.: SoK: Gradient leakage in federated learning. arXiv. 2024, 10.48550/arXiv.2404.05403
77. Wu J, Hayat M, Zhou M, et al.: Concealing sensitive samples against gradient leakage in federated learning. Proceedings of the AAAI Conference on Artificial Intelligence. 2024, 38:21717-21725. 10.1609/aaai.v38i19.30171

78. Lu C, Telang E, Aysu A, et al.: Quantum leak: Timing side-channel attacks on cloud-based quantum services. arXiv. 2024, 10.48550/arXiv.2401.01521
79. Chu C, Jiang L, Swany M, et al.: QTROJAN: A circuit backdoor against quantum neural networks. ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2023, 1-5. 10.1109/ICASSP49357.2023.10096293
80. Chu C, Chen F, Richerme P, et al.: QDoor: Exploiting approximate synthesis for backdoor attacks in quantum neural networks. 2023 IEEE International Conference on Quantum Computing and Engineering (QCE), Bellevue, WA, USA. 2023, 1098-1106. 10.1109/QCE57702.2023.00124
81. Guo J, Jiang W, Zhang R, et al.: Backdoor attacks against hybrid classical-quantum neural networks. arXiv. 2024, 10.48550/arXiv.2407.16273
82. Yang D, Luo S, Zhou J, et al.: Efficient and persistent backdoor attack by boundary trigger set constructing against federated learning. Information Sciences. 2023, 651:119743. 10.1016/j.ins.2023.119743
83. Nguyen S, Nguyen T, Doan KD, et al.: Venomancer: Towards imperceptible and target-on-demand backdoor attacks in federated learning. arXiv. 2024, 10.48550/arXiv.2407.03144
84. Abad G, Picek S, Urbieta A: Time-distributed backdoor attacks on federated spiking learning. arXiv. 2024, 10.48550/arXiv.2402.02886
85. Liu N, Wittek P: Vulnerability of quantum classification to adversarial perturbations. arXiv. 2019, 10.48550/arXiv.1905.04286
86. Gong W, Deng DL: Universal adversarial examples and perturbations for quantum classifiers. National Science Review. 2021, 9:nwab130. 10.1093/nsr/nwab130
87. Qiu Y-Z: Universal adversarial perturbations for multiple classification tasks with quantum classifiers. arXiv. 2023, 10.48550/arXiv.2306.11974
88. Gómez-Ruiz FJ, Rodríguez F, Quiroga L, et al.: Vulnerability of quantum information systems to collective manipulation. Quantum Information Science - Recent Advances and Computational Science Applications. Steijl R (ed): IntechOpen, London; 2024. 10.5772/intechopen.1004935
89. Jiang Y, Li Y, Zhou Y, et al.: Mitigating Sybil attacks on differential privacy based federated learning. arXiv. 2020, 10.48550/arXiv.2010.10572
90. Xiao X, Tang Z, Li C, et al.: SBPA: Sybil-based backdoor poisoning attacks for distributed big data in AIoT-based federated learning system. IEEE Transactions on Big Data. 2024, 10:827-838. 10.1109/TBDATA.2022.3224392
91. Sahu H, Gupta HP: NAC-QFL: Noise aware clustered quantum federated learning. arXiv. 2024, 10.48550/arXiv.2406.14236
92. Zhou S, Li K, Xiao L, et al.: A systematic review of consensus mechanisms in blockchain. Mathematics. 2023, 11:2248. 10.3390/math11102248
93. Xia Q, Tao Z, Li Q: Defending against Byzantine attacks in quantum federated learning. 2021 17th International Conference on Mobility, Sensing and Networking (MSN). 2021, 145-152. 10.1109/MSN53354.2021.00035
94. Madill E, Nguyen B, Leung CK, et al.: ScaleSFL: A sharding solution for blockchain-based federated learning. BSCI '22: Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure. 2022, 95-106. 10.1145/3494106.3528680
95. Rebello GAF, Camilo GF, de Souza LAC, et al.: A survey on blockchain scalability: From hardware to layer-two protocols. IEEE Communications Surveys & Tutorials. 2024, 26:2411-2458. 10.1109/comst.2024.3376252
96. Vadisetty R, Polamarasetti A: Quantum computing for cryptographic security with artificial intelligence. 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA), London, United Kingdom. 2024, 252-260. 10.1109/ICCMA63715.2024.10843897
97. Singh A: An efficient quantum cryptography's algorithm for data security. Indian Journal of Engineering and Materials Sciences. 2007, 14:346-351.
98. Muruganantham B, Shamili P, Ganesh Kumar S, et al.: Quantum cryptography for secured communication networks. International Journal of Electrical and Computer Engineering (IJECE). 2020, 10:407-414. 10.11591/ijece.v10i1.pp407-414
99. Swetha D, Mohiddin SK: Quantum-enhanced security advances for cloud computing environments. International Journal of Advanced Computer Science and Applications (IJACSA). 2024, 15:1162-1171. 10.14569/IJACSA.2024.01506118
100. Barbeau M: Quantum data communication protection with the quantum permutation pad block cipher in counter mode and Clifford operators. F1000Research. 2023, 12:1123. 10.12688/f1000research.140027.1
101. Pabla T, Sultana A: Modular blockchain architecture: Securing data with quantum-safe encryption. 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), Kanazawa, Japan. 2024, 198-203. 10.1109/QCNC62729.2024.00038
102. Wang Z, Li J, Hu Z, et al.: QuMoS: A framework for preserving security of quantum machine learning model. arXiv. 2023, 10.48550/arXiv.2304.11511
103. Kundu S, Ghosh S: STIQ: Safeguarding training and inferencing of quantum neural networks from untrusted cloud. arXiv. 2024, 10.48550/arXiv.2405.18746
104. Dowling N, West MT, Southwell A, et al.: Adversarial robustness guarantees for quantum classifiers. arXiv. 2024, 10.48550/arXiv.2405.10360
105. Madni HA, Umer RM, Foresti GL: Blockchain-based swarm learning for the mitigation of gradient leakage in federated learning. IEEE Access. 2023, 11:16549-16556. 10.1109/ACCESS.2023.3246126
106. Farokhi F: Maximal information leakage from quantum encoding of classical data. arXiv. 2024, 10.48550/arXiv.2307.12529
107. Gurung D, Pokhrel SR, Li G: Secure communication model for quantum federated learning: A post quantum cryptography (PQC) framework. arXiv. 2023, 10.48550/arXiv.2304.13413
108. Kim Y, Chen H, Koushanfar F: Backdoor defense in federated learning using differential testing and outlier detection. arXiv. 2022, 10.48550/arXiv.2202.11196
109. Li L, Xu C, Zhang P: Zero-knowledge with robust learning: Mitigating backdoor attacks in federated learning for enhanced security and privacy. Tools for Design, Implementation and Verification of Emerging Information Technologies. Liu J, Xu L, Huang X (ed): Springer, Cham; 2024. 523:99-116. 10.1007/978-3-031-51399-2_6

110. Chen Z, Wang F, Zheng Z, et al.: Fedward: Flexible federated backdoor defense framework with non-IID data. arXiv. 2023, 10.48550/arXiv.2307.00356
111. Yu H, Ma C, Liu M, et al.: G2uardFL: Safeguarding federated learning against backdoor attacks through attributed client graph clustering. arXiv. 2023, 10.48550/arXiv.2306.04984
112. Rahman G, Saeed-Uz-Zaman, Li B, et al.: Hybridized shield: A framework for backdoor detection in secure federated learning systems. 2024 IEEE 7th International Conference on Big Data and Artificial Intelligence (BDAI), Beijing, China. 2024, 199-204. 10.1109/BDAI62182.2024.10692923
113. Long J, Chen Z, Wang F, et al.: FedCL: Detecting backdoor attacks in federated learning with confidence levels. 2024 IEEE International Conference on Multimedia and Expo (ICME), Niagara Falls, ON, Canada. 2024, 1-6. 10.1109/ICME57554.2024.10687918
114. Wang N, Shi S, Xiao Y, et al.: BoBa: Boosting backdoor detection through data distribution inference in federated learning. arXiv. 2024, 10.48550/arXiv.2407.09658
115. Hamela K, Shrivastava G, Umapathi P, et al.: Enhancing data security and privacy in electronic health records with blockchain technology. 2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan. 2024, 1829-1835. 10.1109/ICTACS62700.2024.10841078
116. Saki AA, Alam M, Ghosh S: Impact of noise on the resilience and the security of quantum computing. 2021 22nd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA. 2021, 186-191. 10.1109/ISQED51717.2021.9424258